Universidad Nacional Autónoma de México

Maestría en Docencia para la Educación Media Superior
Facultad de Ciencias
Matemáticas

Diseño y análisis de una experiencia de enseñanza basada en proyectos en un curso de Álgebra con estudiantes de la Facultad de Ciencias.

TESIS

QUE PARA OPTAR POR EL TÍTULO DE

Maestra en Docencia para la Educación Media Superior

PRESENTA:

Mat. Adriana León Montes

DIRECTOR DEL TRABAJO:
Dr. Alejandro Javier Díaz Barriga Casales

MÉXICO, CDMX.
Noviembre 2018

A todos los que me brindaron su apoyo,
consejo y compañía durante la realización de este trabajo,
mis más sinceros agradecimientos.

Índice general

Introducción

Frecuentemente los verbos explicar, probar y demostrar se utilizan como sinónimos en la práctica de la enseñanza de las matemáticas, ¿pero cuáles son las diferencias en el significado de cada una de estas palabras?.

Una explicación se situa en el nivel del locutor, es decir, aquella persona que pretende garantizar la validez de una proposición. Este hace uso de sus conocimientos y de su propia noción de verdad. La explicación no se reduce necesariamente a una secuencia de pasos lógicos deductivos y su base es esencialmente la lengua natural.

Por otro lado, la prueba es una explicación reconocida y aceptada ante una comunidad. Esto hace referencia que la prueba es un proceso social, cuya aceptación no depende del locutor, si no de un grupo de personas. Cabe señalar que el reconocimiento de una prueba no es definitiva, ya que puede ser aceptada por una comunidad y por otra rechazada. Un ejemplo de esto es la prueba de los cuatro colores. El teorema afirma que; con sólo cuatro colores se puede colorear un mapa en un plano o en una esfera, de tal manera que las regiones que compartan frontera no sea del mismo color. Esta afirmación fue planteada por primera vez en 1852, por Francis Guthrie[1] y fue hasta el año de 1976 que Appel y Haken dan un prueba aceptada. Ellos se apoyaron de la computadora, realizaron un gran número de operaciones para probar la validez de este teorema. Cientos de matemáticos la aceptaron, tal es el caso de Swart[2] y otros, como Tymoczko[3] la rechazan, él argumenta que debido a que la prueba no puede ser demostrada al nivel de las demostraciones tradicionales, la confiabilidad reside principalmente en factores empíricos.

Por último, la demostración es un tipo de prueba dominante en matemáticas. Entende-

[1]Matemático y botánico. Nació en Londres (1831) y falleció en Cap Sudáfrica (1899).

[2]Edward, R. Swart, él publicó en el revista *The American mathematical monthly* en 1980 su perpectiva a favor de la prueba de los cuatro colores realizada por Appel y Hakel. El artículo se encuentra en el siguiente enlace: https://www.tandfonline.com/doi/abs/10.1080/00029890.1980.11995128

[3]Thomas Tymoczko, él publica en la revista *The Journal of Philosophy* su opinión en contra de la prueba de los cuatro colores. Este artículo se encuentra en el siguiente enlace. *http* : *//www.thatmarcusfamily.org/philosophy/Course*$_W$*ebsites/Math*$_S$*08/Readings/tymoczko.pdf*

remos como *demostración* a una serie de enunciados organizados, siguiendo un conjunto bien definido de reglas. Lo que caracteriza a las demostraciones es el rigor formal del discurso, ya que se busca que en una demostración no exista espacio para la ambiguedad y su reconocimiendo no está ligado a la aceptación de una comunidad si no de "aceptar"lo es. Para los matemáticos la noción de demostración es escencial. Dentro de esta comunidad se encontraba David Hilbert, él es probablemente uno de los matemáticos más importantes que ha conocido el siglo XX. Uno de sus grandes intereses fue fundamentar la matemática, es aquí donde pone en manifiesto las ideas fundamentales de la demostración:

> *La ventaja de este tipo de demostraciones*[abstractas] *es que se eliminan las construcciones particulares aisladas para agruparlas bajo una idea fundamental, de modo que se pone claramente en evidencia lo que es escencial en la demostración*[4].

Hilbert soñaba con fundar las matemáticas sobre una base axiomática, esta visión es la que hace diferente la noción de prueba y de demostración, pues, a pesar de que Hilbert estaba equivocado, hoy en día las demostraciones en matemáticas están fundamentadas en los axiomas, en los teoremas, en las proposiciones, en los lemas y en un lenguaje formal.

Motivados en la noción de demostración y en la enseñanza en matemáticas a nivel superior, esta tesis tiene como propósito diseñar y analizar una experiencia de enseñanza basada en proyectos en un curso de Álgebra para estudiantes de las licenciaturas de Matemáticas, Actuaría y Ciencias de la Computación. El contexto de nuestra trabajo es la Facultad de Ciencias, UNAM. Nosotros realizamos una investigación acerca de la trayectoria curricular de las licenciaturas antes mencionadas y notamos que existe, un alto porcentaje de estudiantes que abandonan sus estudios o tienen un rezago extremo. Como consecuencia de esto último el promedio de titulación está alrededor de 10 años, donde el tiempo establecido para terminar en tiempo y en forma es de 5 años.

Así que nos preguntamos, ¿cuáles son los principales factores que causan la deserción y el rezago en estos estudiantes?. Logramos observar que dichas causas están relacionadas con los aspectos académicos (falta de madurez en la matemática formal), vocacionales (mala elección de la licenciatura) e interaccionales (dificultades para integrarse al medio académico y social de la institución). Teniendo en cuenta estos factores, determinamos la dirección de nuestra investigación. Primero, el diseño de actividades tiene como tema principal a desarrollar la Criptografía, ya que además de ser una rama de las matemáticas con gran potencial para enriquecer la educación matemática está vinculada con los temas de la asignatura de Álgebra Superior II (materia del troco común

[4]D. Hilbert, *Die Grunglagen der Mathematik*. Abh. Aus d. Math. Sem. d. Hamb. Univ., (1928), 65-83

de las licenciaturas de Matemáticas, Ciencias de la Computación y Acturía); segundo, la implementación de las actividades fueron pensadas para motivar a los estudiantes a partir de sus intereses profesionales, es decir, desde sus carreras y por último, fortalecer la comunicación entre ellos y el profesor.

Como metodología de investigación nos apoyamos de la Ingeniería Didáctica (?, ?), así logramos estructurar la investigación y para tener una visión más completa de nuestra propuesta de enseñaza utilizamos la Idoneidad Didáctica (?, ?) para evaluar nuestro trabajo y encontrar puntos de mejora. A continuación describiremos brevemente el contenido de cada uno de los capítulos de esta tesis.

En el Capítulo I, se realiza un análisis del contexto de la investigación, la Facultad de Ciencias. Desarrollamos brevemente la historia de esta institución, los planes de estudio de las licenciaturas de nuestro interes y por último mostramos algunos datos que muestran la trayectoria curricular de los estudiantes de Matemáticas, Actuaría y Ciencias de la Computación.

En el Capítulo II, desarrollamos el planteamiento del problema, el marco teórico y la metodología de la investigación. Consideramos que aquellos que son nuevos en el estudio de la didáctica de las matemáticas, este capítulo les proporcionará algunos conceptos básicos y generales fáciles de entender. Se desarrolla de manera sencilla la ingeniería didáctica y la idoneidad didactica.

En el Capítulo III, desarrollamos el análisis preliminar, el cual se corresponde a la primera fase de la ingeniería didáctica. Es aquí donde realizamos un análisis epistemológico de la Criptografía, describimos las ventajas y desventajas de una enseñanza tradicional y finalizamos con las características de los estudiantes que realizaron el proyecto de Criptografía.

En el Capítulo IV, desarrollamos el análisis *a priori*, el cual tiene como finalidad describir las actividades del proyecto de Criptografía, las respuestas que esperabamos de los estudiantes y por último identificar las posibles dificultades que ellos podrían presentar.

En el Capítulo V y VI, describimos los hechos didácticos significativos observados en la fase de la experimentación, utilizamos los indicadores de la idoneidad didáctica para evaluar nuestra propuesta didáctica e identificamos posibles mejoras para implementaciones futuras.

El Capítulo VII, realizamos una síntesis de la investigación para finalizar con las con-

clusiones.

Para finalizar, durante la implemetación de nuestro diseño, los alumnos se enfrentaron a diversas problemáticas que las clasificamos como el quéhacer de un matemático, en otras palabras, ellos conjeturaron, crearon ejemplos, formaron nuevos vínculos entre la Criptografía y otras ramas de las matemáticas, realizaron demostraciones, entre otros. Competencias que consideramos que toda persona debería desarrollar, pues al final hacer matemáticas es una forma de pensar.

Capítulo 1

Contexto de la investigación. Facultad de Ciencias, UNAM.

1.1. Introducción

El ingreso a la universidad es un logro que llena de orgullo, ya que pocos alcanzan esta meta; pero también muchos se quedan en el camino. Esta etapa de transición (del bachillerato a la universidad) es un tema de interés para muchos investigadores, debido a que es el inicio de un periodo crítico de adaptación que involucra diversos retos, entre ellos, socioeconómicos, culturales, personales, escolaridad previa, entre otros. Los cuales, contribuyen a que el estudiante determine su pertenencia o su abandono en sus estudios universitarios.

La decisión que deberán tomar los estudiantes universitarios de permanecer o abandonar sus estudios están en función del nivel de integración académica y social que logran alcanzar en la institución (?, ?). Es claro ver que la incorporación de estos dos aspectos depende de los intereses del alumno y del tipo de institución. Así que, intentando delimitar los factores que provocan que los estudiantes continuen sus estudios profesionales o que los abandonen los clasificamos en dos partes.

1. **Factores que permiten la permanencia de los estudiantes en la educación superior**
    - La calidad y prestigio de la institución.
    - La seguridad en la elección de una licenciatura.
    - La ayuda económica para sostener los estudios.
    - La integración social del estudiante al campus universitario.

2. **Factores que provocan el abandono de los estudiantes en la educación superior**
    - Escaza madurez y orientación académica inadecuada.
    - Situación de *shock* por todos los cambios (compañeros, nuevo sistema educativo, incluso lugar de vivienda).
    - Actitudes de inseguridad y desmotivantes.
    - La falta de recursos económicos.

Cabe señalar que los factores antes descritos tienen más impacto para los estudiantes de primer año de universidad; de modo que es considerado el inicio de un periodo crítico que influye significativamente en ellos.

En el caso particular de las licenciturasas cuya disciplina principal es el estudio de la matemática formal, además notamos que los factores que provocan el abandono están relacionados con los siguientes tres grandes rubros:

1. Falta de pensamiento matemático (el cual está relacionado a la escasa madurez).
2. Falta de competencias para utilizar y relacionar números, realizar operaciones básicas o interpretar resultados básicos en matemáticas (Esta relacionada con la orientación académica inadecuada).
3. Falta de motivación y perseverancia (Esta relacionada con la situación de *shock* y actitudes de inseguridad y desmotivantes).

Como resultado de ésta breve investigación acerca del impacto de la transición del bachillerato a la universidad en los estudiantes; en particular en aquellos que ingresan a licenciaturas donde el estudio principal es la matemática formal. Este trabajo pretende proponer un diseño instruccional de tal forma que los alumnos de primer año de las carreras de Matemáticas, Actuaría y Ciencias de la Computación de la Facultad de Ciencias, continuen sus estudios satisfactoriamente, fomentarles el pensamiento matemático y motivarlos.

El primer capítulo está enfocado a la contextualización de la investigación, es decir, describiremos brevemente la historia de la Facultad de Ciencias, los planes de estudio de cada una de las licenciaturas que nos interesa y por último las trayectorias curriculares de éstas desde 1968 hasta el 2010.

1.2. Orígenes de la Facultad de Ciencias

La Facultad de Ciencias como hoy la conocemos es una intitución dedicada a la investigacion, a la divulgación científica y a la enseñanza de la Ciencia. Esta escuela se creó en el año de 1938 e inició su operación al año siguiente.

Los orígenes de la Facultad de Ciencias comienzan en la década de 1910 con la inauguración de la Escuela Nacional de Altos Estudios en la Ciudad de México, que tiempo después será la madre de dos grandes facultades: la Facultad de Filosofía y Letras y la Facultad de Ciencias.

Esta escuela tenía como objetivo el perfeccionamiento de los estudios, la provisión de herramientas y de conocimientos para la investigación científica, así como la formación de profesores de enseñanza secundaria y superior. Para llevar a cabo lo anterior la institución estaba dividida en tres áreas: Humanidades, Ciencias exactas y naturales, y Ciencias sociales, políticas y jurídicas.

En la sección de Ciencias exactas y naturales, se impartían clases de biología, química, física y matemáticas. Sin embargo fue hasta 1912 que se dio el primer curso avanzado de matemáticas. La popularidad de ingresar a la Escuela Nacional de Altos Estudios aumentó y con el paso del tiempo se fue transformando.

En 1925 se divide en tres grandes escuelas:

1. La Escuela Normal Superior, que posteriormente quedó vinculada a la Secretaría de Educación Pública.
2. La Escuela de Graduados, se encargaba de los estudios de posgrado.
3. La Facultad de Filosofía y Letras donde se otorgaban grados de maestros y doctores en Filosofía y Letras, Ciencias Históricas y Ciencias en Matemáticas, Física y Biología.

Esta separación permitió que cada escuela se desarrollará de manera independiente y diez años después la Facultad de Filosofía y Letras se divide en dos: 1) La Facultad de Filosofía y Bellas Artes, donde se impartían clases de arquitectura, artes plásticas y música y 2) el Departamento de Ciencias Fisicomatemáticas, formada por la Escuela de Ingeniería, la Escuela Nacional de Ciencias Químicas y el Departamento de Ciencias.

Fue hasta este punto en la historia en que, gracias a estas últimas transformaciones y a la colaboración de profesores, se formaran las carreras profesionales de Física y

Matemáticas.

De esta manera la historia nos dice que para la creación de las carreras de Física y Matemáticas en México fue un proceso que estuvo lleno de modificaciones. En 1938 se aprueba la creación de la Facultad de Ciencias y un año después ésta abre sus puertas, a estudiantes interesados en estudiar física, matemáticas y biología.

Desde la inauguración de la Ciudad Universitaria, 1954, la Facultad de Ciencias ocupa un lugar en el campus central de la universidad. Debido al crecimiento en la población estudiantil de esta institución; en 1977 la Facultad se transladó a unas nuevas instalaciones, donde se encuentra hoy en día.

Actualmente, la Facultad de Ciencias capacita a profesionistas en diez licenciaturas distintas, de las cuales cinco están acreditadas con el más alto nivel cuyo objetivo de acuerdo al sitio oficial de la Facultad es formar científicos que realicen investigación y que eleven la cultura científica del país.

1.3. Planes de estudio de las licenciaturas Matemáticas, Actuaría y Ciencias de la Computación

Las licenciaturas de Matemáticas, Actuaría y Ciencias de la Computación tienen una duración currícular de ocho semestres o dicho de otra forma, de cuatro años. El plan de estudios de cada carrera está diseñado de tal forma que en el primer año adquieran los conocimientos básicos para continuar sus estudios universitarios. De modo que las tres licenciaturas comparten algunas asignaturas.

Los planes de estudio de las licenciaturas de Actuaría y Ciencias de la Computación han tenido modificación, actualmente se tiene los planes de los años 2015 y 2013 respectivamente. En matemáticas el currículo es del año 1983.

Debido a los años que corresponde cada plan de estudio y para fines de la investigación analizaremos la trayectoria de los estudiantes que se encuentran en las generaciones de 1986 y 2010.

1.3.1. Matemáticas

La Facultad de Ciencias busca que el perfil de los estudiantes que estén interesados en ingresar a la licenciatura de Matemáticas es principalmente gusto por esta disciplina. Por otro lado, la facultad pretende que el perfil de egreso contemple los siguientes aspectos:

> [$\cdots$] *un profesionista con gran capacidad de encontrar analogías y de modelar situaciones reales. Aprende las matemáticas y sus relaciones con otras disciplinas tanto científicas como sociales, en las cuales motiva y resuelve problemas. En su ejercicio profesional destacan la investigación, así como la aplicación de la matemática a otras ciencias como: economía, medicina, sociología, ingeniería, física y biología. Los matemáticos participan en equipos interdisciplinarios abocados a la resolución de problemas comunes y específicos, así como en actividades de docencia y difusión de la matemática en diferentes niveles.* [1]

La licenciatura está dividida en 8 semestres, en cada uno, el estudiante debe cursar 4 asignaturas, dando un total de 32 materias; 16 son obligatorias y 16 son optativas.

Los estudiantes de Matemáticas cuentan con las siguientes formas de titulación[2] .

- Tesis.
- Actividad de Apoyo a la investigación.
- Seminario de titulación.
- Actividad de apoyo a la docencia.
- Trabajo profesional.
- Proyecto de apoyo a la divulgación.

Todas las formas de titulación antes mencionadas, requieren de un trabajo escrito aprobado por un tutor y un jurado. Además, el estudiante deberá presentar una réplica oral del trabajo ante el jurado.

1.3.2. Actuaría

De acuerdo a la Facultad de Ciencias los actuarios son profesionistas que utilizan las matemáticas con el propósito de proveer información para la planeación, previsión y a

[1] https://web.fciencias.unam.mx/licenciatura/resumen/122)

[2] La información en relación a la licenciatura de matemáticas está diponible en el siguiente enlace http://www.fciencias.unam.mx/secretarias/general/dep/reglamentointernomatematicas.pdf

toma de decisiones, para resolver problemas económicos, demográficos y financieros.

Así como la licenciatura de matemáticas, la duración es de 8 semestres, equivale a un total de 46 asignaturas, de las cuales 42 son obligatorias y 4 son optativas.

Para que los estudiantes de Actuaría obtengan el título de grado, cuentan con las siguientes modalidades de titulación.[3]

- Actividad de apoyo a la docencia.
- Actividad de apoyo a la investigación.
- Exámenes internacionales.
- Proyecto de apoyo a la divulgación.
- Seminario de titulación.
- Servicio social.
- Trabajo profesional.
- Tesis.

Así como en Matemáticas, los estudiantes de Actuaría deberán presentar un trabajo por escrito avalado por un tutor y un jurado. Esta evaluación involucra una réplica oral del trabajo realizado ante el jurado.

1.3.3. Ciencias de la Computación

Ciencias de la Computación es una licenciatura que está diseñada para que los estudiantes logren aplicar los conocimientos matemáticos en el área de la computación. La facultad busca formar profesionales que puedan participar en proyectos que involucren programación, diseño y análisis de sistemas complejos para la automatización de diversas actividades [4].

El perfil de ingreso para la licenciatura de Ciencias de la Computación tiene como características principales.

1. Gusto y talento para las matemáticas.
2. Capacidad para apropiarse de actividades repititivas, como el recordar ciertos enunciados de los lenguajes de programación o secuencias de teclas para obtener algo.

[3] http://www.fciencias.unam.mx/secretarias/general/dep/reglamentointernoactuaria.pdf
[4] https://web.fciencias.unam.mx/licenciatura/resumen/104

3. Capacidad de abstracción y tendencia al perfeccionismo en la elaboración de trabajos.
4. Capacidad de análisis y concentración.
5. Capacidad para trabajar en equipo. [5]

Ciencias de la Computación consta de 8 semestres, con un total de 40 asignaturas, 28 obligatorias de la disciplina, 6 obligatorias de inglés y 6 optativas.

La licenciatura de Ciencias de la Computación, cuenta con las siguientes modalidades de titulación. Las cuales, el estudiante deberá presentar en cada una un trabajo por escrito aprobado por un tutor y un jurado. Además de una réplica oral ante el jurado. [6]

- Tesis.
- Actividad de apoyo a la investigación.
- Seminario de titulación.
- Actividad de apoyo a la docencia.
- Trabajo profesional.
- Servicio social.
- Proyecto de apoyo a la divulgación.
- Participación exitosa del concurso de programación de ACM.
- Quedar en el percentil del 3 % superior en el examen Graduate Record.
- Obtener un promedio superior a 9.5 en los estudios de la licenciatura, en tiempo curricular y sin haber cursado ninguna asignatura más de una vez.

Para fines de esta investigación, nos concentramos en el currículum de los primeros tres semestre de las licenciaturas de Matemáticas, Actuaría y Ciencias de la Computación.

A continuación se muestra una tabla con las asignaturas de las licenciaturas correspondientes a los primeros tres semestres.

Observamos que la asignatura en común durante este periódo es Álgebra. En este trabajo se enfatizará la importancia de esta materia en la formación de los estudiantes.

[5] (https://web.fciencias.unam.mx/licenciatura/resumen/104)
[6] http://www.fciencias.unam.mx/secretarias/general/dep/reglamentointernocomputacion.pdf

Licenciaturas	Primer semestre	Segundo semestre	Tercer semestre
Matemáticas	Álgebra Superior I	Álgebra Superior II	Álgebra Líneal I
	Cálculo diferencial e integral I	Cálculo diferencial e integral II	Cálculo diferencial e integral III
	Geometría Moderna I	Geometría analítica II	Optativa
	Geometría analítica I	Optativa	Optativa
Actuaría	Álgebra superior I	Álgebra superior II	Álgebra Linea I
	Cálculo diferencial e integral I	Cálculo diferencial e integral II	Cálculo diferencial e integral III
	Geometría analítica I	Geometría analítica II	Manejo de datos
	Teoría del Seguro	Programación	Matemáticas Financieras
	Inglés I	Inglés II	Probabilidad I
			Inglés III
Ciencias de la Computación	Álgebra Superior I	Álgebra Superior II	Álgebra Lineal I
	Estructuras discretas	Estructuras de datos	Modela y programación
	Matemáticas para las Ciencias Aplicadas I	Matemáticas para las Ciencias Aplicadas II	Matemáticas para las Ciencias Aplicadas III
	Inglés I	Inglés II	Inglés III

Antes de desarrollar la importancia del Álgebra, conoceremos más acerca de los estudiantes que cursan las licenciaturas de nuestro interés, en la siguiente sección se desarrolla el trayecto curricular desde el año de 1986 hasta el año 2010.

1.4. Trayectoria estudiantil

Desde los orígenes de la Facultad de Ciencias, la popularidad de los interesados en estudiar una carrera científica en esta institución aumenta con cada generación, actualmente se encuentran inscritos $10,126$ estudiantes.

A lo largo de este capítulo, se explicó el contexto de nuestra investigación y en particular tres licenciaturas. Ahora es momento de presentar la trayectoria curricular de los estudiantes, así como, el periodo de titulación.

La finalidad de este análisis es conocer el porcentaje de estudiantes que tienen una trayectoria regular en sus estudios, así como el rezago y el abandono que existe en estas licenciaturas.

Los datos que se presentan se obtuvieron del informe de la Facultad de Ciencias del año

de 2013 – 2014, el avance estudiantil que se muestra es en tiempo curricular, duración de la licenciatura de acuerdo al plan de estudios y en tiempo reglamentado, periodo adicional de un 50 % al determinado plan de estudios. El rango de años que se ilustran es de 1986 hasta el año 2010.

1.4.1. Datos de los estudiantes egresados

Las figuras 1.2 y 1.3 muestran los porcentajes de los estudiantes que terminaron sus estudios en tiempo curricular, y en el tiempo reglamentado de las licenciaturas de Matemáticas, Actuaría y Ciencias de la Computación.

Para el análisis de la información que se mostrará a continuación utilizaremos cierta nomenclatura, la cual se muestra en la siguiente tabla.

Nomenclatura	Significado
TC	Tiempo curricular
TC+1	Un año más del tiempo curricular
TC+2	Dos años más del tiempo curricular
TC+3	Tres años más del tiempo curricular
TC+4	Cuatro años más del tiempo curricular

Figura 1.1: Nomenclatura para el análisis de datos de los estudiantes egresados.

La siguiente gráfica muestra el tiempo currícular y reglamentado en que conluyen los estudiantes de Matemáticas, Actuaría y Ciencias de la Computación.

Observe que durante los últimas generaciones menos del 30 % de los estudiantes de las tres licenciaturas terminan en el TC, con peor porcentaje está Ciencias de la Computación, seguida de Matemáticas y por último de Actuaría.

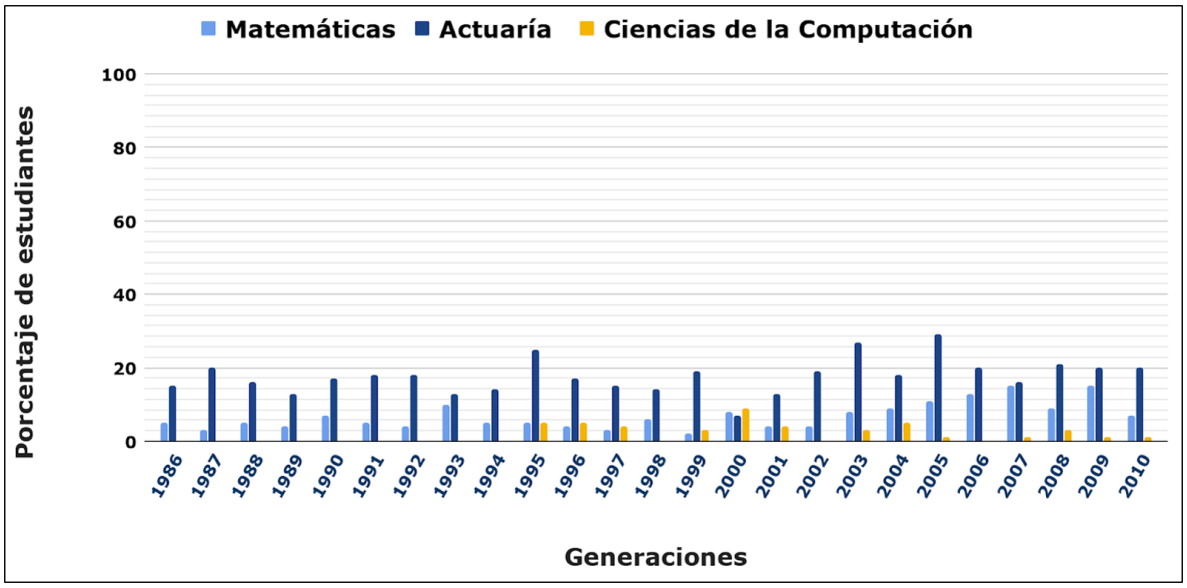


Figura 1.2: Egresados en tiempo curricular

Por otro lado, en la Figura 1.3 se muestra el porcentaje de estudiantes que terminan en tiempo reglamentado, Actuaría llega a un 70 %, Ciencias de la Computación está por debajo del 50 % y Matemáticas a penas sobrepasa el 25 %.

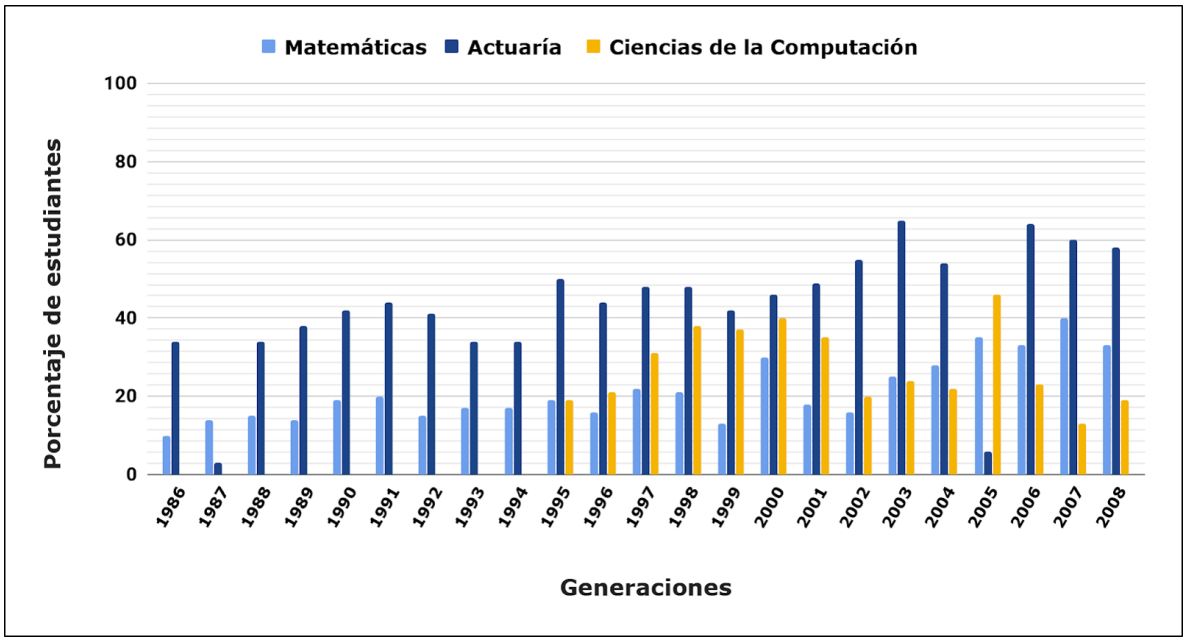


Figura 1.3: Egresados en tiempo reglamentado

1.4.2. Porcentaje egresos en cada licenciatura

Hasta este punto, conocemos el porcentaje de egresados de las licenciaturas de Matemáticas, Actuaría y Ciencias de la Computación. A continuación, analizaremos el porcentaje de estudiantes de cada una de estas carreras, que terminaron sus estudios en el intervalos de 5 años (tiempo curricular) hasta 10 años.

Debido a la complejidad del acceso a datos, consideramos la información de los egresados de las carreras de nuestro interés de la generación 2000 hasta la 2010.

Egresos en la licenciatura de Matemáticas

Observemos la siguiente gráfica 1.4, la cual muestra el porcentaje de estudiantes egresados entre 5 años (TC), hasta 9 años (TC+5).

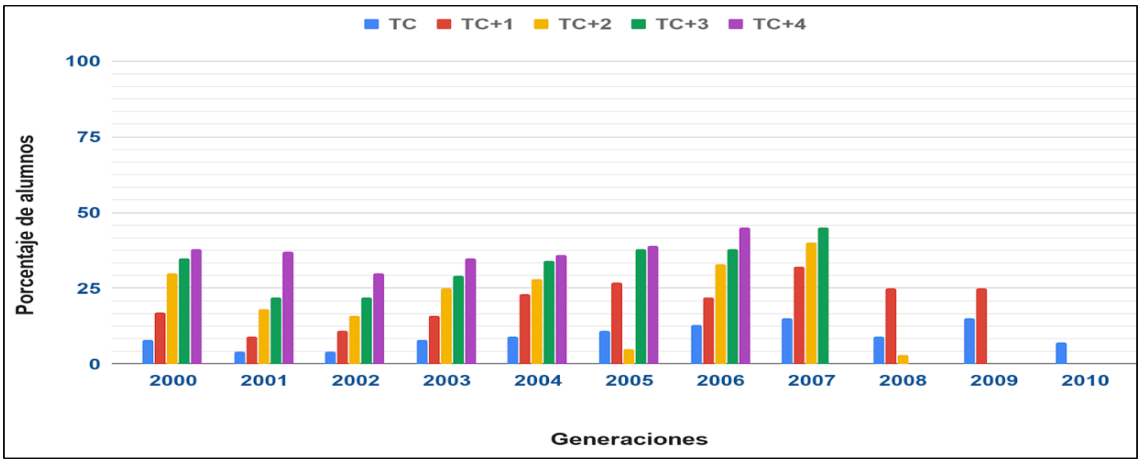


Figura 1.4: Egresados al término curricular uno, dos, tres y cuatro años despues en la licenciatura de Matemáticas.

Nótese que, el porcentaje máximo de estudiantes que terminaron en TC en Matemáticas es del 15 % en las generaciones del 2007 y 2008; y el mínimo es del 4 % en las generaciones 2001 y 2002.

Además, se puede observar que el mayor porcentaje de estudiantes que terminan se encuentran en un rango de 8 años (TC+3) y 9 años (TC+4).

Egresos en la licenciatura de Actuaría

En la gráfica 1.5 se muestran los porcentajes de estudiantes egresados de la licenciatura de Actuaría de cada generación del 2000 hasta 2010.

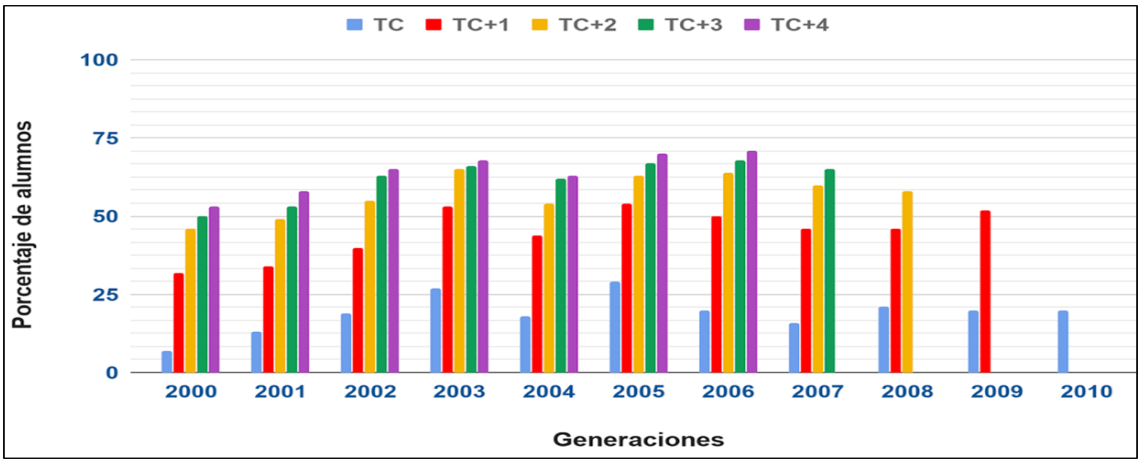


Figura 1.5: Egresados al término curricular uno, dos, tres y cuatro años después en la licenciatura de Actuaría.

Observe que, a diferencia del porcentaje de egresados en matemáticas, los estudiantes de actuaría tiene un mayor porcentaje de egresos en el periodo de 7 y 9 años. Sin embargo, es este porcentaje de egresos en TC es alrededor del 20 %.

Egresos en la licenciatura de Ciencias de la Computación

Por último, la licenciatura de Ciencias de la Computación, es la que tiene el menor número de egresos, el promedio es de un 2.5 %, en el año 2000 tuvo un 7 % de egresos como porcentaje máximo y un 0 % en el 2006.

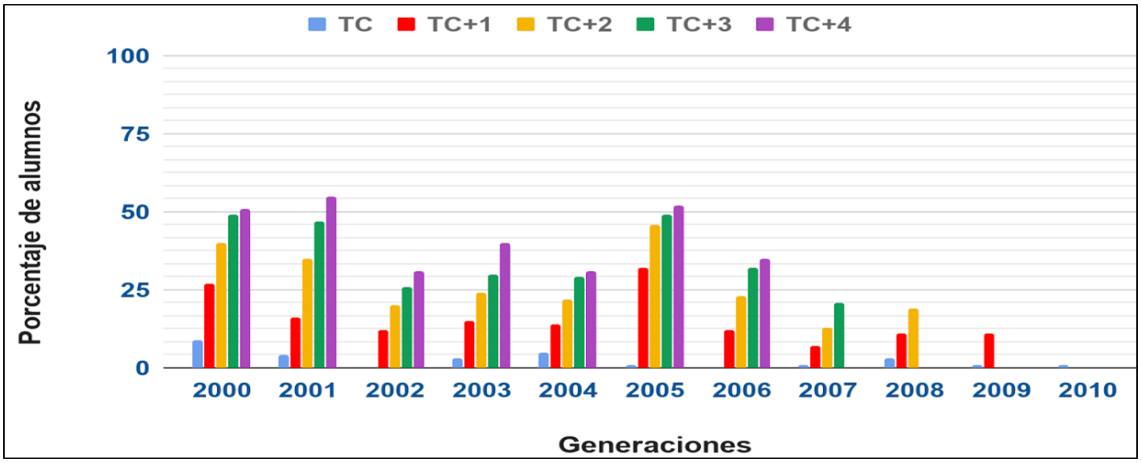


Figura 1.6: Egresados al termino curricular uno, dos, tres y cuatro años despues en la licenciatura de Ciencias de la Computación.

Con la información anterior, es claro observar que existe un problema en la trayectoria

curricular en los estudiantes de Matemáticas, Actuaría y Ciencias de la Computación. De modo que, este trabajo busca proponer una estrategía para que los alumnos continuen sus estudios con un mejor desempeño. Para esto, en el segundo capítulo argumentaremos los factores involucrados para que un estudiante permanezca o abandone sus estudios profesionales; así como las principales dificultades en el pensamiento matemático que ellos se enfrentan al comenzar sus estudios universitarios.

Capítulo 2

Planteamiento del problema, marco teórico y metodología

2.1. Introducción

Este segundo capítulo se enfoca en desarrollar el planteamiento del problema que nos gustaría resolver, el marco teórico y la metodología. Como resultado de este análisis, buscamos diseñar y analizar una propuesta didáctica que apoye al desarrollo de las capacidades argumentativas de los estudiantes del primer año de las carreras de Matemáticas, Ciencias de la Computación y Actuaría. Para llevar a cabo esto, construiremos un diseño instruccional, que consiste en la elaboración de un proyecto con fundamentos en la Criptografía y orientado a que los estudiantes lo resuelvan como parte de sus actividades durante el curso de Álgebra Superior, que es una asignatura del tronco común a estas licenciaturas.

Nuestro diseño instruccional tendrá como eje central el estudio de la Criptografía, el cual tiene un gran potencial para enriquecer la educación matemática. Se destacan las siguientes ventajas para el aprendizaje de los estudiantes (?, ?):

1. Los estudiantes están fascinados por la intriga y la aventura. Lograr que ellos encuentren la forma de cifrar y descifrar un mensaje a través de diversos métodos, permitirá que aprecien el poder y la belleza de las matemáticas.

2. Además, podrán descubrir por sí mismo nuevos conceptos y técnicas de las matemáticas.

Para la estructura de nuestro diseño nos apoyaremos de la Ingeniería Didáctica (?, ?).

Para terminar utilizaremos los Indicadores de la Idoneidad Didáctica como herramienta para encontrar aspectos de mejora de este trabajo.(?, ?).

Consideramos que si los estudiantes de primer año de las licenciaturas de nuestro interés realizan un proyecto de esta naturaleza y apoyado de esta metodología, entonces los estudiantes fortalecerán sus capacidades argumentativas en Matemáticas, obtendrán una mejor noción de cómo hacer demostraciones matemáticas y tendrán una motivación adicional en su trayectoria académica.

2.2. Planteamiento del problema

Con base en el capítulo anterior, es evidente que existe una deficiencia en el avance curricular de los estudiantes de las licenciaturas de Matemáticas, Ciencias de la Computación y Actuaría. Ante esta situación nos preguntamos, ¿cuáles son los principales factores que causan dicha deserción y rezago en estos estudiantes?.

Un estudio realizado por la UNESCO llamado Deserción y Repitencia en la Educación Superior en México, (?, ?). Afirma que el abandono voluntario de los estudiantes de nivel superior se presenta en los primeros meses posteriores al ingreso a la universidad y cinco de cada diez alumnos desertan antes del inicio del segundo año. Además, en este estudio, se describen las diferentes causas que provocan la deserción de estos estudiantes. Nosotros las clasificamos en cuatro:

1. Económica y familiar.
2. Académica.
3. La orientación vocacional y la mala elección de una licenciatura.
4. La interacción entre los estudiantes como pares y la relación con los profesores.

Para llevar a cabo la investigación de la deserción y repitencia en la educación superior en México, la UNESCO entrevistó a estudiantes de diferentes licenciaturas y universidades, tanto públicas como privadas que abandonaron sus estudios. Cabe señalar que la muestra de alumnos con estas características se tomó sin importar el contexto social, económico, cultural o institucional. A pesar de esto, la Organización logró establecer la clasificación antes señalada.

El estudio realizado por la UNESCO, permite visualizar las diferentes causas de la deserción y repitencia en los estudiantes de educación superior en México. De modo que, decidimos contextualizar esta situación a la Facultad de Ciencias y en particular a los

alumnos de las licenciaturas de Matemáticas, Ciencias de la Computación y Actuaria.

Entrevistamos a estudiantes del primer semestre de estas carreras y encontramos que las principales dificultades que se enfrentan al ingresar a sus estudios universitarios estan relacionados con el aspecto académico, el vocacional o la mala elección de la licenciatura y por último la interacción entre los estudiantes con el profesor. Los cuales corresponden a algunos puntos de la clasificación dada por la UNESCO, es decir, los puntos 2, 3 y 4 .

Avanzando con nuestro razonamiento, listamos las principales dificultades que notamos en los estudiantes de primer año que entrevistamos de la Facultad de Ciencias de la UNAM.

1. **Aspecto académico.**
   - Dificultades en el uso y manejo del lenguaje formal.
   - Dificultad para argumentar en matemáticas.
   - Dificultad para comprender y realizar demostraciones matemáticas.
2. **Aspecto vocacional o mala elección de la licenciatura.**
   - La falta de información de qué es estudiar una carrera científica.
   - La falta de personalidad y madurez intelectual del estudiante.
   - La falta de conocimientos y habilidades previas necesarias para realizar estudios superiores en el área científica.
3. **Aspecto interaccional.**
   - Dificultades para integrarse al medio académico y social de la institución.
   - Dificultades para afrontar el fracaso académico.

Por todo esto, nosotros nos enfocaremos en los aspectos 2, 3 y 4 de la clasificación de la UNESCO para el diseño, implementación y evaluación de este trabajo de tesis.

Dicho lo anterior, hemos estabecido la dirección de nuestra investigación, es decir, pretendemos diseñar, implementar y evaluar prácticas matemáticas [1] enfocadas en la realización de argumentaciones y demostraciones matemáticas, en la interacción entre los

[1]Una práctica matemática es toda acción (verbal, gráfica, etc) realizada por una persona para resolver problemas matemáticos, comunicar a otros la solución obtenida, validarla o generalizarla a otros contextos y problemas (?, ?)

estudiantes con el profesor y por último involucrar las actitudes, motivaciones y creencias de los estudiantes.

Con base en lo anterior, nos preguntamos: ¿qué características debería tener nuestro diseño instruccional para contrarestar los aspectos 2,3 y 4 definidos anteriormente?. Motivados por esta pregunta y en delimitar nuestro trabajo a nuestro contexto en la Facultad de Ciencias, nos preguntamos lo siguiente :

- ¿Cuál es la diferencia entre argumentación, prueba o demostración en matemáticas?
- ¿Cambia la noción de demostración en distintos contextos institucionales, (de una cultura a otra, de institución a institución, de nivel académico a otro, etc.)?
- ¿Cuáles son las principales dificultades que presentan los estudiantes al realizar una argumentación, prueba o demostración matemática?
- ¿Cuáles son los conocimientos esenciales para que un estudiante tenga éxito en sus estudios?
- ¿Cómo puede el docente afrontar la problemática del proceso de la enseñanza y aprendizaje en matemáticas?
- ¿Qué tipo de interacciones didácticas se deberían implementar para promover los aprendizajes matemáticos?

Es evidente que estas preguntas no son las únicas relacionadas a nuestro contexto, sin embargo, nos servirán de guía para lograr el fin de nuestra investigación.

2.3. Hipótesis

Para un mejor entendimiento de nuestra hipótesis, analizaremos brevemente el sistema educativo mexicano enfocándonos en el nivel media superior, ya que desde nuestra perpectiva las fortalezas o deficiencias que adquieran los estudiantes en este nivel están reflejadas de forma significativa en la educación superior si ellos deciden (o tienen lo oportunidad) de continuar sus estudios.

El sistema educativo en México tiene diferentes niveles de estudio, la educación básica (preescolar, primaria y secundaria), la media superior (bachilletaro) y la superior (licenciatura, maestría y doctorado). De los cuales, los primeros dos son obligatorios e impartidos por las normas del Estado; específicamente, la educación media superior es aquella cuyos estudios obligatorios antecedentes son los de la secundaria y tiene una duración entre dos y cuatro años[2]. Cabe mencionar que en México existen dos modalidades para cursar el bachillerato [3].

1. **Modalidad propedéutico**. Está interesado en el estudio de diferentes disciplinas científicas, tecnológicas y humanísticas y tiene la finalidad de proporcionar una cultura general de tal manera que sus egresados puedan incorporarse a las instituciones de educación superior.

2. **Modalidad bivalente**. Esta modalidad está estructurada con una componente propedéutica, es decir, que los egresados puedan continuar con sus estudios superiores y con una formación profesional, de modo que, los que terminan sus estudios a nivel medio superior obtengan un título de técnico profesional.

Al mismo tiempo, el último año del bachillerato los estudiantes tienen el derecho y la obligación de elegir un área de conocimiento, el cual tiene la finalidad de orientarlos a los estudios superiores de su interés. En total, existen cuatro áreas.

- **Área 1**: Físico-Matemáticas y de las Ingenierías.
- **Área 2**: Ciencias Biológicas, Químicas y de la Salud
- **Área 3**: Ciencias Sociales
- **Área 4**: Humanidades y de las Artes.[4]

Con lo anterior, describimos brevemente la estructura que tiene el nivel media superior. Ahora veamos lo siguiente: En el último sexenio (2012-2018) se impulsaron diferentes reformas educativas con la finalidad de proporcionar una educación de calidad a los estudiantes durante la educación obligatoria. Analizando la Reforma Integral de la Educación Media Superior (RIEMS, 2013) notamos que uno de sus prinicipales cambios es fomentar una enseñanza, por medio de las competencias, las cuales están clasificadas como generales y disciplinares. Notamos que la RIEMS ilustra la necesidad de que los alumnos desarrollen sus aprendizajes en contextos situados, haciendo uso de sus conocimientos y experiencias previas. Al mismo tiempo, en el área de matemáticas

[2]Esta definición está dada por la Secretaría de Educación Pública, publicado en 2008

[3]Puede consultar esta información en el siguiente enlace https://www.dgb.sep.gob.mx

[4]La descripción de cada área se tomó de la clasificación de la UNAM, la cual está disponible en el siguiente enlace: http://oferta.unam.mx/areas-conocimiento.html

tiene como finalidad propiciar el desarrollo de la creatividad, el pensamiento lógico y crítico, mediante procesos de razonamiento y la estructuración de las ideas.

Con lo elementos descritos en relación a la educación media superior tanto como su estructura y las nuevas reformas educativas en el área de matemáticas, identificamos las deficiencias:

- Al enfatizar en prácticas matemáticas contextualiadas a la vida cotidiana o a otras disciplinas, suponemos que no fortalecen competencias argumentativas propias del área.

- Suponemos que falta una mejor orientación para desarrollar prácticas matemáticas adecuadas para cada una de las cuatro áreas.

Lo anterior no quiere decir que estemos en contra de este tipo de prácticas matemáticas siempre y cuando se analice con mayor detenimiento y en las propuestas que podamos consultar esten descritas de forma más precisa. Aunque este enfoque no es parte de nuestro objetivo de estudio, así que lo consideraremos para investigaciones futuras.

Sintetizando, diremos que la estructura, los cambios en el bachillerato influyen de manera significativa en aquellos estudiantes que desean continuar con sus estudios; como primera consecuencia, está la elección de una licenciatura, seguido de su permanecia y desempeño. Cabe señalar, que es de nuestro interés observar los factores que están íntimamente relacionados con estas dos últimas consecuencias (permanencia y desempeño), en particular en estudiantes que ingresan a Matemáticas, Ciencias de la Computación y Acturía, ya que como se analizó en el capítulo uno, es evidente que existe una problemática en la permanencia y desempeño de estos alumnos. De modo que nuestra hipótesis ante está situación la describimos como sigue:

- El cambio de paradigma entre una enseñanza matemática enfocada en prácticas contextualizadas y las formales provocan un estado de "*shock*" en los estudiantes de nuevo ingreso; provocando niveles de desconfianza, perdida del interés y motivación. De modo que, si nuestro diseño intruccional relaciona estos dos enfoques podría causar: **1)**confianza en los alumnos, **2)** Cambio de perspectiva del quehacer de las matemáticas y de ellos mismos como aprendices de esta disciplina, y **3)** motivarlos a continuar con sus estudios o cuestionarse si están en la licenciatura que quieren.

- Los estudiantes se enfrentan a nuevas formas de prácticas matemáticas, en particular en la forma de validar o generalizar resultados. Como consecuencia, suponemos que si nuestro diseño instruccional tiene como eje principal la construcción de demostraciones por parte de los alumnos, ellos podrán mejorar sus capacidades argumentativas en matemáticas y otras áreas.

- La desconfianza y la falta de motivación se refleja en una interacción limitada entre estudiantes y con el profesor. De modo que, si en la implementación de nuestro diseño instruccional el profesor se involucra con los estudiantes, se fortalecerá la comunicación entre ellos y los alumnos adquirirán autonomía en el proceso de aprendizaje.

- Los alumnos que ingresan a las licenciaturas de nuestro interés generalmente son estudiantes de alto rendimiento en matemáticas, sin embargo, al enfrentarse al cambio de paradigma usualmente hay una baja en sus notas; esto provoca una frustación y difultad en confrontar el fracaso académico. Por lo que, si nuestro diseño instruccional fomenta la construcción de conjeturas[5] ,además que los estudiantes argumenten su validez por medio de una demostración o un contraejemplo, y por último que ellos reformulen la afirmación en caso de ser falsa a un enunciado verdadero. Suponemos que esto abrirá espacios donde el error sea una oportunidad de aprendizaje.

- Suponemos que si la evaluación del nuestro diseño instruccional está involucrada con la calificación final del curso de Álgebra Superior II. Ellos adquirirán una actitud responsable.

- Consideramos que si la evaluación del proyecto consiste en la entrega de un trabajo por escrito y una exposición grupal, entonces los estudiantes reflexionarán y encontrarán nuevas formas de argumentación, de manera que, ellos logren transmitir sus ideas de forma clara.

2.4. Objetivos

En esta sección describiremos los objetivos que pretendemos alcanzar con este proyecto.

Objetivo central:

Diseñar un proyecto de criptografía, que se implementará en un curso de Álgebra Superior II, que es del tronco común para las licenciaturas de Matemáticas, Ciencias de

[5]Una *conjetura* es una afirmación para la cual aún no hay demostración. En el siguiente enlace se encuentran algunas de las conjeturas más famosas en matemáticas. https://link.springer.com/content/pdf/bbm%3A978-1-4614-6636-9%2F1.pdf

la Computación y Actuaría.

Objetivos particulares:

- Que los estudiantes mejoren las prácticas argumentativas en matemáticas y que identifiquen diversos contextos de la demostración.
- Lograr un aprendizaje significativo.
- Fortalecer las interacciones entre los estudiantes y al mismo tiempo con el profesor.
- Que los estudiantes desarrollen habilidades para comunicar sus ideas.
- Que los estudiantes tomando conciencia de sus errores tomen decisiones pertinentes para mejorar su proyecto.
- Que los estudiantes se involucren en el proceso de titulación.

2.5. Metodología y marco teórico

La estructura de esta investigación se apoyará de la Ingeniería Didáctica (?, ?), de la Idoneidad Didáctica (?, ?) para evaluarla y encontrar puntos de mejora y por último nos apoyaremos de la criptografía como tema principal, el cual elegimos dado que permite motivar a los estudiantes y a través de su estudio tratar de llegar a los objetivos antes mencionados. Las metodologías que nos servirán de apoyo para este trabajo las clasificamos en dos:

1. Para la obtención del objetivo central: Nos apoyaremos de la Ingeniería Didáctica (?, ?).
2. Para la obtención de los objetivos particulares: nos apoyaremos principalmente de Significados institucionales de la demostración (?, ?) de la importancia del estudio de la criptografía en la educación superior. (?, ?) y por último de los indicadores de la idoneidad didáctica de procesos de enseñanza y aprendizaje de las matemáticas (?, ?) para la reflexión sobre el diseño, implementación de la evaluación del

proyecto de criptografía y encontrar puntos de mejora.

2.6. Ingeniería didáctica

La ingeniería didáctica (ID) es una metodología de investigación, que se introdujo en la didáctica de las matemáticas a principios de 1980 en Francia, apoyándose de la Teoría de Situaciones (TS) de Guy Brousseau [6]. La ID, buscó describir el trabajo didáctico como el de un ingeniero, el cual para realizar una labor específica, se apoya de los conocimientos científicos de su dominio y al mismo tiempo se encuentra obligado a trabajar sobre objetos (posiblemente) más complejos que los que aborda de forma práctica la ciencia (?, ?).

La Ingeniería Didáctica vista como una metodología de investigación tiene como características generales los siguentes puntos:

1. Es un esquema experimental sobre las realizaciones didácticas en clase, es decir, sobre la concepción, la realización, la observación y el análisis de secuencias.

2. El registro de estudios de caso y de la validación esencialmente, basada en la confrontación de un análisis a priori y a posteriori.

La ingeniería didáctica, con las características generales antes descritas, se ejecuta por medio de cuatro fases:

1. El análisis preliminar.
2. La concepción y el análisis *a priori*.
3. La experimentación.
4. El análisis *a posteriori*.

Para comprender mejor en qué consiste cada una se estas fases las describiremos a continuación.

[6]La Teoría de Situaciones matemáticas aparece en 1970 y nace como un método de descripción y de interrogación matemática de los mecanismos psicológicos y didácticos (?, ?).

2.6.1. Análisis preliminar

El análisis preliminar se sustenta en un marco teórico de la didáctica general, es decir, sobre los conocimientos didácticos adquiridos en el dominio de estudio y sobre un cierto número de observaciones. De los cuales, los más frecuentes son:

- El análisis epistemológico [7] de los contenidos contemplados en la enseñanza.
- El análisis de enseñanza tradicional y sus consecuencias.
- El análisis de las concepciones de los estudiantes, las dificultades y los obstáculos que determinan su evolución.
- El análisis del campo de restricciones en las que va a situarse la realización de la ingeniería didáctica.

Debido a la complejidad de los procesos de enseñanza-aprendizaje, cada una de las observaciones que podrían considerarse en el análisis preliminar son situacionales, es decir, que depende de cada contexto, de las necesidades tanto de los estudiantes como de los profesores e incluso de las instituciones. Por lo que, es indispensable determinar de los objetivos de la investigación y tener claridad de estos en el desarrollo de cada una de las fases de la Ingeniería Didáctica.

2.6.2. Concepción y análisis *a priori*

El análisis *a priori*, comprende de una parte descriptiva y de una predictiva; en el cual se centra el proceso de aprendizaje, es decir, en esta fase el investigador/docente diseña actividades con el objetivo de tener claridad del conocimiento involucrado, de los resultados que espera y en la forma en que se presentará el diseño.

Por otro lado, la Teoría de situaciones nos permite ver al análisis *a priori*, como un análisis de control del significado. Esto quiere decir que, la segunda fase de la Ingeniería Didáctica pretende dar respuestas a preguntas que buscan garantizar que el diseño de

[7] El análisis epistemológico, coloca en evidencia la evolución del rigor matemático con el paso del tiempo, su dependencia de los dominios matemáticos relativos y los niveles de elaboración de los objetos que él manipula (?, ?).

la situación [8] está bien construida y por tanto en la experimentación debería funcionar.

Dicho lo anterior, las preguntas más frecuentes que permiten tener claridad de los conocimientos involucrados, los resultados que se esperan y al mismo tiempo obtener un análisis de control son:

1. ¿Cuál es la respuesta al problema? (La resolución del problema debe ser dada desde el punto de vista del experto, es decir, del investigador/docente que diseña las actividades.)

2. ¿Cuáles son los conocimientos previos que necesitan los estudiantes para resolver la situación? .

3. ¿Cuáles son los conocimientos matemáticos involucrados en la situación? (Con esta pregunta, se busca detectar los conocimientos matemáticos alrededor de las actividades).

4. ¿Cuáles son las posibles estrategias que los estudiantes podrían utilizar para la resolución de problemas? (Esta pregunta marca el inicio de la etapa predictiva, pues el investigador/docente se pone en lugar de los estudiantes y se antepone a las posibles respuestas).

5. ¿Cuáles son las posibles dificultades que podrían tener los alumnos para abordar la situación? (El investigador/docente predice las posibles dificultades de los estudiantes).

6. ¿Cuáles son los posibles errores que podrían cometer los alumnos al resolver las actividades? (El investigador/docente se anticipa a los errores con la finalidad de convertir las dificultades a una situación de aprendizaje).

En conclusión, el análisis *a priori* permite que investigador/docente determine situaciones que posibiliten controlar comportamientos de los estudiantes y su significado. Consecuentemente, esta fase pretende que durante la experimentación se propicie un espacio adecuado para que los estudiantes busquen, indaguen, formulen, conjeturen, validen y comprueben sus resultados. De modo que, la validación del diseño de la situación, se llevará a cabo entre el contraste de los análisis *a priori* y *a posteriori.*

[8] El término situación lo tomamos de la TS de Brousseau, el cual se distingue pos su estructura, sus reglas, sus funcionamientos, las formas de conocimiento producido, etc. Además se clasifican en dos: *Situaciones matemáticas* y *Situaciones didácticas* (?, ?).

2.6.3. Experimentación, análisis *a posteriori* y validación.

La experimentación es la fase donde se implementa el diseño de la situación y es en este punto donde se recolecta la información necesaria para realizar la confrontación entre los dos análisis: *a priori* y *a posteriori*.

Teniendo en cuenta que, la experimentación es el desarrollo de las actividades propuestas por el investigador/docente, esta fase le sigue de forma inmediata el análisis *a posteriori*. Esta se basa en el conjunto de datos obtenidos durante la implementación de la situación, a saber, las observaciones realizadas en secuencias de enseñanza y también en los resultados de los estudiantes en clase o fuera de ésta.

Para ser más específicos en las observaciones obtenidas en la experimentación, los datos a menudo son completados por información obtenida por el uso de metodologías externas como: cuestionarios, entrevistas individuales o en pequeños grupos realizados en diversos momentos de la implementación o en sus resultados.

Por último, la validación de las hipótesis planteadas en la investigación, se fundamentan en la confrontación entre los dos análisis: el *a priori* y el *a posteriori*. Nótese que este proceso evaluativo es distinto a los esquemas usuales, debido a la extensión de análisis de la fase 2.

2.7. Indicadores de la idoneidad didáctica de procesos de enseñanza y aprendizaje de las matemáticas

La Didáctica de las Matemáticas como campo de investigación ha adquirido una consolidación a nivel internacional, ésta la vemos reflejada en revistas como Educación Matemática [9], RELIME [10], JOURNAL FOR RESEARCH IN MATHEMATICS EDUCATION, RDM [11]; así como libros o congresos.[12]

[9]En 2016, Educación Matemática fue clasificada como Revista de Competencia Internacional por el Sistema de clasificación de Revistas del CONACYT y el CONRICYT.

[10]Revista Latinoamerica de Investigación en Matemática Educativa

[11]Recherches en Didactiques des Mathématiques

[12]Las publicaciones consideradas relevantes en didáctica de las matemáticas se encuentran en la base de datos **MathEduc Databse** ((FIZ Karlsruhe)). La lista de estas publicaciones está disponible en: htt://www.zentralblatt-math.org/matheduc/

Pero, ¿qué es la Didáctica de las Matemáticas?. De acuerdo con D'Amore y Brousseau (2005) podemos entender a la Didáctica de las Matemáticas como una doble forma, es decir:

1. Como **divulgación de ideas**, fijando interés en la enseñanza.

2. Como **investigación empírica**, mostrando interés en el aprendizaje.

Nótese que, la doble forma de entender la Didáctica de las Matemátics fija su atención en los procesos de enseñanza-aprendizaje (?, ?) y para esto es indispensable la interacción del profesor (persona que se encarga principalmente del proceso de enseñanza) con el estudiante (individuo que se centra en el proceso de aprendizaje). Consecuentemente, es fácil observar que la educación es relacional, en otras palabras, el docente, el alumno y el tema de estudio sólo pueden ser entendidos en relación de uno y con el otro. El maestro trabaja para orquestar el contenido, las formas de presentarlo y las interacciones entre las personas que intervienen en la clase (?, ?).

Las investigaciones en la Didáctica de las Matemáticas, proveén herramientas a los profesores en formación o en ejercicio y conocimientos que permitan una mejor toma de decisiones en las fases de diseño, implementación y evaluación. Con esto último no pretendemos decir que la Didáctica de las Matemáticas tiene "*la receta*"para enseñar *mejor* o *bien* las matemáticas, pero posiblemente existen trabajos previos que nos ayuden en una nueva investigación o en la práctica docente.

Debido a que el profesor tiene un papel fundamental en los procesos de enseñanza-aprendizaje, es importante que éste reflexione sobre su práctica docente para tratar de mejorarla. Esta reflexión le permitirá detectar posibles ajustes en:

- Si el tema fue demasiado fácil o difícil.

- No se contempló todo el contenido que se pretendía desarrollar o trabajar en clase.

- La distribución del tiempo fue adecuada.

- Los alumnos estuvieron motivados.

- Los alumnos se cansaron.

- Entre otros.

El profesor reflexivo, necesita encontrar las posibles mejoras a su práctica docente. De modo que, es necesario tener una herramienta que permita determinar si su práctica es idónea[13] . En este trabajo, utilizaremos la noción de *Idoneidad Didáctica* basada en Enfoque Ontosemiótico (EOS)(?, ?).

2.7.1. Motivación y supuestos del EOS

El Enfoque Ontosemiótico (EOS) es un marco teórico que surge dentro de la Didáctica de las Matemáticas con la finalidad de articular diferentes puntos de vista y nociones teóricas sobre el conocimiento matemático, su enseñanza y aprendizaje (?, ?).

Dentro de este marco, se define el concepto *Instrucción Matemática* o proceso de estudio dirigido, como los procesos de enseñanza y aprendizaje organizados, en los cuales intervienen unos sistemas de prácticas matemáticas, unos sujetos (los estudiantes) y el profesor. (?, ?).

Nuestro interés en el concepto de la *Instrucción Matemática* son las distintias dimensiones interconectadas: *epistémica* (significados institucionales), *docente* (funciones del profesor), *discente* (funciones de los alumnos), *mediacional* (recursos materiales), *cognitiva* (significados personales) y *emocional* (sentimientos y afectos) (?, ?).

En el marco del EOS las dimensiones de un proceso de enseñanza-aprendizaje o de una instrucción matemática se dividen en seis facetas.

1. Epistemológica. Se refiere a la diversidad de objetos: situaciones, lenguajes, conceptos, proposiciones, procedimientos y a los procesos como la representación, la argumentación o la generalización[14].

[13]Según el diccionario de la RAE *Idóneo* se define como adecuado y apropiado para algo.

[14]De acuerdo con Michel Artigue *" el análisis epistemológico es necesario para el didáctico ya que tiene el fin de ayudarle a colocar a distancia y bajo control las "representaciones epistemológicas" 2 de las matemáticas inducidas por la enseñanza:*

- *Proporcionando una historicidad a los conceptos matemáticas que la enseñanza usual tiende a presentar como objetos universales tanto en el tiempo como en el espacio.*
- *Proporcionando, a la vez, una historicidad a las nociones matemáticas como las de rigor, ya que la enseñanza usual cultiva la ficción de un rigor eterno y perfecto de las matemáticas.*

(?, ?)

2. Ecológica, se refiere al currículum, la institución y la sociedad.

3. Interaccional, se enfoca en el diálogo, la interacción y la comunicación.

4. Mediacional, hace referencia a los recursos técnicos y temporales.

5. Cognitiva, se refiere a la comprensión situacional; conceptual, proposicional; a la comprensión procedimental argumentativa y comunicativa; y por último a la competencia metacognitiva.

6. Afectiva. Involucra las actitudes, afectos motivaciones y creencias.

Cada una de las facetas son análizadas en diversos niveles de análisis didáctico (las prácticas, las configuraciones de los objetos involucrados, las normas que condicionan y soportan las prácticas). La siguiente figura 2.1 (?, ?) nos ilustra las facetas consideradas en el proceso de enseñanza-aprendizaje según el EOS y los niveles de analisis didáctico.

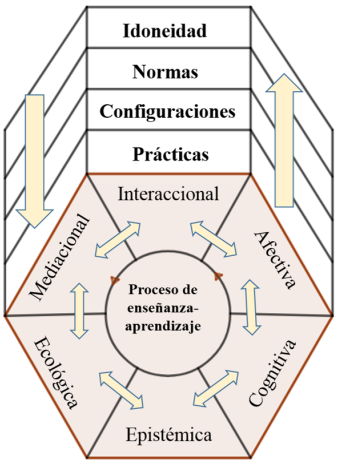


Figura 2.1: Facetas y niveles de análisis didáctico.

Las facetas epistémica y ecológica asumen supuestos antropológicos /socioculturales (?, ?); en cuanto a las facetas cognitivas y afectiva se adoptan de supuestos semióticos (?, ?); y para las facetas instruccional y medicional asumen una perpectiva socioconstructivista (?, ?).

2.7.2. La noción de la idoneidad didáctica

La noción de Idoneidad Didáctica, sus dimensiones, criterios y desglose operativo se introdujo en el marco del EOS como herramienta que permite el paso de una didáctica descriptiva explicativa a una didáctica normativa.

De acuerdo con Godino (2014), la Idoneidad didáctica se define

> [$\cdots$] *como el grado en que dicho proceso reúne ciertas características que permitan catalogarlo como idóneo para conseguir la adaptación entre los significados personales logrados por los estudiantes (aprendizaje) y los significaos institucionales pretendidos o implementados (enseñanza), teniendo en cuenta las circunstancias y recursos, disponibles (entorno)* [$\cdots$] *(?, ?)*

A partir de la definición, la Idoneidad Didáctica supone la articulación coherente y armónica de las seis facetas consideradas en el proceso de enseñanza-aprendizaje. De modo que obtenemos las siguiente definiciones.

- *Idoneidad epistémica*, se refiere al grado de representatividad e interconexión de los significados institucionales implementados (o pretendidos), respecto de un significado de referencia.

- *Idoneidad cognitiva*, expresa el grado en que los significado pretendidos/implementados son comprendidos por los alumnos.

- *Idoneidad interaccional*, se refiere al grado en el que se identifican conflictos semióticos y cómo se resuelven en el proceso de instrucción.

- *Idoneidad mediacional*, es el grado de disponibilidad y adecuación de los recursos materiales y temporales necesarios para el desarrollo del proceso de enseñanza-aprendizaje.

- *Idoneidad afectiva*, se refiere al grado de implicación (interés, motivación, $\cdots$) del alumnado en el proceso de enseñanza-aprendizaje. La idoneidad afectiva está relacionada tanto con factores que dependen de la institución como con factores que dependen básicamente del alumno y de su historia escolar previa.

- *Idoneidad ecológica*, es el grado en que el proceso de estudio se ajusta al proyecto educativo, la escuela, la sociedad.

Si el grado de alguna de las idoneidades antes descritas, satisface las condiciones para ser considerada *idóneo*, se le llamará como *idoneidad alta*, de lo contrario lo nombraremos como *idoneidad baja*. En el diseño de actividades, el investigador/profesor pretende obtener una idoneidad alta, es decir, cada faceta involucrada en el proceso de enseñanza-aprendizaje obtiene un grado máximo. Esta situación lo representamos como un hexágono regular; donde el grado máximo está representado como el vector que inicia del centro del hexágono hasta uno de los vértices. Veamos la siguiente figura 2.1 (?, ?).

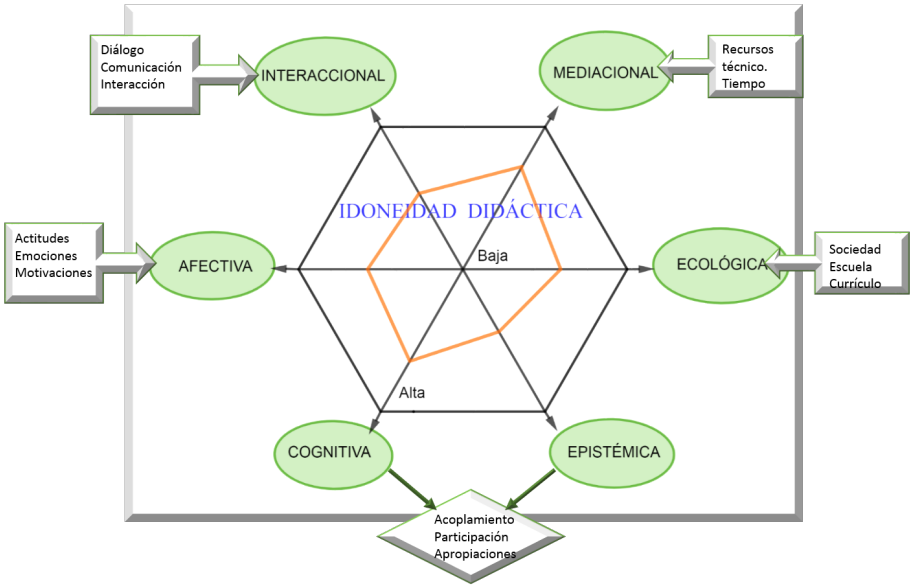


Figura 2.2: Idoneidad didáctica.

El hexágono irregular (color anaranjado) corresponde al grado de cada una de las idoneidades logradas, por ejemplo, en esta figura se obtuvo una idoneidad mediacional alta en comparación a la idoneidad interaccional.

2.7.3. Indicadores de la Idoneidad Didáctica

Nótese que para lograr un diseño instruccional con una idoneidad alta es necesario disponer de indicadores claros y explícitos para realizar un análisis. En esta sección describiremos los componentes y los indicadores para cada una de las idoneidades y así utilizarlos para evaluar el diseño de este trabajo.

Idoneidad epistémica

El análisis de la idoneidad epistémica de un proceso de estudio considera un análisis previo, para el cual se toman en cuenta preguntas como las siguientes:

- ¿Qué problemas contempla el proceso de estudio?
- ¿Qué lenguajes son utilizados?
- ¿Qué definiciones, propiedades y procedimientos están involucrados?
- ¿Qué argumentos o justificaciones se necesitan para llevar a cabo el proceso de estudio?
- ¿Cómo se relacionan cada una de las preguntas anteriores?

Entenderemos que un proceso de estudio tiene mayor idoneidad epistémica si los contenidos implementados (o pretendidos) representan bien a los contenidos de referencia.

En la siguiente tabla se muestran los componentes y los indicadores relevantes para esta idoneidad.

Un punto central para obtener una idoneidad epistémica alta, es la selección y adaptación de situaciones-problemas o tareas ricas. Las cuales deberán proporcionar a los estudiantes diversas maneras de abordarlas, que involucren diversas representaciones,y al mismo tiempo que ellos conjeturen, interpreten y justifiquen sus soluciones.

Idoneidad cognitiva

Entenderemos como idoneidad cognitiva alta, si el grado en que los contenidos de un proceso de estudios implementados son adecuados y son comprendidos por los estudiantes. La siguiente tabla muestra los componentes y los indicadores para esta idoneidad.

Como se indicó en la figura 2.2 la dimensión cognitiva toma supuestos semióticos. De modo que, en la implementación de un proceso de estudio y en el análisis de la idoneidad

COMPONENTES	INDICADORES
Situaciones-problemas	• Se presenta una muestra representativa y articulada de situaciones de contextualización, ejercitación y aplicación. • Se proponen situaciones de generación de problemas
Lenguajes	• Uso de diferentes modos de expresión matemática (verbal, gráfica, simbólica, ...) • Nivel del lenguaje adecuado a los estudiantes que se dirige el diseño. • Se proponen situaciones de expresión matemática e interpretación.
Reglas (Definiciones, proposiciones, procedimientos)	• Las definiciones y procedimientos son claros y correctos, y están adaptados al nivel educativo al que se dirigen. • Se presentan los enunciados y procedimientos fundamentales del tema para el nivel educativo dado. • Se proponen situaciones donde los estudiantes tengan que generar o negociar definiciones o procedimientos.
Argumentos	• Las explicaciones, comprobaciones y demostraciones son adecuadas al nivel educativo a que se dirigen. • Se promueven situaciones donde el alumno tenga que argumentar.
Relaciones	• Los objetos matemáticos (problemas, definiciones, proposiciones, etc.) se relacionan y conectan entre sí. • Se identifican y articulan los diversos significados de los objetos que intervienen en las prácticas matemáticas.

Figura 2.3: Componentes e indicadores de idoneidad epistémica (matemática)

cognitiva se busca que los estudiantes, mediante el proceso de enseñanza, aprendendan las matemáticas entendiendiéndolas, es decir, de una forma no mecánica ni memorística; que construyan nuevo conocimiento a partir de sus experiencias y conocimientos previos.

Idoneidad afectiva

Una idoneidad afectiva alta o baja se basa en el grado de implicación, interés y motivación de los estudiantes. La resolución de un problema matemático está asociado a una situación afectiva para la persona que lo resuelva, ya que están involucradas prácticas operativas y discursivas; moviliza creencias, actitudes, emociones o valores, los cuales influyen en el sentido o la forma de respuesta cognitiva que se espera del problema. La tabla 2.5 incluye los componentes e indicadores para el análisis de esta idoneidad.

Idoneidad interaccional

La idoneidad interaccional es el grado en que los modos de interacción permiten identificar y resolver conflictos de significado y favorecen la autonomía en el aprendizaje y el desarrollo de competencias comunicativas. En la tabla 2.6 contiene los componentes

Componentes	Indicadores
Conocimientos previos	• Los estudiantes tienen los conocimientos previos necesarios. • Los contenidos pretendidos se pueden alcanzar.
Adaptaciones curriculares a las diferencias individuales.	• Se incluyen actividades de ampliación y de refuerzo. • Se promueve el acceso y logro de todos los estudiantes.
Aprendizaje	• Los diversos modos de evaluación indican que los alumnos logran la apropiación de los conocimientos, comprensiones y competencias pretendidas: • Comprensión conceptual y proposicional; competencia comunicativa y argumentativa; comprensión situacional; competencia metacognitiva. • La evaluación considera distintos niveles de comprensión y competencia. • Los resultados de las evaluaciones se difunden y se utilizan para la toma de decisiones.

Figura 2.4: Componentes e indicadores de idoneidad cognitiva

e indicadores de esta idoneidad.

La idoneidad interaccional toma supuestos socio-constructivistitas. De modo que los estudiantes de matemáticas son considerados como participantes activos, en el que ellos mismos desarrollan herramientas y comprensiones, y comparten sus experiencias con otros. En otras palabras, la enseñanza de las matemáticas es considerada una actividad social.

Idoneidad mediacional

La idoneidad mediacional se entiende como el grado de disponibilidad y adecuación de los recursos materiales y temporales para el desarrollo del proceso de enseñanza-aprendiaje.

Dentro de los recursos materiales se encuentra el uso de la tecnología; si bien es un recurso que puede influenciar positivamente en la enseñanza es importante usarla estratégicamente de lo contrario podría no beneficiar al aprendizaje de los estudiantes. En la figura 2.7 se muestran los componentes y los indicadores de la idoneidad mediacional.

COMPONENTES	INDICADORES
Intereses y necesidades	• Las tareas tienen interés para los alumnos. • Se proponen situaciones que permitan valorar la utilidad de las matemáticas en la vida cotidiana y profesional.
Actitudes	• Se promueve la participación en las actividades, la perseverancia, responsabilidad, etc. • Se favorece la argumentación en situaciones de igualdad; el argumento se valora en sí mismo y no por quién lo dice.
Emociones	• Se promueve la autoestima, evitando el rechazo, fobia o miedo a las matemáticas. • Se resaltan las cualidades de estética y precisión de las matemáticas.

Figura 2.5: Componentes e indicadores de idoneidad afectiva

Idoneidad ecológica

La idoneidad ecológica se refiere al grado en que un plan o acción formativa para aprender matemáticas resulta adecuado dentro del entorno [15] en que se utiliza.

Para precisar lo anterior, la idoneidad ecológica toma en cuenta de que la enseñanza de las matemáticas tiene relación con otras materias, está involucrada en un contexto socio-cultural y de las personas involucradas en el proceso de enseñanza-aprendizaje.

En la figura 2.8 se desribe los componentes e indicadores que considera esta idoneidad.

Interacción entre facetas

En las secciones anteriores se identificaron algunos componentes e indicadores que toman en cuenta cada una de las facetas que propone la idoneidad didáctica. Cabe mencionar, que dichas facetas no se deben considerar como factores independientes, ya que en el proceso de enseñaza-aprendizaje todas y cada una se relacionan.

Considerar que el proceso de enseñanza está en constante interacción con diversos factores, implica que la clase tiene un papel importante. Sin embargo, esto no quiere decir que cada uno de los estudiantes alcanza el mismo nivel de desarrollo. Así que, es de

[15] Entendermos como entorno a todo lo que está fuera del salón de clases

COMPONENTES	INDICADORES
Interacción docente-discente	• El profesor hace una presentación adecuada del tema. • Reconoce y resuelve los conflictos de los alumnos. • Se busca llegar a consensos con base al mejor argumento. • Se usan diversos recursos retóricos y argumentativos para implicar y captar la atención de los alumnos. • Se facilita la inclusión de los alumnos en la dinámica de la clase.
Interacción entre los alumnos	• Se favorece el diálogo y comunicación entre los estudiantes. • Tratan de convencerse a sí mismos y a los demás de la validez de sus afirmaciones, conjeturas y respuestas, apoyándose en argumentos matemáticos. • Se favorece la inclusión en el grupo y se evita la exclusión.
Autonomía	• Se contemplan momentos en los que los estudiantes asumen la responsabilidad del estudio (plantean cuestiones y presentan soluciones; exploran ejemplos y contraejemplos para razonar, hacer conexiones, resolver problemas y comunicarlos)
Evaluación formativa	• Observación sistemática del progreso cognitivo de los alumnos.

Figura 2.6: Componentes e indicadores de idoneidad interaccional

suma importancia que una enseñanza de las matemáticas efectiva el profesor identifique qué es lo que saben los estudiantes, qué necesitan y al final los motive.

La noción de la idoneidad didáctica, sus componentes y sus indicadores la utilizaremos como herramienta para realizar la reflexión del profesor ante su propia práctica docente. Consecuentemente obtendremos una evaluación de la misma y así encontraremos puntos de mejora. La figura 2.9 describe los componentes e indicadores relativos a ciertas interacciones entre las facetas.

Por último, la teoría de la idoneidad didáctica trata de interrelacionar las distintas facetas que intervienen en el diseño, implementación y evaluación de procesos de enseñanza-aprendizaje de las matemáticas.

COMPONENTES	INDICADORES
Recursos materiales (Manipulativos, calculadores, computadoras)	• Se usan materiales manipulativos e informáticos que permitan introducir buenas situaciones, lenguajes, procedimientos, argumentaciones adaptadas al contenido pretendido. • Las definiciones y propiedades son contextualizadas y motivadas, usando situaciones y modelos concretos y visualizaciones.
Número de alumnos, horario y condiciones de aula.	• El número y la distribución de los alumnos permite llevar a cabo la enseñanza pretendida. • El horario del curso es apropiado. • El aula y la distribución de los alumnos es adecuada para el desarrollo del proceso instruccional pretendido.
Tiempo (De enseñanza colectiva/ tutorías; tiempo de aprendizaje)	• El tiempo (presencial y no presencial) es suficiente para la enseñanza pretendida. • Se dedica suficiente tiempo a los contenidos más importantes del tema. • Se dedica tiempo a los contenidos que presentan más dificultad de comprensión.

Figura 2.7: Componentes e indicadores de idoneidad mediacional

COMPONENTES	INDICADORES
Adaptación al currículo	• Los contenidos, su implementación y evaluación se corresponden con las directrices curriculares.
Apertura hacia la innovación didáctica	• Innovación basada en la investigación y la práctica reflexiva. • Integración de nuevas tecnologías (calculadoras, computadoras, TIC, etc.) en el proceso educativo.
Adaptación socio-profesional y cultural	• Los contenidos contribuyen a la formación socio-profesional de los estudiantes.
Conexiones intra e interdisciplinares	• Los contenidos se relacionan con otros contenidos intra e interdisciplinares.

Figura 2.8: Componentes e indicadores de idoneidad ecológica

COMPONENTES	INDICADORES
Epistémica-ecológica	• El currículo propone el estudio de problemas de ámbitos variados como la escuela, la vida cotidiana y el trabajo.
Epistémica-cognitiva-afectiva	• El contenido del estudio tienen sentido para los estudiantes en los distintos niveles. • Los estudiantes tienen confianza en sus habilidades para enfrentar problemas difíciles y mantienen sus perseverancia aun cuando la tarea sea compleja. • Se estimula a los estudiantes a reflexionar sobre sus razonamientos durante los procesos de resolución de problemas de manera tal que son capaces de aplicar y adaptar las estrategias que han desarrollado en otros problemas y contextos. • Las tareas que los profesores seleccionan para evaluar son representativos de los aprendizajes pretendidos.
Epistémica-cognitiva-mediacional	• El uso de recursos tecnológicos induce cambios positivos en el contenido de enseñanza, en los modos de interacción, motivación y en el aprendizaje de los estudiantes.
Cognitiva-afectiva-interaccional	• Las explicaciones dadas por los estudiantes incluyen argumentos matemáticos y racionales, no solamente descripciones de procedimientos. • Se incluyen contenidos motivadores, con adaptaciones razonables y apropiadas, que promueven el acceso y el logro de todos los estudiantes
Ecológica-instruccional (papel de docente y su formación)	• El profesor es comprensivo y dedicado a sus estudiantes • El profesor conoce y entiende profundamente las matemáticas que enseña y es capaz de usar ese conocimiento con flexibilidad en sus tareas de enseñanza. • El profesor tiene amplias oportunidades y apoyo para incrementar y actualizar frecuentemente sus conocimientos didáctico-matemáticos.

Figura 2.9: Componentes e indicadores de idoneidad de indicadores entre facetas

Capítulo 3

Análisis preliminar

En el análisis preliminar, buscamos recopilar una serie de datos que permita establecer la procedencia de las dificultades de la comprensión del tema de Criptografía. Este capítulo está clasificado en cuatro secciones:

1. Un análisis epistemológico del concepto de Criptografía.
2. Un análisis de la enseñanza tradicional y sus consecuencias.
3. Un análisis de la concepción que tienen los estudiantes de la Criptografía.
4. Un análisis de las restricciones del medio.

3.1. Análisis epistemológico

Actualmente, la mayoría de las organizaciones públicas o privadas dependen de los procesamientos de datos electrónicos. Las grandes cantidades de información generada son almacenadas en grandes bases de datos de computadora y son transmitidas a otras por medio de una red compleja de comunicación. Si no hay canales de transmisión seguros, los datos que se tranfieran podrían ser interceptados y como consecuencia podrían ser copiados, modificados, eliminados, sustituidos por otros, etc.[1] Hoy en día, existen leyes que protegen la confidencialidad de la información como los datos personales, las cuentas bancarias o las transacciones interbancarias (?, ?). Para lograr eso, las medidas de seguridad son establecidas con ayuda de la *Criptografía* [2]. Según la Real Academia

[1]En el año de 2018, la red social Facebook reportó que fue violada su seguridad. De modo que la información de 30 millones de usarios se vio afectada. El *hacker* o el atacante tuvo acceso a la información del muro, lista de amigos, grupos de los que son miembros y a los nombres de conversación en Messenger de cada usuario. https://www.theguardian.com/commentisfree/2018/oct/08/facebook-security-bad-zuckerberg-account

[2]Debido al aumento de usuarios del internet, es importante garantizar la seguridad en la red. Como consecuencia, por primera vez en la historia de internet, el día 11 de octubre de 2018, se cambiarón

Española, esta disciplina se define como el arte de escribir con clave secreta o enigmáticamente y como propósito principal es proteger la información que se transfiere por medio de redes de comunicación.

La *Criptografía* es una disciplina de gran importancia, ya que, por motivos políticos, militares, religiosos o comerciales, es necesario mantener la privacidad de la información. Por ejemplo, los jeroglíficos egipcios fueron usados por sacerdotes para mantener información política alejada de los faraones y de la población en general[3]; las investigaciones afirman que esta escritura forma parte de los primeros sistemas criptográficos registrados.

Uno de los métodos criptográficos por sustitución más antiguos que se conoce lleva por nombre *Polybios* (150 a.C), nombre que se le dio en reconocimiento del historiador griego del mismo nombre y quien se considera fue su creador. El proceso de cifrado está basado en una tabla como la que se muestra a continuación.

	A	B	C	D	E
A	A	B	C	D	E
B	F	G	H	I/J	K
C	L	M	N	O	P
D	Q	R	S	T	U
E	V	W	X	Y	Z

Se consideran el primer renglón y columna como el par criptográfico correspondiente a cada letra dentro de la matriz de 5×5 mostrada en la tabla, de manera que para cifrar una letra se considera el orden renglón-columna, es decir, cada letra se cifra con dos. Por ejemplo, la letra T corresponde DD, en tanto para la Y es el par ED.

En el siglo I a.C. surge el cifrado de César, el cual se considera que fue utilizado por el emperador Julio César. El cual consiste en desplazar el caracter a cifrar 3 posiciones adelante dentro de alfabeto a utilizar.

Otro ejemplo más actual es el algoritmo RSA, cuyas siglas son las iniciales de sus creadores (Rivest, Shamir y Adleman.)[4], su funcionamiento está basado en la factorización

las claves criptográficas que protegen las direcciones de dominio.
Con esta actualización, toda transacción o consulta que se realice en Internet invocando a los nombres de dominio (DNS), se haga con seguridad. http://www.unamglobal.unam.mx/?p=50043

[3] http://www.revista.unam.mx/vol.7/num7/art54/int54.htm

[4] El diseño del método del RSA fue en el año de 1977 y fue hasta 1997 que se dio a conocer

de números compuestos con grandes números primos y elegidos al azar (?, ?). Por lo que, encontrar una manera rápida y eficiente para descifrar un mensaje encriptado con este algoritmo implica cálculos abrumadores, los cuales involucran el uso de la computación. Actualmente, el *RSA* es considerado uno de los más confiables y utilizados en transacciones bancarias o en las firmas digitales.

Se le conoce como *Criptografía clásica* a los métodos de cifrados clave o llave secreta, la cual es la misma para cifrar o descifrar los cuales están divididos en tres categorías: **Transposición** (consiste en alterar el orden del alfabeto siguiendo un esquema, como escribir al revés el abecedario, es decir, la letra A corresponde a la Z, la B a la Y, así sucesivamente), **sustitución** (es un sistema que consta en el reemplazamiento de los símbolos en el alfabeto) y **producto** (es la composición de ambos cifrados). Estas técnicas de cifrado se enfocan principalmente en la encriptación de los símbolos de algún alfabeto y usualmente aplican técnicas simples para cifrar o descrifrar un texto. De modo que, la seguridad que proporciona estos métodos no son confiables. Actualmente, el uso de las tecnologías y el manejo del internet vino a revolucionar el concepto de seguridad de la información y al mismo tiempo motivó a la creación de nuevos criptosistemas.

Las nuevas técnicas de cifrado deben satisfacer ciertas características. En 1974 la *NBS* (National Bureau of Standards) estableció los estandares que debe cumplir un algoritmo de encriptación aceptable. Ellos los clasifican en cuatro grandes rubros. (?, ?)

1. El algoritmo deberá ser claro y no ambiguo.

2. Deberá proporcionar nivel adecuado de protección, el cual se medirá con respecto al tiempo o el número de operaciones para descubrir la clave (o llave) secreta de encriptación ante una amenaza.

3. Deberá tener métodos de seguridad basados solamente en la confidencialidad de las llaves.

4. No deberá actuar en contra de cualquier usuario o provedor.

Hoy en día, no es necesario estar involucrado en un conflicto político, militar o ser espías para estár en contacto con la Criptografía, la podemos encontrar en cosas como (?, ?)

- La contaseña de nuestro correo electrónico.
- En servidores en linea como los que usan los bancos.
- Todas nuestras tarjetas de crédito o telefónicas están encriptadas.

- Muchas de las aplicaciones que necesita nuestro celular están hace uso de la Criptografía, como la $GSM - Standard$[5] para cifrar llamadas telefónicas

Los ejemplos anteriores muestran la importancia de la Criptografía en la actualidad. Lo más importante e interesante es que en cada uno de estos se encuentran ocultas las matemáticas. De modo que, afirmo que estudiar la Criptografía a nivel superior podría fortalecer la comprensión de conceptos matemáticos como son los de: funciones, permutaciones, aritmética modular, algoritmos, programación, teoría de ecuaciones, algoritmos, modelos, entre otras ramas de las matemáticas.

3.2. Análisis de la enseñanza tradicional y sus consecuencias

La enseñanza tradicional básicamente está centrada en los contenidos y en el profesor. Este es el personaje principal para el éxito educativo, a él le corresponde organizar el conocimiento, vincular y elaborar lo que debe ser aprendido por los alumnos. La clase podría ser una simple colección de individuos donde el razonamiento matemático podría limitarse a procedimientos de memorización. Además, el alumno es el individuo que recibe los conocimientos, sigue las normas, en otras palabras la actividad del estudiante es pasiva.

Lo anterior no quiere decir que la educación tradicional es inadecuada; sin embargo, estas observaciones nos permite concluir algunas de las consecuencias en las competencias y actitudes de los estudiantes bajo este esquema.

1. El estudiante complementa su aprendizaje de los conceptos y resultados presentados por el profesor de una manera autodidacta. Comenzará a formular conjeturas y a buscar la resolución de problemas descando el énfasis de la búsqueda mecánica o memorística de las respuestas. Como consecuencia, el alumno puede desarrollar un pensamiento crítico y capacidades adecuadas de razonamiento matemático, aunque, posiblemente requiera un esfuerzo más arduo para él.

2. El estudiante busca comprender los conceptos y resultados propuestos por el profesor de una forma mecánica, el profesor asume que el ritmo de aprendizaje de ellos es el mismo y la adquisición del conocimiento está basado principalmente en que el alumno escuche; provocando un desinterés de aquellos que prefieren otros estilos de aprendizaje. (?, ?)

[5]GSM son las siglas para una red de comunicaciones Groupe Spécial Mobile o Sistema Global de comunicaciones móviles originaria de Europa.

Con base en lo anterior, suponemos que muchos problemas relacionados con la deficiencia que muestran los estudiantes en matemáticas están intimamente relacionados con la manera en que se presentan los contenidos, por lo que es necesario generar nuevos ambientes de aprendizaje, donde el estudiante esté motivado, tenga curiosidad, que fomente su creatividad y al mismo tiempo la investigación (?, ?). Actualmente exite una tendencia en el uso de las tecnologías, sin embargo esto tiene sus ventajas y desventajas; nosostros buscamos que estas sean parte de un diseño instruccional que brinde la oportunidad de romper los estándares del aprendizaje conductista.

En la educación superior observamos que docentes con un alto nivel de especialización en matemática pura, aplicada o educativa, se resisten con frecuencia al cambio, reproduciendo en su práctica profesional el sistema educativo donde ellos mismos fueron formados; un sistema caracterizado por el predominio de clases magistrales, asignación de listas de ejercicios y un comportamiento pasivo de los estudiantes. (?, ?). Nótese que nosotros no estamos en contra de esta metodología, sin embargo consideramos que es importante que existan otras formas de enseñanza para aquellos prefieran otro tipo de aprendizaje.

En el siguiente apartado mostraremos algunas definiciones relacionadas al proyecto de Criptografía (?, ?). La finalidad de esto es ilustrar que si la planeación y la forma de mostrar estos conceptos no es adecuada, los estudiantes podrían manifestar dificultades para compreder estos conceptos y como consecuencia tendrán dificultades para realizar argumentaciones o demostraciones matemáticas.

Sistemas Criptográficos

Entenderemos como **Sistema Criptográfico** o **Criptosistema** a un conjunto de reglas o técnicas que sirven para cifrar o descifrar un mensaje, el cual consiste en establecer una correspondencia entre dos conjuntos de palabras o símbolos. Esta relación deberá ser uno a uno.

Definición: 1

Un *criptosistema* es una quíntupla ($\mathcal{P}$,$\mathcal{C}$,$\mathcal{K}$,$\mathcal{E}$,$\mathcal{D}$), tal que satisface lo siguiente:

1. $\mathcal{P}$ es un conjunto finito de los posibles *textos en plano* (texto original).
2. $\mathcal{C}$ es un conjunto finito de los posibles *textos cifrados*.
3. $\mathcal{E}$, es un conjunto finito con las posibles *llaves secretas*. A este conjunto se le llamará el *espacio de llaves.*
4. Para cada $K \in \mathcal{K}$, existe una *regla de cifrado* $e_k \in \mathcal{E}$ y una *regla de descifrado* correspondiente $d_k \in \mathcal{D}$. Cada $e_k : \mathcal{P} \longrightarrow \mathcal{C}$ y $d_k : \mathcal{C} \longrightarrow \mathcal{P}$ son funciones tales que $d_k(e_k(x)) = x$ para cada texto en plano (o texto original) $x \in \mathcal{P}$.

La propiedad principal de la definición 1 es el número cuatro, ya que nos indica que si un texto plano (o texto original) es cifrado por la función e_k entonces para descifrarlo se utiliza la función d_k y viceversa. La figura 3.1 ilustra el canal de comunicación entre dos personas utilizando un sistema criptográfico al azar.

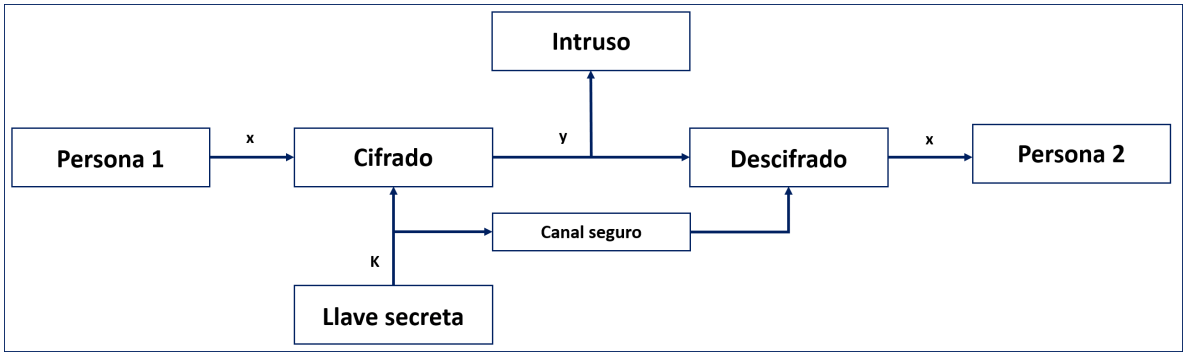


Figura 3.1: Canal de comunicación

Criptografía Clásica.

La Criptografía clásica, es aquella que se utilizó hasta mediados del siglo XX. También se le conoce como los métodos de encriptación no computarizada. De modo que, las técnicas para ocultar un mensaje podían darse manualmente o con utensilios simples pero al mismo tiempo ingeniosos. Generalmente la Criptografía clásica se divide en dos; los cifrados por transposición y por sustitución. Al mismo esta división tiene sus subdivisiones. Observemos la figura 3.2, donde muestra la clasificación de la Criptografía clásica.

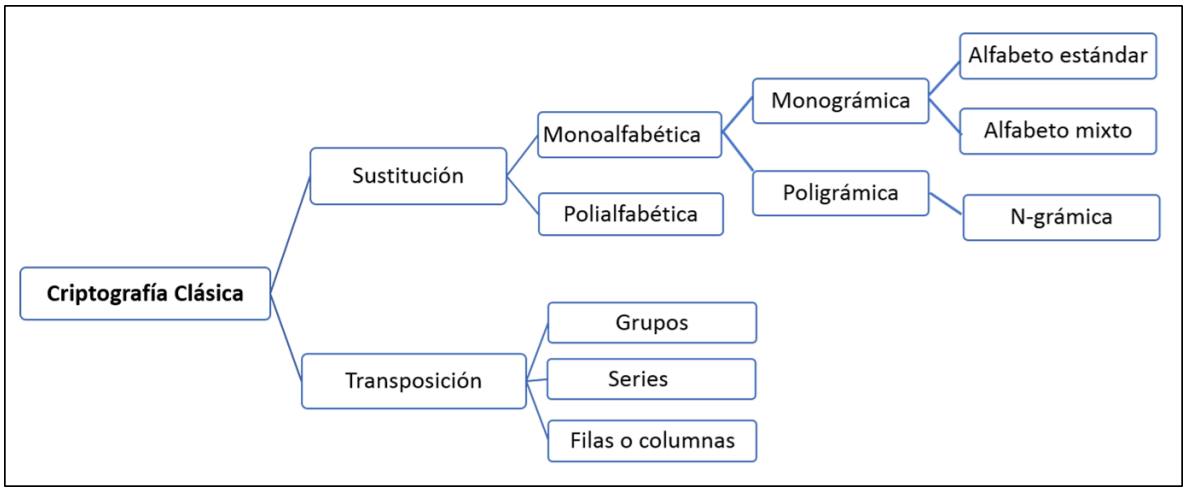


Figura 3.2: Canal de comunicación

Cifrado por transposición

Los cifrados por transposición, utilizan la técnica de permutación de los carácteres del texto en plano (o mensaje original). El primer caso reconocido dentro de esta clasificación es la *escítala*. Esta que se utilizó, durante la guerra de Atenas y Esparta a principios de 400 B.C.. El funcionamiento de este método consistía en enrollar en espiral una tira de cuero en un palo. En seguida se se escribía el mensaje en columnas paralelas al eje del bastón. Cuando es desenrrollada, el mensaje es irreconocible y sólo podrá ser leido con un cilidro, vara, bastón, etc. del mismo diámetro (?, ?).

Cifrado por sustitución

La técnica que utilizan los cifrados por sustitución consiste en que las letras de un texto en plano (u original) son remplazadas, sin cambiar la secuencia con una o más letras, figuras o símbolos. El ejemplo más común de estos sistemas es el *cifrado de César*. La siguiente definición describe este ejemplo en términos de la aritmética modular y

en concreto se definie bajo el anillo $\mathbb{Z}_{26}$, donde 26 representa el número de caracteres que tiene el alfabeto estándar o latín. Aunque la definición de este método puede ser definido bajo cualquier anillo $\mathbb{Z}_m$.

Definición: 2

Sean $\mathcal{P}, \mathcal{C}, \mathcal{K} = \mathbb{Z}_{26}$. Para $0 \leq K \leq 25$, definimos

$$e_k(x) = (x + K) \quad \text{mód } 26$$

y

$$d_k(y) = (y - K) \quad \text{mód } 26 \text{ con } x, y \in \mathbb{Z}_{26}$$

En particular si la llave es $K = 3$ el criptositema es llamando frecuentemente *Cifrado de César*, el cual fue usado por el emperador Julio César.

Cifrado decimado

El sistema criptográfico por producto o también conocido como cifrado con alfabeto decimado consiste en el símbolo que reemplaza al *i-ésimo* es obtenido multiplicando i por un algún número en lugar de sumar como el esquema anterior. La definición considera el alfabeto estándar, por lo que está en términos del anillo $\mathbb{Z}_{26}$.

Definición: 3

Sean $\mathcal{P}, \mathcal{C}, \mathcal{K} = \mathbb{Z}_{26}$. Para $m \in \mathcal{K}$ y $mcd(m, 26) = 1$, definimos

$$e_k(x) = m(x) \quad \text{mód } 26$$

y

$$d_k(y) = m^{-1}(y) \quad \text{mód } 26 \text{ con } x, y \in \mathbb{Z}_{26}$$

y m^{-1} el inverso multiplicativo de m módulo 26

Cifrado Afín

El cifrado Afín es un caso especial de los sistemas por sustitución; éste consiste en combinar los dos cifrados anteriores. En lugar de solo transladar con una suma o con un producto se realizan ambas operaciones. De modo que la difición es como sigue:

Definición: 4

Sean $\mathcal{P}, \mathcal{C} = \mathbb{Z}_{26}$ y sea

$$\mathcal{K} = \{(a, b) \in \mathbb{Z}_{26} \times \mathbb{Z}_{26} \mid mcd(a, 26) = 1\}$$

Para $(a, b) \in \mathcal{K}$, definimos

$$e_k(x) = (ax + K) \quad \text{mód } 26$$

y

$$d_k(y) = (a^{-1})(y - K) \quad \text{mód } 26 \text{ con } x, y \in \mathbb{Z}_{26}$$

y a^{-1} el inverso multiplicativo de a módulo 26

3.3. Análisis de las concepciones de los estudiantes, las dificultades y los obtáculos

La Criptografía al ser una disciplina que tiene una estrecha relación con las matemáticas y la computación, permite que pueda ser utilizada como parte de una enseñanza interactiva para estudiantes de carreras como matemáticas, ciencias de la computación y actuaria. Además ellos podrán relacionar la teoría detrás de la Criptografía con la necesidad de proteger la información.

La teoría y la práctica de la Criptografía es complicada y difícil de seguir para los estudiantes de nivel superior, debido a que relaciona con diversas áreas de las matemáticas (teoría de números, álgebra abstracta, probabilidad, algoritmos, etc, $\cdots$), además, los alumnos con menos conocimientos matemáticos podrían sentirse intimidados por los temas involucrados y manifestar dificultades en la comprención de esta disciplina (?, ?). Dentro de las dificultades que encontramos son las siguientes:

1. Esquema de encriptación utilizando funciones.

2. La aritmética modular.

3. Permutaciones.

4. Identificar las condiciones necesarias y suficientes para definir un sistema criptogáfico.

Por otro lado, consideramos que, las dificultades antes mencionadas podrían ser consecuencia de los siguientes conflictos: **1)**la comprensión de los enunciados de los teoremas o proposiciones, en particular en identificar las hipótesis y lo que se desea verificar y **2)** la construcción de demostraciones matemáticas .

Cabe mencionar que, como la Criptografía tiene una estrecha relación con las matemáticas y la computación, es natural pensar cómo deberían ser los argumentos o las demostraciones que realmente verifican los teoremas, proposiciones o los algoritmos. Clasificamos las dificultades alrededor de la noción de demostración en 4.

1. **La veracidad de un teorema**. Este aspecto está relacionado con la idea de que un teorema aparece como una consecuencia lógica y necesaria de las premisas con las que parte. Además el enunciado (teorema) es aceptado como una verdad universal en el sistema e intemporal.

2. **La estructura de la demostración**. En este caso, la dificultad está relacionada en la forma de justificar, tener la máxima garantía de que la demostración de un enunciado será una verdad absoluta y con ello es neceario un rigor en el uso del lenguaje formal.

3. **La verficación de resultados en otras áreas como la computación o la física**. Este aspecto está relacionado en la verificaciones que presentan cierta complejidad técnica, pero no tiene un carácter absoluto y universal. Su validez se incrementa a medida que se muestran o producen más hechos que se ajusten al enunciado y un ejemplo que no se cumpla no invalida completamente la afirmación. El concepto de demostración en este caso, está basada principalmente en prácticas argumentativas de tipo sustancial; es aquí donde se pone en juego los leguajes ordinarios, simbólicos y cualquier tipo de dispositivo. En el caso de las ciencias experimentales, los experimentos u observaciones se hacen con el máximo cuidado para controlar todos los posibles factores que influyean en el resultado (?, ?).

4. **La relación entre las demostraciones con un rigor matemático o en**

otra área con las argumentaciones en la vida cotidiana. En este caso las argumentaciones en la vida cotidiana son contextualizadas e incluso dependen de la situación emocional del sujeto. Nótese que este tipo de argumentaciones no da lugar necesariamente a las verdades, ya que pueden estar basadas en situaciones locales, careciencido de una visión objetiva. Este tipo de argumentos son utilizadas tanto en la vida cotidiana como en cuestiones académicas, una de las virtudes de esto es la continuidad cognitiva entre la fase de conjeturar y la construcción de demostraciones en matemáticas (?, ?).

3.4. Análisis del campo

A continuación mostraremos las características de los estudiantes que realizarán el proyecto de Criptografía; así como algunas de las restricciones posibles para el desarrollo.

Características de los estudiantes y del curso donde se llevará a cabo el proyecto de Criptografía.

- Los estudiantes que realizarán el proyecto de Criptografía se inscribirán en un curso del segundo semestre, Álgebra Superior II, asignatura del tronco común de las carreras de Matemáticas, Actuaría y Ciencias de la Computación.

- El número de inscritos en el curso de Álgebra Superior II es de 74 alumnos. De los cuales, 24 están en Matemáticas, 35 en Actuaría, 14 en Ciencias de la Computación y 1 en Física.

- El curso de Álgebra Superior II se llevará a cabo de forma regular, es decir, corresponde al semestre que señala el plan de estudios de la Facultad de Ciencias. Además, se aceptan estudiantes que la cursarán en la modalidad ordinaria y extraordinaria, De los 74 alumnos incritos tenemos de ambas modalidades 70 y 4 respectivamente.

- Los cursos en la Facutad de Ciencias están organizados de tal manera que hay un profesor titular y un ayudante. En nuestro caso, por el número de alumnos el curso consta de dos ayudantes.

Posibles restricciones para el desarrollo del proyecto de Criptografía de acuerdo a las características de los alumnos y del curso.

- Debido a que las materias del tronco común de las licenciaturas en Matemáticas, Actuaría y Ciencias de la Computación no están seriadas; los alumnos que se inscriban al curso de Álgebra Superior II, la cual correspone a una asignatura del segundo semestre en el plan de estudios de las tres carreras, no implica que los estudiantes pertenezcan a las mismas generaciones. Como consecuencia, el nivel académico, la experiencia como estudiantes de la Facultad de Ciencias y la madurez de pensamiento matemático no necesariamente será el mismo.

- Al ser un grupo con un gran número de estudiantes, la organización para la implementación del proyecto y al mismo tiempo en la formación de equipos será más compleja.

- Al tener una mayoria de alumnos inscritos en la carrera de Actuaría, existirán equipos de trabajo que sólo sean de esta misma licenciatura. Como consecuencia, la interacción con otras áreas podría verse limitada.

- Es fundamental una buena organización y comunicación entre el profesor titular y los dos ayudantes para que se realice el proyecto de Criptografía y al mismo el curso de Álgebra Superior II con éxito.

Capítulo 4

La concepción y el análisis a priori

4.1. Introducción

En este capítulo desarrollaremos el análisis *a priori* de nuestro trabajo, el cual corresponde a la segunda fase de la Ingeniería Didáctica. Primero, desarrollaremos las actividades que los estudiantes realizarán acerca del tema de Criptográfica, seguido de las posibles respuestas que esperamos por parte de los alumnos, así como las dificultades que podrían presentar al resolver las tareas propuestas. De modo que, el análisis *a priori* comprende dos partes: una descripptiva y otra predictiva.

Definitivamente, nuestro diseño está pensado para lograr los objetivos planteados en el capítulo uno, dicho esto, a continuación, describiremos cómo pretendemos lograrlos.

1. Para que los estudiantes mejoren las prácticas argumentativas en matemáticas e identifiquen los diversos contextos de la demostración, ellos resolverán problemas del tema de Criptografía. Debido a que nuestros alumnos de interés estarán cursando el segundo semestre de la licenciatura, el planteamiento de las preguntas comenzarán desde un enfoque básico hasta llegar a una profundización adecuada.

2. Para lograr un aprendizaje significativo, el diseño del proyecto, además de estar involucrado con el Álgebra, se relaciona con la Historia, la Probabilidad, la Programación y por último con algunas aplicaciones relevantes de la Criptografía hoy en día, como es la seguridad bancaria.

   Para fortalecer las interacciones entre los estudiantes y al mismo tiempo con el profesor, los alumnos del grupo de Álgebra se dividirán en equipos, el número de integrantes dependerá del número de inscritos, ya que este no está determinado

desde antes que comience el semestre escolar. Al tener los equipos, se establecerán espacios de comunicación entre ellos y el profesor para discutir las dudas o las dificultades que podrían tener al momento de resolver el proyecto.

Para que los estudiantes desarrollen habilidades para comunicar sus ideas, se fomentará la expresión oral en los espacios de comunicación antes mencionados, y ellos periódicamente entregarán avances del proyecto en forma escrita.

Para que los estudiantes a través de sus errores tomen decisiones pertinentes para mejorar su proyecto, es importante la retroalimentación constante del profesor acerca de sus avances. Además, al desarrollar este proyecto en conjunto a la clase de Álgebra Superior II, obligará a los alumnos organizarse mejor.

Para que los estudiantes se involucren en el proceso de titulación, ellos entregarán un trabajo por escrito al terminar las clases del semestre; durante las semanas de exámenes los equipos expondrán su trabajo, al finalizar la exposición se realizarán preguntas al equipo y a cada integrante.

4.2. Descripción de las actividades del proyecto de Criptografía

La estructura de las actividades del proyecto de Criptografía están ordenadas a partir de lo general hasta lo particular y están divididas en tres etapas.

1. **Breve historia de la Criptografía**. Se busca que a través de la historia los estudiantes logren un mejor entendimiento del desarrollo de la Criptografía como parte de una área de las matemáticas. Así mismo buscamos que a través de una investigación histórica en matemáticas, los alumnos observen que esta ciencia está inmersa en una cultura, que su desarrollo está influenciado por la época y las necesidades que se le presentan al hombre.

2. **Cifrados Clásicos**. Se busca que los estudiantes conozcan y comprendan tres métodos de encriptación: César, Decimado y Afín. Estos sistemas criptográficos son categorizados como de Sustitución Monoalfabética.

3. Una aplicación o tema a profundizar de Criptografía. Se busca que los estudiantes a través de sus investigaciones al desarrollar los sistemas criptográficos clásicos,

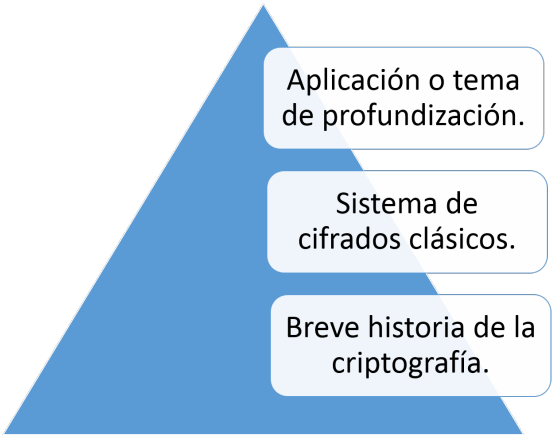


Figura 4.1: La estructura del proyecto es similar a la de un triángulo, la base ilustra las nociones generales de la Criptografía, hasta profundizar el conocimiento en esta rama de las matemáticas.

sus áreas de interés y su formación académica desarrollen una aplicación de la Criptografía de hoy en día o que ellos logren profundizar algún tema de Criptografía. Esta elección tomada por cada equipo, por lo que al finalizar el proyecto cada grupo tendrá uno distinto.

Para ayudar a entender mejor la estructura del proyecto, la siguiente tabla ilustra cada una de las secciones que tendrá, así como el número de actividades que comprende.

Secciones del proyecto	Subtemas	Número de actividades
Breve historia de la Criptografía	Orígenes de la Criptografía	Una actividad
Sistema de cifrados clásicos	Cifrado de César	Once actividades
	Cifrado Decimado	Cinco actividades
	Cifrado Afín	Cuatro actividades
Aplicación o tema de profundización por parte de cada equipo	Depende de la orientación que selecciones los equipos.	Depende de la orientación que selecciones los equipos.

4.3. Breve historia de la Criptografía

Según la Real Academia Española, la historia es una disciplina que estudia y narra cronológicamente los acontecimientos del pasado. Frecuentemente al referirnos a la historia de algo o de alguien, se confunde con conocer datos precisos acerca de lo que pasó y listarlos de forma ordenada. Sin embargo, esta disciplina busca más que eso, pretende comprender, entre algunos factores, los orígenes, desarrollo y consecuencias del pasado.

Para compredender los sucesos del pasado, es necesaria una investigación histórica adecuada, es decir, es indispensable consultar fuentes confiables, analizar los eventos desde una perspectiva crítica y considerar que la historia está relacionada con factores sociales, culturales, religiosos y económicos. (?, ?).

De modo que, si los estudiantes tienen un acercamiento a la historia de las matemáticas les proporcionará una visión del cómo han evolucionado hasta el día de hoy, ya que esta ciencia, al igual que la historia, está vinculada a diversos factores de la sociedad (?, ?).

Pretendemos que los estudiantes utilizen sus investigaciones históricas de la Criptografía para reconstruir parte ella. Debido que esta indagación depende de las fuentes que cada equipo consulte, la reconstrucción será diferente. A pesar de esto, esperamos que la información que encuentren la analicen con una perspectiva crítica.

4.3.1. Descripción de las actividades de los orígenes de la Criptografía

Actividad: 1.1

Investiga los orígenes de la Criptografía.

Esta actividad tiene como finalidad una indagación histórica de la Criptografía. Los estudiantes deberán encontrar los orígenes, el desarrollo y sus consecuencias. Además deberán encontrar la diferencia entre los términos criptoanálisis, criptografía y criptología.

Buscamos que los estudiantes realizen una investigación a conciencia, con esto nos referimos a que ellos deberán encontrar fuentes confiables, las cuales las clasificamos en tres:

1. Fuentes primarias; es decir, aquellas que proporcionan datos directos del pasado.

2. Fuentes secundarias, las cuales son los resultados de investigaciones que utilizaron fuentes primarias.

3. Fuentes terciarias o ene-arias, es decir, es la información basada principalmente de fuentes secundarias (?, ?).

Para lograr esta clasificación, los estudiantes tendrán que examinar con un espíritu crítico las fuentes que consulten; seleccionar las confiables y las útiles. Ellos podrán apoyarse en libros, artículos, internet, enciclopedias, entre otros.

4.4. Sistema criptográfico de César

En el siglo I a.C. el emperador César ideó una técnica para ocultar mensajes; el cual consistía en sustituir la letra A por la letra D, la B por la E, la C por la F y así sucesivamente con cada una de las letras del alfabeto. Actualmente éste método se le conoce como Cifrado de César.

El Cifrado de César es un sistema criptográfico categorizado como de Sustitución Monoalfabética. La simpleza de este método permitirá relacionar conceptos matemáticos con otras áreas como la computación. De modo que, se acopla a las condiciones de los estudiantes que realizarán este proyecto.

Las fortalezas que encontramos del Cifrado de César es que de forma gradual los estudiantes podrán fortalecer los conocimientos que adquieran durante el curso de Álgebra Superior II, conseguir relacionar el marco histórico de este método con la evolución de la matématica formal que está de por medio y lograr potencializar el pensamiento abstracto por medio prácticas que involucren validar o generalizar a otros contextos y problemas que tenga este sistema criptográfico.

El diseño de las actividades del Cifrado de César están organizadas de tal manera que el estudiante profundice gradualmente sobre este tema, sea conciente de las generalizaciones o de la abstracción matemática que existe y que es provocada por los diversos factores considerados para que un sistéma criptográfico esté bien definido, sea capaz de organizarse con sus compañeros y esté interesado (o motivado) al relacionar las actividades sus gustos literararios o conozca otros.

A continuación describiremos cada una de las actividades de esta sección y cada una de las posibles respuestas que esperamos obtener de los estudiantes.

4.4.1. Descripción de las actividades del sistema criptográfico de César

La actividad está motivada en la relación de la Historia con la enseñanza de las matemáticas. Los estudiantes de la Facultad de Ciencias deben tener la sensibilidad del hecho de que las matemáticas que estudian el día de hoy son el producto de una construcción cultural, surgieron de las necesidades de las personas, de la época, de los conocimiento previos e incluso de las preferencias de los individuos.

Actividad: 2.3

Investiga los orígenes de la Criptografía

Esperamos que los estudiantes investiguen y encuentren los orígenes del cifrado de César, la motivación que tuvo este emperador en "inventarlo". Además pretendemos que ellos tengan claridad del comportamiento de este cifrado de forma intuituva.

Actividad: 2.2

¿Cuál es el procedimiento para cifrar un texto utilizando el Cifrado de César?

A partir de la actividad anterior, suponemos que los estudiantes no tendrán dificultades del comportamiento del cifrado. Por consiguiente, esperamos que los equipo consideren cada una de las siguiente observaciones.

- Primero, ellos deberán considerar que el Cifrado de César supone la existencia de un alfabeto, mismo que se utilizará para cifrar o descifrar mensajes. Además tiene un orden establecido.

- Segundo, la correspondencia entre el alfabeto original y el cifrado es uno a uno.

- Tercero, para aplicar el mecanismo del cifrado de César es indispensable considerar un número $d \in \{0, 1, ..., n-1\}$ que será la clave secreta (o el desplazamiento). Nótese que el número n representa la cantidad de símbolos que tiene el alfabeto, en otras palabras, el tamaño que tiene el alfabeto.

Posiblemente los estudiantes realizen un diagrama o un ejemplo particular para describir el procedimiento del cifrado. Tomamos el siguiente como ejemplo, cuando el desplazamiento es igual a 3.

Posición de cada letra del alfabeto	**0**	**1**	**2**	**3**	**4**	**5**	**6**	**7**	**8**	**9**	**10**	**11**	**12**	**13**	**14**	**15**	**16**	**17**	**18**	**19**	**20**	**21**	**22**	**23**	**24**	**25**
Alfabeto Original	a	b	c	d	e	f	g	h	i	j	k	l	m	n	o	p	q	r	s	t	u	v	w	x	y	z
Posición de cada letra del alfabeto trasladada tres lugares	**3**	**4**	**5**	**6**	**7**	**8**	**9**	**10**	**11**	**12**	**13**	**14**	**15**	**16**	**17**	**18**	**19**	**20**	**21**	**22**	**23**	**24**	**25**	**0**	**1**	**2**
Alfabeto Cifrado	d	e	f	g	h	i	j	k	l	m	n	o	p	q	r	s	t	u	v	w	x	y	z	a	b	c

Figura 4.2: Cifrado de César con un desplazamiento igual a 3 con el alfabeto estándar.

Actividad: 2.3

Si el desplazamiento es $d = 3$, encuentra el mensaje original del siguiente mensaje:

FXDQGRGHVSHUWRHOGLQRVDXULRWRGDYLDHVWDEDDOOL

Esperamos que los estudiantes realicen la correspondencia entre el alfabeto estandar consigo mismo con un desplazamiento igual a 3. Ellos podrán apoyarse de tablas para representar la relación.

Consideraremos la tabla 4.2 dibujada en la actividad anterior, de tal forma que cada equipo encuentre la posición a cada letra del mensaje cifrado y encuentre el simbolo que le corresponde en el alfabeto original. Los alumnos podrán apoyarse de tablas o diagramas para realizar la actividad.

Para encontrar el texto original es necesario que los estudiantes resten la posición que ocupa una letra del texto cifrado el número 3 (número del desplazamiento para cifrar el texto), es decir:

Letra cifrada	**Posición**	Diferencia	**Letra original**
F	5	$5 - 3 = 2$	C

Repetimos el procedimiento con cada una de las letras del texto cifrado hasta obtener

el original.Para visualizar mejor este procedimiento, dividimos el texto oculto en tres partes. A continuación mostraremos las tablas con la correspondencia entre cada mensaje (oculto y original).

Posición de cada letra del texto cifrado	5	23	3	16	6	17	6	7	21	18	7	20	22	17	7	14
Texto cifrado	F	X	D	Q	G	R	G	H	V	S	H	U	W	R	H	O
Posición de cada letra del texto menos tres	3	20	0	13	16	14	3	4	18	15	4	17	19	14	4	11
Texto original	C	U	A	N	D	O	D	E	S	P	E	R	T	O	E	L

Figura 4.3: Primera parte del texto cifrado.

Posición de cada letra del texto cifrado	6	11	16	17	21	3	23	20	11	17
Texto cifrado	G	L	Q	R	V	D	X	U	L	R
Posición de cada letra del texto menos tres	3	8	13	14	18	0	20	20	8	14
Texto original	D	I	N	O	S	A	U	R	I	O

Figura 4.4: Segunda parte del texto cifrado.

Posición de cada letra del texto cifrado	22	17	6	3	24	11	3	7	21	22	3	4	3	4	14	14	11
Texto cifrado	W	R	G	D	Y	L	D	H	V	W	D	E	D	D	O	O	L
Posición de cada letra del texto menos tres	19	14	3	0	21	8	0	4	18	19	0	1	0	1	11	11	8
Texto original	T	O	D	A	V	I	A	E	S	T	A	B	A	A	L	L	I

Figura 4.5: Tercera parte del texto cifrado.

Utiliando las tablas anteriores e identificando cada palabra del mensaje cifrado, el mensaje que deben encontrar cada equipo es el siguiente:

CUANDODESPERTOELDINOSAURIOTODAVIAESTABAALLI

Para que el texto tenga sentido, los estudiantes deberán identificar cada palabra, añadir espacios entre cada una y los acentos ortográficos correspondientes. Como consecuencia encontrarán el siguiente cuento.[1]

Cuando despertó, el dinosaurio todavía estaba allí.

Por último, esperamos que los estudiantes observen que se perderá la ortografía de las palabras o mensajes que se desee cifrar con esta técnica, ya que es indistinto una letra acentuada a una que no lo está.

Actividad: 2.4

Da una función que defina el sistema criptográfico de César con un desplazamiento de 3.

Los estudiantes deben ser capaces de encontrar la función que defina el cifrado de César utilizando el tema de congruencias. Este tema corresponde al temario de Álgebra Superior II, el cual se estará desarrollando cuando los equipos realicen esta actividad.

Para que los equipos definan una función que describa el método de César, primero deberán determinar el dominio y el contradominio. Por lo cual, ellos tomarán un alfabeto fijo, es decir,

$$\text{Sea } \Lambda = \{a, b, c, d, e, f, g, h, i, j, k, l, m, n, o, p, q, r, s, t, u, v, r, s, w, x, y, z\}$$

el alfabeto estándar o básico

Claramente la cardinalidad del conjunto $\mid \Lambda \mid = 26$, de modo que el dominio y el contradominio será el siguiente conjunto.

$$\{0, 1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11, 12, 13, 14, 15, 16, 17, 18, 19, 20, 21, 22, 23, 24, 25\}$$

Por otro lado, esperamos a través del comportamiento de este cifrado observen que el dominio y contradomio es equivalente al conjunto $\mathbb{Z}_{26}$.

Los estudiantes deben ser capacer de realizar las siguientes observaciones.

- Recordar que los elementos del anillo finito, $\mathbb{Z}_{26}$ son clases de equivalencia.

[1] ***El dinosaurio*** es un minicuento escrito por el hondureño Augusto Monterroso en 1959.

- En este caso, el dominio de la función f es $\mathbb{Z}_{26}$; el cual representa al conjunto de las clases de equivalencia tales que contienen la posición de cada letra en el alfabeto estándar o básico original, es decir, no está cifrado. Por ejemplo, la posición de la letra a es el cero, entonces la clase de equivalencia asociada a la letra a es, $[0]$ en $\mathbb{Z}_{26}$.

- El contradominio de la función f también es el anillo $\mathbb{Z}_{26}$. La observación importante que deberá señalar los alumnos es que las clases de equivalencia son distintas a las del dominio, es decir, si el desplazamiento del cifrado es 3, entonces la clase de equivalencia asociada a la letra a es, $[3]$ en $\mathbb{Z}_{26}$, para el siguiente caracter, b la clase de equivalencia es $[4]$ en $\mathbb{Z}_{26}$ y así sucesivamente.

Con el dominio y contradominio definidos, los estudiantes definirán la función como sigue:

$$f : \mathbb{Z}_{26} \longrightarrow \mathbb{Z}_{26} \text{ dada por } f(n) = n + 3 \text{ módulo } 26$$

Esperamos que los estudiantes comprendan el significado y la interpretación de la función f. Para orientar e identificar los posibles conflictos para ellos listamos los conceptos significativos de esta definición.

- $f(n) = n + 3$ representa a la posición de la letra cifrada con un desplazamiento igual a tres.

- Debido a que el dominio y el contradominio es $\mathbb{Z}_{26}$, los alumnos deberán notar que el símbolo de la igualdad en la función f, es un abuso de notación para el mejor manejo de la teoría. Ellos deberan reflexionar acerca de lo siguiente:

  1. Si dos clases de equivalencia son iguales, entonces sus representantes son congruentes módulo 26, es decir, están relacionados.

  2. Los alumnos deberán notar que la función f definida por $f(n) = n+3$ módulo 26 para $n \in \mathbb{N}$ significa que nos estamos refiriendo a la igualdad de dos clases de equivalencia en $\mathbb{Z}_{26}$

Ejemplo 1. Tomamos la letra $a \in \Lambda$, entonces su posición es 0 y $0 \in \mathbb{Z}_{26}$.

Evaluamos 0 en la función f, entonces

$$f(0) = 0 + 3 \text{ módulo } 26$$

Esta igualdad implica que:

$$f(0) = 3 \text{ módulo } 26$$

Esto implica que la imágen del número 0 bajo la función f es 3, entonces la letra a al cifrarla con el método de César con un desplamiento igual a 3 corresponde al caracter d

Ejemplo 2. Tomamos la letra $n \in \Lambda$, entonces su posición es 13 y $13 \in \mathbb{Z}_{26}$.

Si evaluamos el número 13 en la función f obtenemos lo siguiente

$$f(13) = 13 + 3 \text{ módulo } 26$$
$$f(13) = 16 \text{ en } \mathbb{Z}_{26}$$

De esto último obtenemos que el cifrado de la letra n es q.

Ejemplo 3. El último ejemplo es el caso en el que la letra que se desea cifrar es la z. Sabemos que su posición en el alfabeto estandar o latino es el número 25. Entonces:

$$f(25) = 25 + 3 \text{ módulo } 26$$
$$f(25) = 28 \text{ en } \mathbb{Z}_{26}$$

Por lo tanto $f(26)$ es igual a 2 módulo 26

Por lo tanto el cifrado de la letra z es c.

Actividad: 2.5

Modifiquen la función f que definieron en el ejercicio anterior para cualquier desplazamiento d.

Esta actividad tiene por objetivo la generalización de la función f antes definida.

La respuesta inmediata esperada es la siguiente:

$$\begin{aligned} &\text{Para } d \in \mathbb{N} \text{ tenemos} \\ &f : \mathbb{Z}_{26} \longrightarrow \mathbb{Z}_{26} \quad \text{con} \\ &f(n) = n + d \text{ módulo } 26 \end{aligned}$$

Esperamos que los estudiantes observen que es suficiente tomar un desplazamiento que tome valores entre el 0 y el 25. De modo que la función f se modificaría de la siguiente forma.

$$\begin{aligned} &\text{Consideramos } d \in \{0, 1, \cdots, 25\} f : \mathbb{Z}_{26} \longrightarrow \mathbb{Z}_{26} \quad \text{con} \\ &f(n) = n + d \text{ módulo } 26 \end{aligned}$$

Esta afirmación, deberá ser demostrada por los estudiantes. Así que esperamos apliquen la siguiente definición para lograrlo.

Definición 1 *Dos funciones f y g son iguales si:*

- *f y g tienen el mismo dominio y rango.*
- *$f(x) = g(x)$ para todo elemento x del dominio.*

A partir de esta definición, esperamos que los estudiantes formulen el siguiente ***Teorema*** a modo de conjetura y lo demuestren.

(Conjetura por los estudiantes) 1 *Diremos que las funciones f y g definidas como:*

$$\begin{aligned} &\text{Para } d, d' \in \mathbb{Z} f : \mathbb{Z}_{26} \longrightarrow \mathbb{Z}_{26} \quad \text{con} \\ &f(n) = n + d \text{ módulo } 26. \end{aligned}$$

y

$$\begin{aligned} &g : \mathbb{Z}_{26} \longrightarrow \mathbb{Z}_{26} \quad \text{con} \\ &g(n) = n + d' \text{ módulo } 26 \end{aligned}$$

Entonces $d \equiv d'$ mód 26

Actividad: 2.6

1. ¿Cómo redefines la función f del sistema criptográfico de César si se toman en cuenta cualquier desplazamiento y cualquier alfabeto existente (finito)?
2. ¿Qué observaciones deberán considerar para cifrar un texto?
3. ¿Se puede usar la técnica de cifrado de César para encriptar cualquier conjunto de letras o símbolos?

La finalidad de esta actividad es que los estudiantes conozcan la diversidad de alfabetos existentes, al mismo tiempo que sean capaces de generalizar aún más la función f y de observar detalles del tipo:

- El sentido ortográfico se pierde en un texto cifrado, pues se utiliza exclusivamente los símbolos de un alfabeto.
- El conjunto de caracteres para cifrar un texto no es único.
- El conjunto de números que representan las posiciones de un alfabeto (finito) son comparables como anillos finitos $\mathbb{Z}_n$ con $n \in \mathbb{N}$.

Esperamos que los equipos investiguen los diferentes tipos de alfabetos existentes e incluso muestren algunos ejemplos como los siguientes:

Ejemplos de alfabetos

A B C D E F G H I J K L M N O P Q R S T U V W X Y Z

Ejemplo 1. Alfabeto básico o estándar (26 letras).

A B C D E F G H I J K L M N Ñ O P Q R S T U V W X Y Z

Ejemplo 2. Alfabeto latino o estándar (27 letras).

А Б В Г Д Е Ж З И Й К Л М Н О П Р С Т У Ф Х Ц Ч Ш Щ Ъ Ь Ю Я

Ejemplo 3. Alfabeto búlgaro (30 letras).

Con las observaciones antes mencionadas, esperamos que los equipos definan la función que describa el método de César como:

(Conjetura por los estudiantes) 2 *Sean* $\Lambda = \{$letras de un alfabeto $\}$ *con la cardinalidad del conjunto* $| \Lambda | = k$.

Definimos a la función $f : \mathbb{Z}_k \longrightarrow \mathbb{Z}_k$ *como* $f(n) = n + d$ módulo k

Cada equipo deberá argumentar (o demostrar) por qué la función f está bien definida.

Actividad: 2.7

La función f que definieron en el ejercicio anterior (2.6). ¿Es inyectiva o suprayectiva o biyectiva?

A través de cada una de las actividades, es evidente que la función f es biyectiva. Pretendemos que para los estudiantes sea clara esta afirmación y que la demuestren.

Deseo subrayar que, el tema de funciones se estudia desde el primer semestre en el curso de Álgebra Superior I y Cálculo Integral y Diferencial I (curso que también es del tronco común de los estudiantes de Matemáticas, Actuaría y Ciencias de la Computación.), pero es en la primera asignatura que se enfatiza en las funciones que satisfacen ser inyectivas, suprayectivas y biyectiva.

Hay que mencionar, además que el tema de funciones es un tema escencial en el estudio de las matemáticas para cualquiera de las licenciaturas de nuestro interés, por lo que es indispensable que los estudiantes fortalezcan este concepto y profundicen sus conocimientos previos.

De modo que, esperamos que cada equipo determine sin dificultad alguna, que la función f es biyectiva. Además que demuestren esta afirmación usando el siguiente teorema, el cual pertenece a un tema que corresponde al primer semestre:

Teorema 1 *Sea $f : A \longrightarrow B$. Entonces f es biyectiva si y sólo si existe $f^{-1} : B \longrightarrow A$ tal que $f^{-1} \circ f = Id_A$ y $f \circ f^{-1} = Id_B$, es decir, f es invertible.*

Considerando este teorema, esperamos que los equipos propongan la siguiente afimación, en otras palabras, pretendemos con este ejercicio que los estudiantes conjeturen.

(Conjetura por los estudiantes) 3 *Sean* $\Lambda = \{$ letras de un alfabeto $\}$
y $d \in \{0, 1, \cdots, k-1\}$ *donde k es la cardinalidad de Λ . Entonces*

$$f : \mathbb{Z}_k \longrightarrow \mathbb{Z}_k \text{ dada por } f(n) = n + d \text{ módulo } k \text{ es biyectiva.}$$

Prueba 1 *Sea* $\Lambda = \{$ letras de un alfabeto $\}$ *un conjunto tal que su cardinalidad es k.*

y sea $d \in \{0, 1, \cdots, k-1\}$

Para demostrar que la función

$$f : \mathbb{Z}_k \longrightarrow \mathbb{Z}_k \text{ dada por } f(n) = n + d \text{ módulo } k \text{ es biyectiva.}$$

Encontraremos $f^{-1} : \mathbb{Z}_k \longrightarrow \mathbb{Z}_k$ *tal que* $f^{-1} \circ f = Id_{\mathbb{Z}_k}$ *y* $f \circ f^{-1} = Id_{\mathbb{Z}_k}$.

Definimos $f^{-1} : \mathbb{Z}_k \longrightarrow \mathbb{Z}_k$ *como* $f^{-1}(n) = n - d$ módulo k.

Nótese que

$$Dom(f^{-1} \circ f) = Dom(Id_{\mathbb{Z}_k}) = \mathbb{Z}_k$$
$$Cod(f^{-1} \circ f) = Cod(Id_{\mathbb{Z}_k}) = \mathbb{Z}_k$$

De modo que, falta ver que $(f^{-1} \circ f)(n) = n$ *para todo* $n \in \mathbb{Z}_k$

$$Sea\ n \in \_k$$

$$\begin{aligned}(f^{-1} \circ f)(n) &= f^{-1}(f(n)) \\ &= f^{-1}(n + d) \\ &= (n + d) - d \text{ módulo } k \\ &= n \text{ módulo } k \\ &= n\end{aligned}$$

$$Esto\ implica\ que\ (f^{-1} \circ f)(n) = n\ para\ toda\ n \in \mathbb{Z}_k$$
$$Por\ lo\ tanto\ f^{-1} \circ f = Id_{\mathbb{Z}_k}$$

Análogamente se demuestra que $f \circ f^{-1} = Id_{\mathbb{Z}_k}$.

Por lo tanto f *es invertible y por tanto* f *es biyectiva.* ■

La virtud de realizar esta demostración es la definición de la función inversa f^{-1}, ya que describe la manera de descifrar cualquier mensaje encriptado por el método de César.

Actividad: 2.8

¿Cuál es la función que corresponde para descifrar el cifrado de César?

Si los equipos demostraron la actividad (2.7) como sugerimos en este trabajo, esperamos que la respuesta de esta actividad sea inmediata para los estudiantes.

La función que describe el descifrado de cualquier texto encriptado por el método de César con $d = \{0, 1, \cdots, k - 1\}$es:

$$f^{-1} : \mathbb{Z}_k \longrightarrow \mathbb{Z}_k \text{ dada por } f^{-1}(n) = n - d \text{ módulo } k \text{ con } d \in \{0, 1, \cdots, k - 1\}$$

Actividad: 2.9

Realiza un diagrama de flujo que describa el método de César con el alfabeto estándar y para un desplazamiento d igual a 3.

Los diagramas de flujo son una representación esquemática que ilustra la secuencia de las operaciones que se realizarán para conseguir la solución de un problema, en nuestro caso particular la problemática a resolver es cifrar un texto o descifrarlo con el método de César.

Consideramos que la noción de un diagrama de flujo permitirá a los estudiantes estructurar la secuencia lógica del comportamiento de este cifrado y como consecuencia esperamos que lo utilicen en las demostraciones, ya que una *demostración* se entiende, en términos generales, como una secuencia de enunciados organizados según reglas determinadas para establecer su validez.

A continuación mostraremos un diagrama de flujo como posible respuesta de los equipos, el cual está cifrando un texto con letras del alfabeto estándar y un desplazamiento igual a 3.

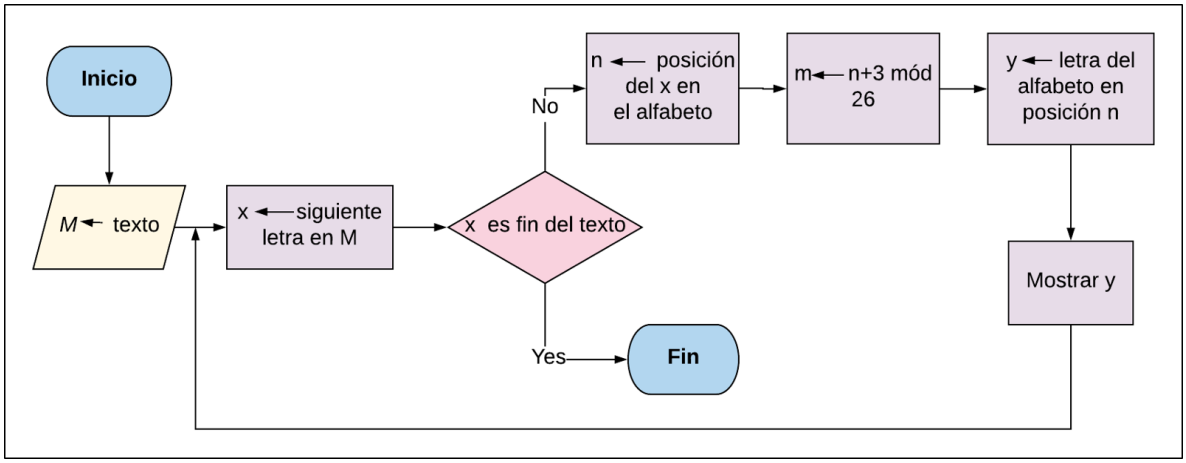


Figura 4.7: Diagrama de flujo con el alfabeto estándar y un desplazamiento igual a 3.

Actividad: 2.10

- Seleccionen un texto de su preferencia; este puede ser un fragmento de un cuento, de un poema, de una novela, etc. Encríptenlo con el desplazamiento que ustedes prefieran.
- Tendrán que escribir el texto original, el cifrado y la justificación

Esta actividad tiene dos finalidades:

1. Involucrar los gustos e intereses literarios de los estudiantes con una rama de las matemáticas.

2. Utilizar el Cifrado de César para ocultar el texto que seleccionen. Así mismo, que los alumnos sean creativos y flexibles al elegir el conjunto de caracteres que se desea cifrar y el desplazamiento.

Esperamos que los estudiantes realicen esta actividad sin problemas.

Actividad: 2.11

- Cada equipo tendrá que descifrar el texto que se les asigna.
- Cuando tengan su texto cifrado, comparte tu respuesta con los demás equipos. ¿Qué pasará si juntan sus mensajes desencriptados?
- Tendrán que escribir el texto original, el cifrado y la justificación.

Esta última actividad del cifrado de César pretendemos dos finalidades:

1. Fomentar el trabajo colaborativo entre los integrantes de cada equipo y con los demás.

2. Enfatizar en que el cifrado de César está bien definido gracias al trabajo matemático antes hecho (argumentaciones y demostraciones en relación a este método de encriptación).

Con base en lo anterior se dividirá un fragmento de un cuento llamado " El caos reptante"[2] (?, ?) entre el número de equipos que se formen al inicio del semestre.

Cada parte del relato estará cifrada con un desplazamiento distinto y será asignada de forma ordenada a cada equipo. Finalmente, cuando ellos obtengan el texto original, esperamos que compartan sus resultados son los demás para que al final obtengan el fragmento completo.

4.5. Cifrado con alfabeto decimado

Las actividades del cifrado de César, están organizadas de tal manera que el estudiante se familiarice con un método de encriptación por sustitución. Al mismo tiempo, que ellos logren potencializar el pensamiento abstracto a través de la generalización de los

[2]Relato de terror escrito por el escritor norteamericano H.P. Lovecraft (considerado como innovador del cuento de terror) en colaboración de Winifred V. Jackson en 1920. Se publicó por primera vez en la revista *The United Amateur* en abril de 1921. Nosotros tomamos una traducción publicada en 1997 (?, ?)

resultados y mantenerlos motivados por medio de sus gustos literarios.

De igual manera, pretendemos mantener esta dirección en el desarrollo de las actividades del segundo cifrado (cifrado con alfafeto decimado), es decir, que los estudiantes continuen conjeturando, analizando y abstrayendo el contenido matemático.

El cifrado con alfabeto decimado, consiste en reemplazar al $i-$ésimo símbolo del alfabeto original por el símbolo $j-$ésimo, el cual se obtiene de multiplicar la posición i por un número entero d. [3]

A continuación describiremos las actividades que corresponden al Cifrado con alfabeto decimado, así como las posibles respuestas que esperamos de los alumnos.

4.5.1. Descripción de las actividades basadas en el cifrado decimado

Actividad: 3.1

El cifrado con alfabeto decimado, consiste en reemplazar al $i-$ésimo símbolo del alfabeto original por el símbolo $j-$ésimo, el cual se obtiene de multiplicar la posición i por un número entero d'. Encuentra la función (congruencia) que defina este método.

Esperamos que los estudiantes comprendan el funcionamiento de esta técnica de cifrado sin problemas. Para su comprensión ellos deberán utilizar sus conocimientos previos y actuales de álgebra, tales como, el tema de funciones, de divisibilidad, de clases de equivalencia, de congruencias. También haber desarrollado todas las actividades del método de César les ayudará al mejor entendimiento de este sistema, así como el desarrollo de la siguiente sección.

La función que esperamos que encuentren es

$$f : \mathbb{Z}_k \longrightarrow \mathbb{Z}_k \text{ como } f(n) = d' \cdot n \text{ módulo } 26 \text{ con } d' \in \{0, 1, 2, \cdots, 25\}$$

Actividad: 3.2

Encuentra la relación entre alfabetos inducida por el cifrado decimado si el número que multiplica es igual a 4.

[3] Ver capítulo 3 para mejor comprensión.

Esperamos que los estudiantes encuentren la relación entre los alfabetos (original y cifrado) y cada equipo deberá determinar la congruencia que corresponde a cada letra utilizando la congruencia de la actividad 3.1. Observemos los siguientes ejemplos.

Ejemplos

1. Tomamos la primera letra del alfabeto, a. Como tiene la posición igual a cero, entonces.

   $$f(0) = 0 \cdot 4 \text{ módulo } 26 \text{ lo cual es equivalente a } f(0) = 0 \text{ módulo } 26$$

   Por lo tanto, la letra a del alfabeto original está cifrada bajo este método con ella misma.

2. Tomamos la letra, c. Como tiene la posición igual a dos, entonces.

   $$f(2) = 2 \cdot 4 \text{ módulo } 26 \text{ lo cual es igual a } f(2) = 8 \text{ módulo } 26$$

   Por lo tanto, la letra c del alfabeto original está cifrada bajo este método con la i.

3. Tomamos la primera letra del alfabeto, p. Como tiene la posición igual a quince, entonces.

   $$f(15) = 15 \cdot 4 \text{ módulo } 26 \text{ lo cual es igual a } f(2) = 8 \text{ en } \mathbb{Z}_{26}$$

   Por lo tanto, la letra p del alfabeto original está cifrada bajo este método también con la i.

Esperamos que al terminar los estudiantes encuentren la siguiente relación.

Posición del alfabeto original	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25
Alfabeto	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z
Posición resultante de multiplicar por 4	0	4	8	12	16	20	24	28	32	36	40	44	48	52	56	60	64	68	72	76	80	84	88	92	96	100
Posición del alfabeto cifrado	0	4	8	12	16	20	24	2	6	10	14	18	22	0	4	8	12	16	20	24	2	6	10	14	18	24
Alfabeto Cifrado	A	E	I	M	Q	U	Y	B	G	K	O	S	W	A	E	I	M	Q	U	Y	B	G	K	O	S	w

Figura 4.8: Alfabeto estándar cifrado con el método decimado igual a 4

Actividad: 3.3

¿La asociación determinada por el método de cifrado con alfabeto decimado "sirve" para cifrar mensajes?

A partir de sus observaciones con el Cifrado de César esperamos que los estudiantes tengan en mente que para que una técnica de encriptado "funcione", cada letra del alfabeto original le debe corresper una y solamente una letra en el alfabeto cifrado y viceversa. En otras palabras que la correspondencia sea biyectiva.

De modo que, esperamos que cada estudiante observe que la función no es biyectiva y sea capaz de argumentar.

(Conjetura por los estudiantes) 4 *La función definida*

$$f : \mathbb{Z}_{26} \longrightarrow \mathbb{Z}_{26} \text{ como } f(n) = 4n \text{ módulo 26, no es biyectiva.}$$

Para demostrar que la función f no es biyectiva es suficiente que cada equipo demuestren que no es inyectiva o suprayectiva. Realizaremos cada caso.

Prueba 2 *Es sufienciente mostrar que la función no es inyectiva, ya que existen*

$$3, 16 \in \mathbb{Z}_{26} \text{ tales que}$$

$$\begin{aligned} f(3) &= 3 \cdot 4 \quad \text{módulo 26} \\ &= 12 \quad \text{módulo 26, además} \\ f(16) &= 4 \cdot 16 \quad \text{módulo 26} \\ &= 64 \quad \text{módulo 26} \\ f(16) &= 12 \quad \text{en } \mathbb{Z}_{26} \end{aligned}$$

Lo cual implica que $f(3) = f(16)$ en $\mathbb{Z}_{26}$ con $3 \neq 16$ en $\mathbb{Z}_{26}$. Por lo tanto f no es inyectiva. ■

En la siguiente prueba veremos que la función f no es suprayectiva. Para esto, demostraremos que $Im(f)$ es un subconjunto propio de $\mathbb{Z}_{26}$

Prueba 3 *Sea $f : \mathbb{Z}_{26} \longrightarrow \mathbb{Z}_{26}$ la función dada por*

$$f(n) = 4n \text{ módulo 26}$$

Dada la tabla 4.8 obtenemos que

$$Im = \{0, 2, 4, 6, 8, 12, 14, 16, 18, 20, 22, 24\}$$

Claramente esto implica que Im es un subconjunto propio de $\mathbb{Z}_{26}$.

Por lo tanto, f no es una función suprayectiva. ■

Cada equipo puede dar como respuesta a esta actividad cualesquiera de estas dos o ambas.

Actividad: 3.4

¿Cuáles son las condiciones necesarias y suficientes para que la función f sea biyectiva si consideran cualquier alfabeto y cualquier factor multiplicación d'?

Esperamos que los estudiantes apliquen resultados de los temas de divisibilidad y de congruencias, los cuales estarán viendo en el curso de álgebra. Además, con ayuda de las sesiones de discusión, pretendemos que los equipos logren conjeturar lo siguiente:

(Conjetura por los estudiantes) 5 *Sea* $f : \mathbb{Z}_k \longrightarrow \mathbb{Z}_k$ *la función dada por*

$$f(n) = d' \cdot n \quad \text{mód } k \text{ con } d' \in \{0, 1, 2, \cdots, k-1\}$$

Entonces f *es biyectiva si y sólo si* $mcd(d', k) = 1$

Suponemos que los estudiantes lograrán plantear esta conjetura si ellos construyen ejemplos particulares. A continuación mostraremos algunos.

Posición resultante de multiplicar por 3	0	3	6	9	12	15	18	21	24	27	30	33	36	39	42	45	48	51	54	57	60	63	66	69	72	75
Posición resultante módulo 26	0	3	6	9	12	15	18	21	24	1	4	7	10	13	16	19	22	25	2	5	8	11	14	17	20	23
Alfabeto Cifrado	A	D	G	J	M	P	S	V	Y	B	E	H	K	N	Q	T	W	Z	C	F	I	L	O	R	U	X

Figura 4.9: Alfabeto cifrado con un factor de desplazamiento igual a 3

Observe que, si multiplicamos la posición de cada letra del alfabeto estándar con 3 la correspondencia es biyectiva. Es importante la discusión entre equipos y con el profesor para que se logre la observación que se busca.

Suponemos que al momento de realizar esta actividad, los estudiantes ya trabajaron con el concepto de primos y de primos relativos, así que por medio de sus clases de Álgebra y con ayuda de las sesiones con el profesor ellos logren deducir que la respuesta a la pregunta anterior que es por ser primos relativos.

Es importante que los estudiantes consideren el siguiente resultado en relación con los primos relativos.

Teorema 2 *Sean* $a, b, c \in \mathbb{Z}$ *tal que* $a \mid bc$. *Si* $mcd(a, b) = 1$ *entonces* $a \mid c$

Prueba 4 *Sean* $a, b, c \in \mathbb{Z}$ *tal que* $a \mid bc$. *Como* $mcd(a, b) = 1$, *entonces existe una combinación lineal igual a* 1 *de* a *y* b, *es decir,*

$$1 = as + bt \text{ con } s, t \in \mathbb{Z}$$

Si multiplicamos la igualdad anterior por c tenemos que,

$$c = (as + bt)c \text{ con } s, t \in \mathbb{Z} \cdots \textbf{(1)}$$

Distribuyendo, asociando y conmutando, obtenemos

$$c = a(cs) + (bc)t \text{ con } s, t \in \mathbb{Z} \cdots \textbf{(2)}$$

Como a|bc,entonces existe $q \in \mathbb{Z}$ tal que $bc = aq$. Así que al sustituir esto último en (2) *tenemos que*

$$c = a(cs) + a(qt) \text{ con } s, t, q \in \mathbb{Z}$$

Esta igualdad nos dice que c es un múltiplo de a, es decir

$$c = a(cs + qt) \text{ con } (cs + qt) \in \mathbb{Z}$$

Por lo tanto, a|c . ■

Con el teorema anterior, esperamos que los estudiantes logren demostrar el siguiente resultado.

(Conjetura por los estudiantes) 6 *Sea $f : \mathbb{Z}_k \longrightarrow \mathbb{Z}_k$ la función dada por*

$$f(n) = d' \cdot n \text{ módulo k y con } d' \in \{0, 1, 2, \cdots, k-1\}$$

Entonces f es biyectiva si y sólo si $mcd(d', k) = 1$

Prueba 5 *Sea $f : \mathbb{Z}_k \longrightarrow \mathbb{Z}_k$ la función dada por*

$$f(n) = d' \cdot n \quad \text{mód } k \text{ con } k \in \{0, 1, 2, \cdots, k-1\}$$

Suponemos que $mcd(d', k) = 1$. Queremos demostrar que la función f es biyectiva.

Para demostrar que la función f es biyectiva, es suficiente demostrar que la función es inyectiva, ya que el dominio y el contradominio de la función f son conjuntos finitos de la misma cardinalidad.

Sean $n_1, n_2 \in \mathbb{Z}_k$, tales que $f(n_1) = f(n_2)$ en $\mathbb{Z}_k$. Por definción de f se tiene que

$$(d' \cdot n_1) = (d' \cdot n_2) \text{ en } \mathbb{Z}_k$$

lo cual implica que

$$d' \cdot n_1 \equiv d' \cdot n_2 \mod k$$

por definción de congruencias tenemos

$$k|(n_1 - n_2)d'$$

Como $mcd(d', k) = 1$ *y por el teorema 3, se tiene que*

$$k|n_1 - n_2$$

entonces

$$n_1 - n_2 \equiv k \mod k$$

$$\text{Como} k \equiv 0 \mod k, \text{ tenemos que}$$

$$n_1 - n_2 \equiv 0 \mod k$$

Por lo tanto

$$n_1 \equiv n_2 \mod k$$

o dicho de otra manera $n_1 = n_2$ *módulo* k

Entonces f *es una función inyectiva y por tanto* f *biyectiva.*

Falta ver que si f *es biyectiva entonces* $mcd(d', k) = 1$.

Sea $f : \mathbb{Z}_k \longrightarrow \mathbb{Z}_k$ *la función biyectiva dada por*

$$f(n) = d' \cdot n \mod k \text{ con } d' \in \{0, 1, 2, \cdots, k-1\}$$

Suponemos que $mcd(d', k) \neq 1$. *Entonces existe* $1 < m$ *tal que* $mcd(d', k) = m$. *Entonces* $\frac{d'}{m}, \frac{k}{m} \in \mathbb{Z} - \{0\}$.

Si evaluamos $\frac{k}{m}$ *en la función* f *tenemos,*

$$\begin{aligned} f\left(\frac{k}{m}\right) &= \left(\frac{k}{m}\right) d' \text{ en } \mathbb{Z}_k \\ &= \left(\frac{d'}{m}\right) k \text{ entonces} \\ &= 0 \end{aligned}$$

pues cualquier múltiplo de k es igual a 0 en $\mathbb{Z}_k$

Por lo que, $f\left(\frac{k}{m}\right) = f(0)$ *módulo* k *con* $\frac{k}{m} \neq 0$ *módulo* k*. Como consecuencia obtenemos que* f *no es inyectiva, lo cual contradice el hecho de ser biyectiva por hipótesis. Por lo tanto* $mcd(d', k) = 1$*.*

De donde la conjetura queda demostrada. ■

Actividad: 3.5

Seleccionen un texto literario de su preferencia. Encríptelos utilizando el método del alfabeto decimado, de tal manera que la correspondencia sea biunívoca.

Buscamos que los estudiantes construyan sus propios ejemplos utilizando la actividad anterior. A continuación daremos un ejemplo que ellos podrían dar.

Como el $mcd(3, 26) = 1$, entonces la función definida por

$$f : \mathbb{Z}_{26} \longrightarrow \mathbb{Z}_{26} \text{ con } f(n) = 3n \text{ módulo26 es biyectiva}$$

. La siguiente tabla muestra la correspondencia entre los alfabetos (original y cifrado.)

Posición resultante de multiplicar por 3	**0**	**3**	**6**	**9**	**12**	**15**	**18**	**21**	**24**	**27**	**30**	**33**	**36**	**39**	**42**	**45**	**48**	**51**	**54**	**57**	**60**	**63**	**66**	**69**	**72**	**75**
Posición resultante módulo 26	**0**	**3**	**6**	**9**	**12**	**15**	**18**	**21**	**24**	**1**	**4**	**7**	**10**	**13**	**16**	**19**	**22**	**25**	**2**	**5**	**8**	**11**	**14**	**17**	**20**	**23**
Alfabeto Cifrado	A	D	G	J	M	P	S	V	Y	B	E	H	K	N	Q	T	W	Z	C	F	I	L	O	R	U	X

Figura 4.10: Alfabeto cifrado con un factor producto igual a 3.

Actividad: 3.6

Encuentren la función inversa de $f : \mathbb{Z}_k \longrightarrow \mathbb{Z}_k$ dada por

$$f(n) = n \cdot d \text{ módulo } k \text{ con } d \in \{0, 1, 2, \cdots, k-1\}$$

En este punto, nos gustaría que los estudiantes apliquen los resultados vistos en el curso de Álgebra con los correspondientes a este proyecto. Para resolver esta actividad, ellos deberán encontrar los inversos multiplicativos (si es que los hay) en $\mathbb{Z}_k$.

Esperamos que los equipos consideren el siguiente teorema para encontrar la función inversa de f.

Teorema 3 *Sea $d' \in \mathbb{Z}_k$. Entonces d' tiene inverso multiplicativo si y sólo si*

$$mcd(d', k) = 1$$

Prueba 6 *Sea $d' \in \mathbb{Z}_k$.*

Suponemos que d' tiene inverso mutiplicativo en $\mathbb{Z}_k$, entonces existe $\bar{d} \in \mathbb{Z}_k$ tal que $d' \cdot \bar{d} = \bar{d} \cdot d' \equiv 1 \mod k$, así

$$k \mid (d' \cdot \bar{d} - 1)$$

de modo que, existe $q \in \mathbb{Z}$ tal que

$$(d' \cdot d' - 1) = kq \text{ con } q \in \mathbb{Z}$$

entonces

$$1 = d' \cdot \bar{d} + k(-q)$$

La última igualdad implica que existe una combinación lineal de d' y k igual a uno. Por lo tanto $mcd(d', k) = 1$

Falta ver que si $mcd(d', k) = 1$, entonces d' tiene inverso mutiplicativo en $\mathbb{Z}_k$

Suponemos que $mcd(d', k) = 1$, entonces existe una combinación lineal de d' y k igual a uno, es decir,

$$1 = d's + kt \text{ con } s, t \in \mathbb{Z}$$

Esto implica que,

$$1 - d's = kt \text{ con } s, t \in \mathbb{Z}$$

Esta implica que $1 - d's$ es un múltiplo de k lo que es lo mismo que,

$$k \mid (1 - d's) \text{ entonces } 1 \equiv ds \mod k$$

La congruencia implica que d' tiene como inverso multiplicativo a s en $\mathbb{Z}_k$

Con esto último se ha demostrado el teorema. ■

Con el teorema anterior, esperamos que los estudiantes definan la función inversa del cifrado con alfabeto decimado para cualquier primo relativo como factor producto y cualquier conjunto de símbolos para cifrar como:

(Conjetura por los estudiantes) 7 *Si $f : \mathbb{Z}_k \longrightarrow \mathbb{Z}_k$ definida como $f(n) = d' \cdot n$ en $\mathbb{Z}_k$ con $d' \in \{0, 1, \cdots, k-1\}$ y $mcd(d', k) = 1$ la función que describe el cifrado decimado. Entonces la función inversa de f es*

$$f^{-1} : \mathbb{Z}_k \longrightarrow \mathbb{Z}_k \text{ dada por } f^{-1}(n) = n \cdot \bar{d}$$

con $\bar{d}$ el inverso multiplicativo de d' en $\mathbb{Z}_k$

Prueba 7 *Queremos demostrar que* $f^{-1} \circ f = f \circ f^{-1} = Id_{\mathbb{Z}_k}$

Sea $n \in \mathbb{Z}_k$, *entonces*

$$\begin{aligned}(f^{-1} \circ f)(n) &= f^{-1}(f(n)) \\ &= f^{-1}(d' \cdot n) \\ &= (n \cdot d')\bar{d} \text{ módulo } k \\ &= n(d' \cdot \bar{d}) \text{ módulo } k, \\ &= n \cdot 1 \text{ módulo } k \\ &= n \text{ módulo } k\end{aligned}$$

Por lo tanto $f^{-1} \circ f = Id_{\mathbb{Z}_k}$ *Análogamete se demuestra que* $f \circ f^{-1} = Id_{\mathbb{Z}_k}$ ■

Nótese que la segunda parte de esta demostración, los argumentos fueron totalmente similares a la primera. En estos casos, podemos escribir frases como análogamente o se demuestra de la misma manera. Esperamos que los estudiantes sean capaces de identificar estas situaciones y las utilicen cuando hagan una demostración.

4.6. Sistema Criptográfico Afín.

El último cifrado a desarrollar es el afín, este método es la generalización de los anteriores. Es decir, en lugar de sólo multiplicar o sumar para realizar la correspondencia de cada letra hacemos ambas cosas.

4.6.1. Descripción de las actividades del cifrado afín

Actividad: 4.1

Considera el alfabeto estándar como el conjunto de letras a cifrar. Encuentra la "regla"que se utilizó para encriptar el siguiente texto.

Texto original	**C**	**U**	**E**	**N**	**T**	**O**	**D**	**E**	**H**	**A**	**D**	**A**	**S**
Texto cifrado	O	Q	X	F	N	C	R	X	D	I	R	I	K

Figura 4.11: Texto original y cifrado utilizando el cifrado afín.

Pretendemos que los estudiantes generalicen los dos métodos de cifrado anteriores, y obtengan la imagen de cada letra del recuadro, es decir, multipliquen como el cifrado decimado y que sumen como el cifrado de César en ese orden de razonamiento.

Primero los estudiantes deben encontrar la posición de cada letra del texto original y del cifrado, así como se ve en la siguiente tabla 4.12.

Posición original	2	20	4	13	19	14	3	4	7	0	3	0	18
Posición del cifrado	14	16	23	5	13	2	17	23	3	8	17	8	10

Figura 4.12: Posiciones del texto original y del cifrado utilizando el cifrado afín.

A partir de las posiciones de las letras, los alumnos deberán notar que la correspondencia de cada letra del alfabeto original al cifrado está determinado por cada una de las siguiente igualdades.

$$\begin{aligned} f(2) &= d'(2) + d \text{ módulo } 26 \\ &= 14 \text{ en } \mathbb{Z}_{26} \\ f(20) &= d'(20) + d \text{ módulo } 26 \\ &= 16 \text{ en } \mathbb{Z}_{26} \\ f(4) &= d'(4) + d \text{ módulo } 26 \\ &= 23 \text{ en } \mathbb{Z}_{26} \\ f(13) &= d'(13) + d \text{ módulo } 26 \\ &= 5 \text{ en } \mathbb{Z}_{26} \\ f(19) &= d'(19) + d \text{ módulo } 26 \\ &= 13 \text{ en } \mathbb{Z}_{26} \\ f(14) &= d'(14) + d \text{ módulo } 26 \\ &= 2 \text{ en } \mathbb{Z}_{26} \\ f(3) &= d'(3) + d \text{ módulo } 26 \\ &= 17 \text{ en } \mathbb{Z}_{26} \\ f(4) &= d'(4) + d \text{ módulo } 26 \\ &= 23 \text{ en } \mathbb{Z}_{26} \end{aligned}$$

$$\begin{aligned} f(7) &= d'(7) + d \text{ módulo } 26 \\ &= 3 \text{ en } \mathbb{Z}_{26} \\ f(0) &= d'(0) + d \text{ módulo } 26 \\ &= 8 \text{ en } \mathbb{Z}_{26} \\ f(3) &= d'(3) + d \text{ módulo } 26 \\ &= 17 \text{ en } \mathbb{Z}_{26} \\ f(18) &= d'(18) + d \text{ módulo } 26 \\ &= 10 \text{ en } \mathbb{Z}_{26} \end{aligned}$$

Además, esperamos que los estudiantes seleccionen las congruencias que sean de ayuda para encontrar los valores de n y de k; tales como:

$$\begin{aligned} f(0) &= d'(0) + d \text{ módulo } 26 \\ f(0) &= 8 \text{ en } \mathbb{Z}_{26} \\ f(2) &= d'(2) + d \text{ módulo } 26 \\ f(2) &= 14 \text{ en } \mathbb{Z}_{26} \end{aligned}$$

De la primera igualdad tenemos que, $d'(0) + d$ módulo 26 es igual a 8 en $\mathbb{Z}_{26}$, lo cual implica

$$8 = d \text{ módulo} 26$$

Por lo tanto, $d = 8 + 26q$ para algún $q \in \mathbb{Z}$

Sin pérdida de generalidad, suponemos que $d = 8$, entonces al sustituir en la segunda congruencia seleccionada, se tiene que

$$\begin{aligned} 2d' + 8 &= 14 \text{ módulo} 26 \text{ entonces} \\ 2d' &= 6 \text{ en } \mathbb{Z}_{26} \end{aligned}$$

Como $mcd(2, 26) = 2$, entonces

$$\begin{aligned} \frac{2d'}{2} &= \frac{6}{2} \text{ módulo} 26 \\ d' &= 3 \text{ en } \mathbb{Z}_{26} \end{aligned}$$

Por lo tanto $d' = 3 + 26q'$ módulo 26 y con $q' \in \mathbb{Z}$

Por último, suponer sin pérdida de generalidad los alumnos pueden tomar a $d' = 3$ y $d = 8$.

Actividad: 4.2

- ¿Cuál es la función que describe el cifrado afín?
- La función que definieron. ¿Es biyectiva?

Esperamos que los alumnos, definan la función para este cifrado como:

$$f : \mathbb{Z}_{26} \longrightarrow \mathbb{Z}_{26} \text{ dada por } f(n) = 3 \cdot n + 8 \quad \text{mód } 26$$

Además, que ellos noten que al ser un cifrado que combina los primeros dos cifrados y tener el factor producto la condición para que la función sea biyectiva es la misma que en el sistema criptográfico decimal, es decir, $mcd(3, 26) = 1$.

Después de que los equipos encuentren la función que define al cifrado del ejemplo, esperamos que ellos demuestren que es biyectiva.

(Conjetura por los estudiantes) 8 *La función*

$$f : \mathbb{Z}_{26} \longrightarrow \mathbb{Z}_{26} \text{ dada por } f(n) = 3 \cdot n + 8 \text{ módulo 26 es biyectiva}$$

Prueba 8 *Para demostrar que* $f : \mathbb{Z}_{26} \longrightarrow \mathbb{Z}_{26}$ dada por $f(n) = 3 \cdot n + 8$ módulo 26 *es biyectiva es suficiente demostrar que* f *es inyectiva.*

Sean $n_1, n_2 \in \mathbb{Z}_{26}$ *tal que* $f(n_1) = f(n_2)$*, entonces*

$$\begin{aligned} 3 \cdot n_1 + 8 &= 3 \cdot n_2 + 8 \text{ módulo 26, entonces} \\ 3 \cdot n_1 &= 3 \cdot n_2 \text{ módulo 26} \end{aligned}$$

Como $mcd(3, 26) = 1$*, entonces* $3 \in \mathbb{Z}_{26}$ *tiene inverso multiplicativo, así que*

$$\begin{aligned} 3^{-1}(3 \cdot n_1) &= 3^{-1}(3 \cdot n_2) \text{ módulo 26, entonces} \\ n_1 &= n_2 \text{ módulo 26} \end{aligned}$$

Por lo tanto , $n_1 = n_2$ *en* $\mathbb{Z}_{26}$

Por lo tanto, la función f *es inyectiva.* ■

Actividad: 4.3

- Generaliza la función anterior para cualquier conjunto de letras, de desplazamiento y de factor producto.
- ¿Cuáles son los condiciones necesarias y suficientes para el cifrado afín sea una función biyectiva?

La conjetura esperada por parte de los estudiantes es:

(Conjetura por los estudiantes) 9 *Sea* $\Lambda = \{$las letras de un alfabeto$\}$*, tal que la cardinalidad de* Λ *es* k*. Sean* $n, m \in \mathbb{Z}_k$ *, entonces la función que determina al cifrado afín está dada por:*

$$f : \mathbb{Z}_k \longrightarrow \mathbb{Z}_k \text{ dada por } f(n) = d' \cdot n + d \quad \text{mód } k \text{ con } d, d' \in \{0, 1, \cdots k-1\}$$

Además f *es biyectiva si y sólo si* $mcd(d', k) = 1$

Prueba 9 *Para demostrar que la función definida como*

$$f : \mathbb{Z}_k \longrightarrow \mathbb{Z}_k \text{ dada por } f(n) = d' \cdot n + d \text{ módulo } k$$

. es biyectiva es suficiente demostrar que la función f *es inyectiva.*

Sean $n_1, n_2 \in \mathbb{Z}_k$*, tales que* $f(n_1) = f(n_2)$ *módulo* k*. Entonces*

$$\begin{aligned} d' \cdot n_1 + d &= d' \cdot n_2 + d \text{ módulo } k \\ d' \cdot n_1 &= d' \cdot n_2 \text{ módulo } k \text{ como } mcd(d', k) = 1, \text{ entonces existe } \bar{d} \\ \text{tal que } \bar{d} \cdot d' &= 1 \text{en } \mathbb{Z}_k \\ \bar{d}(d' \cdot n_1) &= \bar{d}(d' \cdot n_2) \text{ módulo } k \\ (\bar{d} \cdot d')n_1) &= (\bar{d}d')n_2) \text{ módulo } k \\ n_1 &= n_2 \text{ en } \mathbb{Z}_{26} \end{aligned}$$

Por lo tanto f *es una función inyectiva.* ■

Los estudiantes pueden dar una prueba alterna a la anterior, la cual consiste en exhibir la función inversa de la función f.

Prueba 10 *Para demostrar que la función definida como*

$$f : \mathbb{Z}_k \longrightarrow \mathbb{Z}_k \text{ dada por } f(n) = d' \cdot n + d \text{ módulo } k$$

. es biyectiva es suficiente demostrar que existe

$$f^{-1} : \mathbb{Z}_k \longrightarrow \mathbb{Z}_k \text{ tal que } f^{-1} \circ f = f \circ f^{-1} = Id_{\mathbb{Z}_k}$$

.

Como $mcd(d', k) = 1$ *entonces existe* $\bar{d} \in \mathbb{Z}_k$ *tal que* $\bar{d} \cdot d' \equiv 1$ módulo k

Definimos a $f^{-1}(n) = \bar{d}'(n - d)$ *módulo* k

Entonces

$$\begin{aligned}(f \circ f^{-1})(n) &= f(\bar{d}(n-d)) \\ &= d'(\bar{d}(n-d)) + d \text{ módulo } k \\ &= (d' \cdot \bar{d})(n-d) + d \text{ módulo } k \text{ entonces} \\ (n-d) + d &= n \text{ módulo } k, \text{ esto implica que} \\ (f \circ f^{-1})(n) &= n \text{ en } \mathbb{Z}_k\end{aligned}$$

Por lo tanto, $f^{-1} \circ f = Id_{\mathbb{Z}_k}$. *Análogamente se obtiene que* $f \circ f^{-1} = Id_{\mathbb{Z}_k}$.

Por lo tanto la función f *es biyectiva.* ■

Con esta demostración se busca que los estudiantes resuelvan la siguiente actividad sin ninguna dificultad.

Actividad: 4.4

- ¿Cuál es la función que descifra un mensaje encriptado con el método afín?

Si los estudiantes realizaron la prueba de que la función que describe el sistema criptográfico afín es invertible si y sólo si es biyectiva, entonces la respuesta esperada es la descrita en el ejercicio anterior.

4.7. Aplicación o tema a profundizar de Criptografía

Esta última sección está motivada por el aprendizaje autorregulado, este consiste en que el o los estudiantes escojan sus metas, y en nuestro caso buscamos que los equipos seleccionen una aplicación a desarrollar o que ellos profundicen en un tema de Criptografía.

La selección de los equipos dependerá de los intereses de cada uno, es decir, al ser estudiantes de diferentes carreras; Matemáticas, Actuaría y Ciencias de la Computación, ellos podrán darle al proyecto una dirección de una fundamentación en matemáticas al desarrollar algún otro cifrado clásico, o investigar y comprender cifrados relacionados

con las finanzas, o buscar la relación de los cifrados clásico u otros con los algoritmos, es decir, con la computación.

Es crucial la comunicación entre los estudiantes de cada equipo con el profesor, por lo que, a lo largo del proyecto se buscará crear un entorno en el que los alumnos se sientan seguros, que les permita orientar su trabajo y consecuentemente obtengan resultados satisfactorios.

4.7.1. Descripción de las actividades de aplicación

Actividad: 4.4

- A partir de los intereses del equipo y su formación como estudiantes de las diferentes carreras, escojan una aplicación o un tema de la Criptografía distinto a los cifrados clásicos que se trabajaron anteriormente y desarrollen.
- Cada equipo deberá determinar el objetivo de esta sección, es decir, decidir si la dirección que le darán a su trabajo de Criptografía será con un enfoque desde la fundamentación matemática, o con un enfoque práctico, como la relación de la Criptografía en la seguridad financiera o en el mundo cibernético.

Con una buena comunicación, esperamos que cada equipo analice las características de la orientación que desean darle al trabajo, analicen el valor que tiene el proyecto para sí mismos, establezcan objetivos, determinen el nivel de perfección de lo que desarrollarán y planifiquen estrategias de trabajo colaborativo.

Suponemos que si los equipos logran realizar cada uno de los procesos antes descritos, ellos se encontrarán motivados, visualizarán la relevancia de los conocimientos que están adquiriendo al realizar el proyecto para sus futuros estudios, relacionarán la utilidad de la matemática con las necesidades sociales y por último, fortalecerán el trabajo colaborativo.

4.8. Distribución temporal de las actividades

Las actividades del proyecto estarán distribuidas a lo largo del semestre escolar, el cual consideramos 15 semanas. Por lo que, la implementación del proyecto estará limitado por este tiempo.

Dentro de este periodo, cada 15 días los estudiantes tendrán espacios dentro y fuera del aula, para 1) tener sesiones grupales para expresar sus avances y dudas del proyecto o de temas relacionados y 2) sesiones de cada equipo con el profesor para realizar las retroalimentaciones pertinentes. Las sesiones se distribuirán de la siguiente manera.

Sesiones	Temas
Sesión 1 (1 hora)	Avances históricos de la criptografía: La sesión será presencial, gran grupo. Interacción magistral, dialógica.
Sesión 2 (1-2 horas)	Actividades del 1-4 del cifrado de César: La sesión será presencial, gran grupo. Interacción magistral, dialógica y trabajo colaborativo.
Sesión 3 (1-2 horas)	Actividades del 5-8 del cifrado de César. La sesión será presencial, gran grupo. Interacción magistral, dialógica y trabajo colaborativo.
Sesión 4 (1-2 horas)	Actividades del 9-11 del cifrado de César y discutir la primera actividad del cifrado con alfabeto decimado. La sesión será presencial, gran grupo. Interacción magistral, dialógica, trabajo colaborativo, la clase se dividirá en tres subgrupos.
Sesión 5 (1-2 horas)	Actividades del 2-5 del cifrado con alfabeto Decimado. La sesión será presencial, gran grupo. Interacción magistral, dialógica y trabajo colaborativo.
Sesión 6 (1-2 horas)	Actividades del 1-4 del cifrado Afín. La sesión será presencial, gran grupo. Interacción magistral, dialógica y trabajo colaborativo.
Sesión 7 (1-2 horas)	Dudas acerca de la orientación seleccionada por cada equipo. La sesión será presencial, gran grupo. Interacción magistral, dialógica, trabajo colaborativo, clase dividida en tres subgrupos.

Figura 4.13: Distribución de las actividades por sesión.

4.9. Otros recursos instruccionales y modos de interacción

El proceso de desarrollo contempla, además de la realización de cada una de las actividades propuestas, los siguiente recursos institucionales y modos de interacción.

Colección de ejercicios resueltos.

- La sesiones presenciales del curso de Álgebra Superior II.

- Seminarios de discusión de temas del curso de Álgebra Superior II.

- Textos de estudio. Se trata de la bibliografía básica para el curso de Superior II (Gómez, 2014 y Zaldivar, 2012).

- Pizarrón; se utiliza como espacio de comunicación entre los estudiantes y el profesor.

- Un blog virtual; se utiliza como espacio de comunicación asincrónica entre estudiantes como pares y el profesor.

4.10. Instrumentos de evaluación

Después de la implementación del proyecto de Criptografía, los equipos nos entregarán el trabajo final y se les asignará fechas para que los expongan. Para evaluar los proyectos y las exposiciones utilizaremos como instrumentos de evaluación:

- **Lista de cotejos**. Consiste en una relación de elementos relevantes para el desarrollo del proyecto, tiene como objetivo verificar si los estudiantes ponen en juego los conocimientos que está adquiriendo (?, ?). En nuestro caso, utilizaremos el análisis preliminar de cada una de las actividades propuestas.

- **Autoevaluación**. Es una herramienta que busca la reflexión del desempeño de los estudiantes, asi como identificar situaciones en las cuales él podrá mejorar.

- **Coevaluación**. Con este instrumento buscamos que el estudiante se involucre en la toma de decisiones para la evaluación (?, ?), así como la reflexión del trabajo de cada uno de los integrantes de su equipo.

Capítulo 5

Descripción de la implementación

5.1. Introducción

La implementación del proyecto de Criptografía se realizó durante un curso normal de Álgebra superior II, la duración de éste fue de un semestre escolar. Utilizaremos nociones de *configuración* y *trayectoria didáctica* (?, ?) para realizar un análisis de:

- El progreso de los significados institucionales implementados.
- Los aprendizajes logrados.
- Los patrones de interacción profesor-alumno.
- El reconocimiento de conflictos cognitivos e interaccionales.

La descripción y el análisis de la implementación considera los conocimientos y las interacciones que efectivamente se llevaron a cabo. El número de estudiantes inscritos en el curso de Álgebra Superior II fue de 74.

La implementación del proyecto se llevó a cabo en tres etapas: **1)** La presentación del proyecto y la formación de equipos; **2)** el seguimiento de las actividades propuestas y **3)** la presentación del trabajo final de forma escrita y oral.

5.1.1. Trayectoria didáctica generada mediante el proyecto de Criptografía

En la Facultad de Ciencias al inicio de cada semestre todos los estudiantes que se inscribirán al segundo, o un semestre posterior, tienen la oportunidad de conocer a los

profesores que impartirán las asignaturas de su interés y como consecuencia ellos escojan a los docentes que les convenzan por su forma de enseñanza o de evaluación.

Sesión 0 (1 hora)

Con base en lo anterior, el primer día de clases del curso de Álgebra Superior II (asignatura donde se implementó el proyecto) el profesor presentó los temas a desarrollar y la forma de evaluación.

El profesor explicó que el curso cubrirá los temas propuestos por la facultad y al mismo tiempo ellos deberán realizar un proyecto de Criptografía a lo largo del semestre. La evaluación estará dividida en dos partes: **1)** exámenes parciales y tareas de apoyo y **2)** el proyecto de Criptografía que se evaluará un trabajo por escrito y una exposición al finalizar el semestre.

Por ultimo, el profesor explica que el objetivo principal del curso de Álgebra Superior es que adquieran los conocimientos pretendidos por la institución y que logren aplicarlos en una disciplina en concreto, es decir, en la Criptografía.

Sesión 1 (2 hora)

Una vez presentados los objetivos del curso de Álgebra Superior II. El profesor realizó un cuestionario diagnóstico con una duración de *15 minutos* con el objetivo de identificar los conocimientos previos que tenían los estudiantes de la Criptografía. Al finalizar se discutieron las respuestas en grupo. Las preguntas que se realizaron fueron las siguientes:

1. ¿Sabes en qué consiste la Criptografía?
2. ¿Cómo se relaciona la Criptografía con las matemáticas?
3. ¿Sabes o conoces qué relación existe entre la Criptografía y la licenciatura que estudias?

Destacamos un primer hecho didáctico significativo (HDS) en el que el profesor *interactúa* con los estudiantes en la discusión de las respuestas dadas y que los estudiantes *recuerdan* nociones básicas de la Criptografía en la vida cotidiana.

HDS_1 *Cuestionario diagnóstico e interacción entre el profesor y alumno*

P:[$\cdots$] Vamos a compartir las respuestas que contestaron en el cuestionario, ¿quién tiene noción o sabe qué es la Criptografía? [$\cdots$]

[· · ·] ¿En alguna ocasión han ocultado un mensaje por medio de una técnica o han recibido un mensaje "encriptado"que deban descubrir? [· · ·]

[· · ·] Las personas que han ocultado o recibido un mensaje usando algún método, ¿qué tan segura fue su técnica?, ¿tuvieron que mejorarla o tuvieron que ser ingeniosos para encontrar otras formas de ocultar su mensaje?[· · ·]

[· · ·] La Criptografía es una rama de las matemáticas cuyo objetivo es encontrar método funcionales para proteger la información, así como ustedes querían ocultar un texto de alguien; hoy en día las grandes organizaciones como el banco tienen la necesidad de mantener la seguridad de todos los datos que manejan. De manera que, se apoyan de la Criptografía para lograr el objetivo.[· · ·]

[· · ·] El curso de Álgebra Superior II, permite adquirir los conocimientos básicos para iniciar un estudio de la Criptografía. Además, lo relevante es que sin importar la licenciatura que estén estudiando, esta rama permite apreciar sus implicaciones tanto en la matemática teórica, en la programación y eficiencia de los algoritmos, así como el impacto en la seguridad financiera o la protección de la información personal de hoy en día. [· · ·]

[· · ·] Hemos explicado los objetivos de este curso y dentro de la evaluación ustedes realizarán un proyecto de Criptografía que se realizará paralelamente al desarrollo de los temas del curso. Para esto, les pido formar equipos de 8 a 10 personas como máximo y elijan el nombre de su equipo, pero que esté relacionado con la ciencia.[· · ·]

[· · ·] Por equipo deberán investigar acerca de los orígenes de la Criptografía y entregar sus avances [· · ·]

La interacción del docente con los estudiantes tuvo una duración de 30 minutos aproximandamente, el tiempo restante se dedicó a la formación de los equipos. Esta sesión la relacionamos con los criterios de la idoneidad interaccional y afectiva. Se presentaron actividades donde los alumnos identificaron la utilidad de las matemáticas en la vida cotidiana. A través de la discusión del cuestionario fomentamos la participación de ellos y al mismo tiempo su inclusión en la dinámica de la clase.

Sesión 2 (1 hora)

Después de que el profesor recolectó los conocimientos previos de Criptografía de los estudiantes y de indicarles la primera actividad a desarrollar, ellos entregaron sus avances por escrito una semana posterior a la sesión 1. De modo que en la segunda sesión, el

docente *explicó* la importancia de las fuentes de información, como identificarlas y por último retroalimentó los trabajos entregados por cada equipo. Las investigaciones realizadas por los estudiantes manifestaron los conflictos para identificar fuentes confiables de información y como consecuencia obtener un indagación histórica de la Criptografía confiable.

[HDS_2] *Interacción dialógica entre el profesor y los alumnos.*

P:[$\cdots$] Para realizar una investigación histórica confiable es de suma importancia identificar fuentes adecuadas. Hoy en día el uso del internet ha cambiado la forma de obtener la información. Lamentablemente no todo sitio en la red contiene información verídica. Por lo que, ustedes deberán identificar los autores, su trayectoria, la institución que está publicando la revista o el libro que consultan, el número de citas que tiene el medio de información, [$\cdots$]

[$\cdots$] Los trabajos que les regreso tienen notas y sugerencias que les ayudará mejorar la indagación histórica. ¿En qué otras fuentes puedes ustedes consultar?[$\cdots$]

[$\cdots$] ¿Cuál es la importancia de consultar y citar fuentes confiables?[$\cdots$]

Este hecho didáctico lo consideramos significativo, ya que los alumnos toman consciencia de la importancia de las fuentes de información. Además, puede influir en el desarrollo de las argumentaciones y demostraciones matemáticas, ya que en ambas evitan tener afirmaciones ambiguas que puedan llevar a una contradicción o un hecho falso.

Terminando la discusión presencial de esta sesión, el profesor proporcionó un sitio de internet en el cual se utilizó para porporcionarles las actividades de la segunda parte del proyecto de Criptografía. Se pretende utilizar el espacio para que los estudiantes compartan sus dudas, las cuales podrán contestarlas entre ellos o el profesor. Además, se podrán compartir sitios de internet o material digital útiles para el desarrollo del proyecto. Esta sesión está relacionada con los criterios de la idoneidad cognitiva, interaccional y mediacional.

Sesión 3 (1 hora)

Una vez que los estudiantes tienen el blog donde se publicaron las actividades del proyecto de Criptografía, en la tercera sesión se realizó una discusión entre todo el grupo acerca del Cifrado de César. El profesor *otorgó* la palabra a los alumnos y por equipos (voluntariamente) *explicaron* el origen y el funcionamiento de este método. La intervención del profesor está en la interacción entre los estudiantes; de modo que involucra a todo el grupo para realizar juntos la verificación de la información de sus compañeros de clase.

Seguidamente, el profesor solicitó que los estudiantes intentaran escribir con sus propias

palabras el Cifrado de César sin utilizar el lenguaje matemático. Se pretendió que ellos lograran formular enunciados claros para argumentar el método.

Debido al limite de tiempo disponible en el salón de clases, el profesor proporcionó la opción de seguir trabajando en la discusión de las actividades del Cifrado de César por equipo en horarios extra clases. Recordemos que el desarrollo del proyecto de Criptografía se realizó paralelamente a un curso normal de Álgebra Superior II. Hasta este momento, los estudiantes tenían la noción del concepto de la estructura de un anillo y en particular del anillo de los números enteros. Se pretende que mientras ellos resuelven las actividades del primer cifrado clásico, adquieran los conocimientos básicos de la aritmética modular (que establece el programa curricular de la asignatura) y los apliquen en el proyecto.

Sesión 4 (2 horas)

A partir de este momento, la interacción entre los estudiantes y el profesor es adecuada, es decir, los alumnos tienen la confianza de expresar sus dudas, tienen la iniciativa de comenzar debates en relación al proyecto y los contenidos desarrollados en el curso. De modo que ellos solicitaron sesiones extras para fortalecer los conocimiento que van adquiriendo en el curso de Álgebra y para responder dudas acerca del proyecto de Criptografía.

Varios equipos entregaron avances de sus indagaciones históricas junto con la bibliografía de las fuentes de consulta. La cuarta sesión se caracterizó por una interacción magistral por parte de los equipos, dialógica entre los estudiantes y el profesor.

A través de las exposiciones de los equipo, notamos que tenían dificultades en las demostraciones matemáticas alrededor del concepto de divisibilidad y máximo común divisor. De modo que se realizaron diversos ejemplos para comprender el concepto y algunos de los resultados (Teoremas) involucrados.

Cada equipo trabajó colaborativamente para resolver algunos ejercicios propuestos en clase y comprender los temas de divisiblidad y de máximo común divisor. El uso del pizarrón fue importante para la discusión en relación a la solución de los problemas y para fomentar la participación de los estudiantes. Ejemplos de ejercicios que los estudiantes resolvieron en conjunto fueron los siguientes:

1. Si $m \in \mathbb{Z}$ impar, demuestra que no es combinación lineal de 198 y 290
2. Si existe $n \in \mathbb{N}$ tal que $p \mid a^n$, demuestra que $p \mid a$
3. Si p es un primo impar, observa que al dividirlo entre 4 deja residuo 1 o 3.Demuestra

que hay un número infinito de primos de la forma $p = 4n + 3$. También es cierto que hay un número infinito de primos de la forma $p = 4n + 1$, sin embargo, la demostración no es tan sencilla como la que seguramente obtuviste para el caso de primos de la forma $p = 4n + 3$. ¿Podrías decir donde falla esta demostración para el caso $p = 4n + 1$?.

Sesión 5 (2 horas)

Los estudiantes son responsables de entregar los avances del proyecto de Criptografía y el profesor realizó las observaciones pertinentes. El objetivo principal de la retroalimentación es verificar que toda afirmación esté bien fundamentada. Consecuentemente, se busca el fortalecimiento de la realización de las demostraciones matemáticas.

En la quinta sesión se trabajó por equipo en el desarrollo de las actividades del cifrado Decimado. Cabe señalar que las actividades de este método busca que los estudiantes construyan sus propias afirmaciones matemáticas, sin el apoyo de una guía exhausta de actividades como es el caso de las del cifrado de César. La dinámica de la sesión fue similar a la anterior, es decir, el estudiantes es el que dirige, expone sus avances y sus dudas en la comprensión del cifrado Decimado.

En el desarrollo de las actividades de este cifrado, se identificaron dificultades al definir la función que descifra un mensaje encriptado con este méodo. La dificultad se debió en cómo identificar si un elemento a en un anillo $\mathbb{Z}_k$ tiene un inverso multiplicativo y si lo tiene cómo encontrarlo. Como consecuencia el profesor realizó diversos ejemplos, *recordó* la definición de clases de equivalencia, la operación producto entre ellas y de dominio entero. De modo que solicitó a los equipo que resolvieran las siguientes preguntas.

- Considera el anillo $\mathbb{Z}_3$, ¿cuáles son los elementos en $\mathbb{Z}_3$ que tienen inverso multiplicativo?
- Encuentra $n \in \mathbb{Z}$ tal que $[1][2] = [1]$ con $[1], [2] \in \mathbb{Z}_n$
- ¿El anillo $\mathbb{Z}_6$ es un dominio entero?
- Sea $g = mcd(a, m)$. entonces $ax \equiv ay \mod m$ si y sólo si $x \equiv y \mod (m/g)$

A través del trabajo colaborativo y la interacción con el profesor, los estudiantes lograron resolver las preguntas sin dificultad. Una vez teniendo la claridad de esto la dirección que tomó la sesión fue en discutir de qué manera se puede definir una función que esté bien definida para decifrar cualquier texto oculto por el método decimado.

$[HDS_3$] *Interacción dialógica entre el profesor y los alumnos.*

P:[$\cdots$] Para definir la función que descifra un mensaje cifrado por el método decimado, es necesario verificar que satisface la definición de función. ¿Cuáles son los detalles

que deben prestar atención al definir la función que buscan?[...]

[···] ¿Cuáles son las codiciones necesarias y suficientes para que la función del cifrado decimado sea biyectiva? [···]

Sesión 6 (1 horas)

Hasta este punto los estudiantes encontraron espacios para dialogar entre ellos acerca de los temas del curso de Álgebra y al mismo tiempo para el desarrollo de las actividades del proyecto de Criptografía. La sexta sesión se llevó acabo en el horario de clases, fue una interacción magistral donde el docente *explica* la idea intuitiva del comportamiento del cifrado Afin. Solicitó que los estudiantes construyeran sus propios ejemplos y se realizó una discusión entre todos para poder definir la función que describe este método y la relación con los dos anteriores.

Sesión 7 (2 horas)

Como consecuencia de las sesiones anteriores y el desarrollo de las actividades los estudiantes solicitaron sesiones por equipo para la revisión de sus trabajos. La intereacción fue presencial y en línea, donde se aprovecharon los sitios de internet como el blog que se proporcionó al inicio del curso y el Drive, con el cual algunos equipos compartieron sus documentos con el profesor para que éste realizara comentarios en línea y cada uno de los integrantes tengan acceso inmediato a ellos.

Además, ellos expresaron sus intereses para orientar la última parte del proyecto de Criptografía. Las áreas de interes para los equipos fueron los siguientes:

1. Fundamentos matemáticos para llevar a cabo el criptoanálisis de los cifrados clásicos.
2. Las diferencias entre la Criptografía simétrica y asimétrica.
3. La evolución de la Criptografía a través de las neceidades de la sociedad.
4. La relación entre un sistema criptográfico y la computación.

Sesión 8 (1 hora)

El profesor *explicó* los criterios que debería tener el trabajo por escrito de cada equipo, las fechas donde se llevarán a cabo las exposiciones, así como las características que deberrían considerar para realizar una presentación.

Sesión 9 (1 horas)

Una vez que los equipos entregaron sus trabajos por escrito al profesor, ellos trabajaron en la dinámica que realizarían en las exposiciones. El profesor pregunta a cada uno de ellos su avance y da sugerencias.

Sesión 10 (1-2 horas)

La sesión 10 consideramos todas y cada una de las exposiciones de los equipos. Se dió un máximo de 30 minutos para que los estudiantes expusieran sus trabajos ante el profesor y sus compañeros. Al finalizar, se realizaron preguntas dirigidas al equipo en general y a cada integrante.

La motivación de este tipo de distinción de reactivos fue motivada para que cada equipo reflejara el trabajo colaborativo que se realizaró a lo largo de todo el semestre y al mismo identificar que cada alumno haya logrado adquirir los conocimientos básicos de Criptografía y del curso de Álgebra Superior II.

[HDS_4] *Interacción dialógica entre el profesor y los alumnos. Sesiones magistrales por parte de los alumnos*

Equipo 1:[$\cdots$] El objetivo de este proyecto es el de describir la evolución de la Criptografía desde sus orígenes hasta la actualidad haciendo especial enfásis en aquellos cifrados que revolucionaron al mundo respecto al manejo de datos.[$\cdots$]

[$\cdots$] Se busca destacar la importancia de la seguridad, utilizando conceptos del Álgebra.[$\cdots$]

$\cdots$ El sistema de encriptación que más nos gustó fue el de Vigenère. Les estamos repartiendo una hoja con una tabla con una serie de símbolos y lo que deben hacer es descubrir el mensaje oculto [$\cdots$]

Equipo 2 :$\cdots$] La finalidad de nuestro trabajo es comprender el significado de la Criptografía. Además nuestro trabajo por escrito está dirigida a aquellas personas que tengan conocimiento acerca de temas matemáticos, tales como el Álgebra modular, y panoramas históricos básicos [$\cdots$]

[$\cdots$] Notamos que hay factores como el tipo de alfabeto, los signos de puntuación y signos de separación que influyen de manera significativa en la interpretación del mensaje. [$\cdots$]

[$\cdots$] En lugar de realizar un diagrama de flujo que explique el funcionamiento de cifrado de césar, nosotros lo programamos, observemos como es el código y como se implementa [$\cdots$]

[$\cdots$] Después de haber estudiado los cifrados clásicos con detenimiento, afirmamos que el más díficil de descifrar es el afín ya que es una combinación del cifrado de césar y el decimado [$\cdots$]

[$\cdots$]Estudiar los cifrados clásicos nos permitió ver la aplicación del Álgebra modular [$\cdots$]

[$\cdots$] Traemos una actividad para nuestros compañeros, este es un tríptico donde

resumimos los temas más importantes de los cifrados clásicos y al final deben completar un crucigrama [· · ·]

Equipo 3: [· · ·] Nuestro trabajo está orientado en proporcionar una visión generalizada de cómo evolucionaron los procesos para proteger la información [· · ·]

[· · ·] Tendrá un enfoque matemático, razón por la cual es necesario introducir conceptos y demostraciones [· · ·]

[· · ·] La Criptografía ha crecido a la par de dos ciencias: las matemáticas y la computación. Nosotros investigamos métodos de encriptación más modernos y los programos utilizando lenguajes de programación como java y Pyton [· · ·]

[· · ·] Uno de los cifrados que investigamos y nos gustó el es llamado GAMAL, veamos en qué consiste y como lo programamos [· · ·]

Los hechos didácticos descritos ilustran algunas rasgos princiales del diseño intruccional implementado. En el siguiente apartado, describiremos una síntesis de los hechos didácticos significativos que identificamos en la experimentación del proyecto de Criptografía. Los cuales los clasificaremos según las facetas consideradas en un proceso intruccional.

5.2. Síntesis de hechos didácticos significativos y análisis *a posteriori*

En esta sección realizaremos una síntesis de los hechos significativos que identificamos en la implementación del proyecto de Criptografía, clasificados en las facetas epistémica-ecológica, cognitiva-afectiva, instruccional-mediacional.

5.2.1. Facetas epistémica y ecológica

- El proyecto de Criptografía se centró en el proceso de aprendizaje de los cifrados clásicos (César, Decimado y Afín). Los estudiantes mencionaron disciplinas relacionadas a estos cifrados y ellos involucran el algoritmo del cifrado de César con la programación.

- Los *conceptos* y *definiciones básicas* de la aritmética modular fueron presentados por el profesor (divisibilidad, números primos, máximo común divisor, congruencias, clases de equivalencia, dominio entero, · · ·)

- Las principales *representaciones* utilizadas para el estudio de la aritmética modular fueron la notación de función, diagramas y tablas. Las cuales fueron presentadas por el profesor y posteriormente los alumnos las utilizaron para realizar el proyecto de Criptografía.

- Los *procedimientos fundamentales* del tema de Criptografía (definir las funciones de cifrado y de descifrado, la construcción de demostraciones, ocultar y descubrir textos bajo un método de encriptación) fueron empleados por los estudiantes para dar respuestas a cada una de las actividades propuestas, formar conjeturas y verificarlas.

- Se propusieron *procesos de traducción* entre distintas representaciones de un sistema criptográfico: representación de la correspondencia biunívoca entre alfabetos (funciones), representación de la posición de un alfabeto en plano y cifrado en tablas y la interpretación del significado de un algoritmo de cifrado en el lenjuaje natural.

- Se promuevió el desarrollo de argumentos, de demostraciones matemáticas en cada actividad propuesta en el proyecto.

- Los estudiantes relacionaron los temas de Álgebra del curso con otras áreas, como la computación. Ellos utilizaron el uso de diferentes lenguajes de programación como $C++$, *java* y *Pyton*.

5.2.2. Facetas interaccional y mediacional

- En las sesiones de trabajo grupales y por equipos se manifiestaron las diversas dificultades; algunos estudiantes no entendieron el concepto de un anillo finito, de clases de equivalencia, congruencias y la relación con la Criptografía. Ante esta situación el profesor sugirió que ellos construyeran sus propios ejemplos en relación a sus dudas, los motiva a escribir sus ideas y que le expusieran la resolución que obtuvieron. Cabe señalar que esta solución se fundamentó en la interacción del profesor con los alumnos de manera personal, buscando que ellos vieran las dificultades para comprender algún concepto matemático como una oportunidad para cambiar la perspectiva de estudio.

- La distribución de las actividades del proyecto y del desarrollo de los temas del curso de Álgebra necesitó mejor presición. De modo que se necesitaron más sesio-

nes fuera del salón de clases para discutir temas tanto del proyecto como de los temas de la materia.

- El uso del blog y de medios de comunicación por internet facilitaron intercambiar sugerencias en los avances de los equipos y compartir sitios en la red que cifran textos utilizando diversos métodos.

- Se promovieron espacios donde los alumnos asummieron la responsabilidad del estudio. Aquí, el profesor trabajó como un guía.

5.2.3. Facetas cognitiva y afectiva

Se identificaron como relevantes los siguientes conflictos:

- Los alumnos comprendían intuitivamente el funcionamiento de los cifrados clásicos propuestos; sin embargo la formalización matemática de cada uno se les dificultó. Conflicto cognitivo en el uso del lenguaje y la interpretación de las funciones que definan a cada cifrado.

- El diseño de las actividades no contempló el criptoanálisis. De modo que los alumnos tuvieron dificultades para encontrar los métodos para encontrar la clave secreta de un mensaje oculto por alguno de los cifrados.

- Cálculo de congruencias lineales; se insistió a los alumnos que utilizaran los teoremas demostrados en el curso de Álgebra y los emplearan en la resolución de las actividades del proyecto de Criptografía. Conflicto cognitivo en la representación de las hipótesis de algunos teoremas correspondientes al curso de Álgebra en el proyecto.

- Construir conjeturas. A los estudiantes se les dificultó encontrar las condiciones necesarias y suficientes para definir las funciones biyectivas de los cifrados Decimado y Afín. Así como la demostración de estas afirmaciones.

- Elaboraran ejemplos de los cifrados clásicos utilizando diferentes tipos de conjunto de símbolos para cifrar.

- El trabajo colaborativo; los estudiantes se enfrentaron a diversas dificultades de comunicación para organizarse en la elaboración del proyecto de Criptografía, así como en la presenación final. Las principales obtáculos fueron: integrantes del

equipo que no colaboraban y la diferencia de intereses y objetivos para decidir un tema concreto en la tercera sección del trabajo.

- Elaborararan de los diagrámas de flujo o en su caso propramar algún cifrado.

Capítulo 6

Idoneidad del proceso de estudio. Identificación de posibles mejoras

En este capítulo se compara, en primer lugar, el diseño del proyecto de Criptografía, es decir, el análisis *a priori* con los hechos didácticos significativos observados. Seguidamente, se determina y se discute el aspecto normativo en el cual fue condicionado tanto el diseño como la implemtentación. Por último, se valora la idoneidad didáctica y se proponen posibles mejoras.

6.1. Comparación del diseño con los hechos didácticos observados

Tipo de problema y prácticas álgebraicas (teoría modular)

Las prácticas algebraicas en el área de la teoría modular realizadas en el desarrollo del proyecto de Criptografía fueron concordantes con las que se comtemplaron en el análisis *a priori*. Los estudiantes utilizaron tablas para mostrar el comportamiento de cada cifrado, conjeturaron los posibles teoremas para encontrar y demostrar las funciones que definen a cada sistema criptográfico. Emplearon los conceptos vistos en el curso de Álgebra Superior II, así como aplicaron sus conocimientos en programación para definir los algortimos del método de César.

Los ayudantes complementaron algunos conceptos de Criptografía con el uso de tablas, de ejemplos de congruencias como otra forma de visualizar los comportamientos de cada cifrado.

Elementos lingüisticos

Los alumnos mostraron dificultades en expresiones lingüisticas relativas al lenguaje de símbolos y funciones asociadas a los métodos de encriptación. Ante esto el profesor realizó explicaciones magistrales (dentro y fuera de clase) y puntuales (a toda la clase o a cada equipo) que permitieron dar el significado y la comprensión a dichas expresiones.

Elementos conceptuales

Los conceptos elementales de la teoría modular fueron introducidos por el profesor y los ayudantes en el curso de Álgebra Superior II. En este espacio se propició la construcción de ejemplos, la conjetura de resultados y en las demostraciones en matemáticas. Hubo conceptos con los que se esperaba que los estudiantes estuvieran familiarizados que resultaron conflictivos para el desarrollo del proyecto de Criptografía; específicamente, los conceptos de relación de equivalencia, clases de equivalencia y particiones.

Ante esto el profesor y los ayudantes abordaron estos temas a través de clases magistrales y asesorias extras para reforzar dichos conceptos.

Procedimientos

Los procedimientos considerados, conocidos por los estudiantes en el diseños, el cálculo de congruencias y la contrucción de funciones para cada cifrado se fueron desarrollando con poca dificultad.

Argumentos

La construcción de argumentos y de demostraciones por parte de estudiante fueron concordantes al diseño.

Debido a la falta de formalidad y de argumentos sólidos para construir las demostraciones involucradas en el diseño; el profesor fue quien los orientó y los motivó. Como consecuencia; los estudiantes tomaron conciencia de sus errores y buscaron la manera de reformular sus argumentos para encontrar una demostración adecuada.

Procesos

Los procesos considerados en el análisis *a priori* fueron empleados por los estudiantes.

Ellos identificaron los procesos generales que debían seguir para dar respuesta a las actividades propuestas; tales como analizar, proponer problemas, demostrar, describir u observar.

Dichos procesos se reflejaron en la resolución de sus últimos exámenes parciales para la materia de Álgebra Superiori II, al realizar las exposiciones de los proyectos y la forma de expresarse.

En síntesis, el contraste entre los HDS observados y el análisis *a priori*, muestra que desde el punto de vista cognitivo los estudiantes manifestaron los conflictos previos y algunos otros. Desde el punto de vista instruccional los estudiantes estuvieron guiados por el profesor; donde poco a poco mostraron autonomía y adquirieron la responsabilidad total para aplicar los procesos considerados y dar respuesta a cada una de las actividades propuestas en el proyecto. Un hecho interesante es que en la realización de las exposiciones los estudiantes mostraron un caracter profesional. Escencialmente encontraron la conexión entre las matemáticas escolares (nivel superior), con su licenciatura y con el campo laboral.

6.2. Dimensión normativa. Condicionamientos del proceso de estudio

La implementación del proyecto de Criptografía que se analiza en este trabajo, se ajustó al plan de estudios de la Facultad de Ciencias en una asignatura del tronco común de las tres licenciaturas de interés (Matemáticas, Actuaría y Ciencias de la Computación).

6.3. Idoneidad del proceso de estudio. Identificación de posibles mejoras

6.3.1. Faceta epistémica y ecológica

La idoneidad epistémica y ecológica del proceso de estudio la consideramos media, tanto como de diseño como de implementación. Esta valoración la basamos en la guía propuesta por Godino (2011) y la listamos en los siguientes puntos.

- El diseño de las actividades propiciaron la construcción de conjeturas por parte de los estudiantes.
- Consideramos que faltó relacionar las actividades propuestas con el tema de algoritmos, el cual consideramos esencial para los estudiantes de Ciencias de Computación y que podría ayudar a los otros estudiantes en la construcción de demostraciones.
- Las actividades fueron adecuadas al nivel educativo de los alumnos.
- Las actividades se apoyaron de definiciones y teoremas fundamentales del curso de Álgebra Superior II.
- Se utilizaron diferentes modos de expresión matemática en la implementación del proyecto; verbal, escrita, símbolos y tablas.
- Los argumentos y las demostraciones fueron adecuadas para el nivel académico de los estudiantes.
- La mayoría de las actividades promovían la construcción de argumentos o demostraciones. Además de que cada una de ellas se relacionaban entre sí.
- Los contenidos básicos de la teoría modular del proyecto correspondían al currículo. Los temas relacionados exclusivamente con Criptografía no forman parte del programa sugerido del curso de Álgebra Superior II.
- Dos aspectos innovadores del proyecto fueron la investigación histórica en relación a la Criptografía con otras áreas como la computación o la seguridad bancaria.
- Los contenidos y las instrucciones de las actividades contribuyeron a la formación socio-profesional de los estudiantes.

6.3.2. Facetas cognitivas y afectiva

La idoneidad cognitiva y afectiva del proceso de estudio la consideramos de nivel alto, tanto en el diseño como en la implementación. Esta valoración la basamos en la guía propuesta por Godino (2011). Para mejor compresión de los factores que tomamos en cuenta para esta valoración los listamos como sigue.

- Los contenidos pretendidos en cada una de las actividades se alcanzaron, es decir, la dificultad fue manejable.
- Algunos de los alumnos no tenían los conocimientos previos suficientes para desarrollar las actividades.

- La revisión de los trabajos finales evaluó la comprensión conceptual de los contenidos, las competencias argumentativas en la resolución de cada actividad y la orientación que le dio cada equipo al proyecto.
- Las exposiciones evaluaron la comprensión de los temas y las competencias argumentativas de forma oral.
- Las actividades propuestas fueron interesantes para los estudiantes.
- Faltó mejor contextualización de las actividades con la vida cotidiana.
- El diseño y la implementación del proyecto fomentó la participación de los alumnos. Como consecuencia ellos adquieron la responsabilidad de terminar el trabajo en forma y a tiempo. Ellos se organizaron para tener reuniones fuera del aula de forma presencial y virtual; definieron roles dentro de cada equipo y realizaron varias exposiciones piloto antes de la presentación ante el profesor y los ayudantes.
- La implementación del proyecto causó en los alumnos la detección de los errores cometidos tanto en la parte conceptual como en la organización grupal siendo esto una oportunidad de aprendizaje; tomaron nuevas y distintas decisiones para colaborar en equipo y terminar satisfactoriamente el trabajo.
- Los alumnos mostraron las cualidades que tienen las matemáticas dependiendo del área y la orientación que le dieron a su proyecto.

6.3.3. Faceta interaccional y mediacional

De acuerdo con los indicadores de idoneidad didáctica, consideramos que la idoneidad interaccional y mediacional es de nivel medio. Los factores que consideramos son los siguientes:

- Se utilizó principalmente el pizarrón para introducir situaciones, lenguajes o procedimientos relacionados con el proyecto.
- El gran número de alumnos dificultó la distribución de los tiempos para la implementación. De modo que el tiempo no fue suficiente para la enseñanza pretendida. Se necesitó tomar varias horas extras.
- El horario de clase y de las sesiones presenciales fue adecuado.
- El profesor realizó una buena presentación del tema y enfatizó en los temas claves tanto para el proyecto como para el curso de Álgebra Superior II.
- En todo momento el profesor y los ayudantes dieron respuesta a los conflictos de los estudiantes. De modo que, ellos abrieron espacios donde los alumnos podían expresar sus dudas o sus avances.

- Algunos equipos abrieron espacios en línea como Drive para realizar modificaciones, comentarios, correcciones o sólo desarrollar el proyecto de forma conjunta. Sitio donde los cuales estudiantes compartieron con el profesor y los ayudantes; quienes fueron principalmente espectadores; sólo intervinieron en situaciones muy específicas.

6.3.4. Idoneidad didáctica

Por lo que se refiere a la noción de idoneidad didáctica correspodiente al proceso de estudio implementado, veásela figura 7.1, la representamos como el siguiente hexágono irregular, donde se obseva que tuvimos una idoniedad alta en las facetas interaccional, afectiva, cognitiva y epistémica; en cambio, hubo una idoneidad media en las dimensiones ecológica y mediacional. Para comprender mejor esto, lo argumentaremos como sigue:

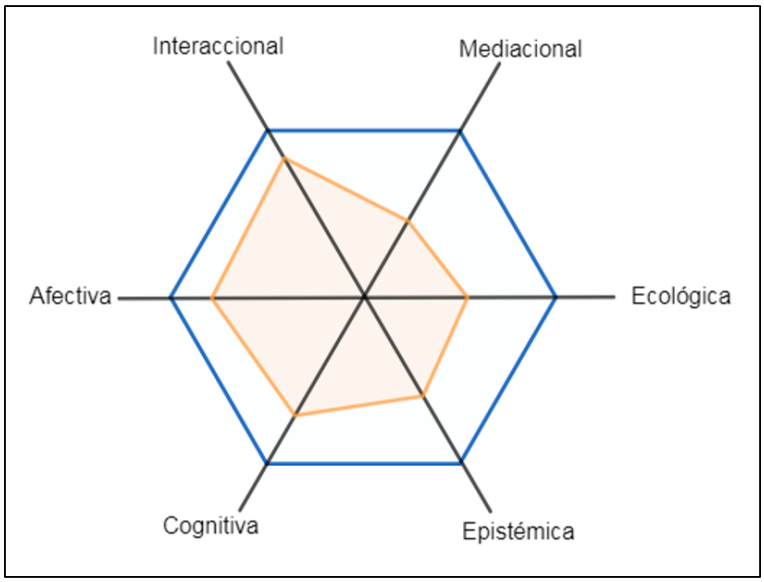


Figura 6.1: Idoneidad didáctica correspondiente a la implementación del proceso de estudio.

En la implementación del proceso de estudio identificamos que el comportamiento fue de tipo autoregulado [1] por parte de los alumnos fue de tipo autónoma; ya que hubo frecuentes momentos de trabajo autónomo. Por consiguiente, ellos tomaron la responsabilidad de este proceso y adecuaron sus intereses a los objetivos del proyecto de Criptografía. De modo que consideramos que esto es reflejo de una idoneidad afectiva

[1]Este concepto lo tomamos desde la perspectiva de Zimmerman, donde los alumnos pueden considerarse autorregulados si desde el punto de vista metacognitivo, motivacional y conductual, ellos son activos en su propio proceso de aprendizaje(?, ?)

alta. Además, buscaron espacios para compartir sus avances o dudas con el profesor, así como organizar en varias ocasiones el desarrollo del proyecto entre cada equipo. De ahí que obtenemos una idoneidad interaccional alta.

Los alumnos fueron capaces de apropiarse de los conocimientos pretendidos por el profesor en relación al proyecto de Criptografía; como evidencia se tiene los trabajos por escrito y las exposiciones. Como resultado tenemos una idoneidad cognitiva alta. En relación a la idoneidad epistémica se logró una buena conexión entre el proyecto y el currículo sugerido, esto se reflejó en los resultados de los exámenes parciales, en las reposiciones o en el final; los cuales corresponden a la evaluación de los temas desarrollados en el curso de Álgebra Superior II.

Llegados a este punto, examinaremos brevemente las idoneidades tanto mediacional y ecológica; las cuales obtuvieron un nivel medio en la implementación del diseño instruccional. En vista de que el número de alumnos inscritos en la asignatura fue de 74 [2] , el seguimiento del proyecto tanto individual como por equipo fue conflictivo. Los medios que utilizó el profesor en el proceso de estudio fueron principalmente el uso de pizarrón y por último, consideramos que faltó establecer mejores conexiones entre la Criptografía, con la computación y con la vida cotidiana.

[2]Los estudiantes pertenecían a las licenciaturas de Matemáticas, Ciencias de la Computación, Actuaría y Física.

Capítulo 7

Síntesis de resultados e implicaciones

A través de la metodología de la ingeniería didáctica, nos proporcionó herramientas para organizar y analizar el proceso de estudio. En el análisis preliminar se estudio el concepto de Criptografía a lo largo de la historia y su relación en la enseñanza tradicional; mientras que en el análisis *a priori* se muestran las actividades o situaciones-problemas; así como los objetos y procesos que pone en juego la resolución de cada actividad propuesta, a fin de identificar posibles conflictos de aprendizaje y los elementos que deben tenerse en cuenta en la implementación.

En la fase de la implementación utilizamos distintos tipos de configuraciones y procesos didácticos para identificar hechos didácticos significativos. Por último en el análisis *a posteriori* contrastamos los resultados obtenidos con las actividades seleccionadas y descritas en el análisis *a priori*.

La noción de idoneidad didáctica nos proporcionó una síntesis global sobre los procesos de estudio involucrados en nuestro trabajo, además aportó vías para la reflexión sobre las distintas facetas e se identificaron decisiones que mejoren potencialmente dicho proceso en futuras implementaciones. Para ser más específicos identificamos como posibles mejoras los siguientes puntos.

- En la idoneidad epistémica se requiere un mejor uso de expresiones matemáticas[1].

- En la idoneidad cognitiva se precisa de información detallada de los significados

[1]Entendemos como expresiones matemáticas a la simbolización, el uso de tablas, gráficas, diagramas, entre otros.

personales, la identificación de conflictos semióticos[2] y de los conocimientos previos suficientes de los alumnos involucrados en el proceso de estudio.

- En la idoneidad interaccional se requiere de evaluaciones formativas más detalladas.

- En la idoneidad mediacional se requiere visualizar o contemplar situaciones donde el número de alumnos inscritos es mayor a 40 (mínimo número de alumnos inscritos en una asignatura para tener un profesor y dos ayudante).

- En la idoneidad ecológica precisamos de mejores conexiones intradisciplinares, con la vida cotidiana y evaluaciones detalladas.

- En la idoneidad afectiva se necesita un análisis previo de los intereses y actitudes [3] de los estudiantes.

Para sintetizar el diseño general de nuestra propuesta y concluir este trabajo de tesis veamos la siguiente tabla, donde muestra de manera breve la motivación de nuestra intervención, nuestras hipótesis, los objetivos generales, los contenidos, la metodología, la evaluación, la bibliografía para las actividades de Criptografía y los recursos.

COMPONENTE	DESCRIPCIÓN
Motivación	Las causas relacionadas al abandono y deserción en los estudiantes de las licenciaturas en Matemáticas, Ciencias de la Computación y Actuaría.
Hipótesis	Si el diseño instruccional tiene como características: 1) Las actividades que relacionen la matemática formal con las prácticas contextualizadas, 2) Énfasis en la reflexión y la construcción de demostraciones matemáticas , 3) La implementación involucra activamente a los estudiantes y son acompañadas por el profesor , 4) Las actividades fomentan la construcción de conjeturas y 4) la implementación y la evaluación involucran diferentes formar de expresión, entonces los estudiantes lograrán los siguientes objetivos.
Objetivos generales	1)Mejorar las prácticas argumentativas en matemáticas e identificar diversos contextos de la demostración. 2)Lograr un aprendizaje significativo. 3)Fortalecer las interacciones entre los estudiantes y con el profesor. 4)Desarrollar habilidades para comunicar sus ideas. 5)Transformar los errores (académicos y organizacionales) a oportunidades de aprendizaje. 6)Involucrar el proceso de estudio del primer año con el proceso de titulación.
Contenidos	La criptografía: Funciones, Anillos finitos, Aritmética modular (clases de equivalencia, particiones, congruencias…), diagramas de flujo. Breve historia de la criptografía. Criptología, Criptoanálisis.
Metodología	Ingeniería Didáctica e idoneidad didáctica. Las sesiones de la implementación fue presencial, virtual, por grupo y por cada equipo. Interacción magistral y trabajo colaborativo.
Evaluación	El trabajo por escrito fue evaluado contrastando las respuestas obtenidas y las esperadas descritas en el análisis preliminar. Tuvimos una evaluación continua y nos apoyamos de los hechos relevantes durante la implementación, consideramos la sesiones presenciales, las exposiciones previas, avances del trabajo, trabajo colaborativo de los estudiantes fuera de aula tanto presencial como en espacios virtuales. Una autoevaluación y una co evaluación que se realizó después de las exposiciones finales.
Bibliografía y recursos	Galaviz José, Introducción a la Criptología. Departamento de Matemáticas, Facultad de Ciencias, UNAM, Vínculos Matemáticos #15, 2003 ; Koblitz, Neal, A Course in Number Theory and Cryptography, 2a ed., Springer Verlag, 1994, Graduate Texts in Mathematics. ; Stinson, Cryptography, theory and practice, CRC Press. Drive, Blogger, https://cifraronline.com

Figura 7.1: Diseño general del proyecto de Criptografía.

Hay que mencionar además, que este trabajo decidimos utilizar como metodología principal la Ingeniería Didáctica (?, ?) para su diseño e implementación y completamos el

[2]Los conflictos semióticos los entendemos como problemas relacionados con los signos, la comunicación y el significado (?, ?).

[3]Nos referimos a actitudes tanto positivas y matemáticas, esta última aborda una actitud inductiva, de precisión y rigor (?, ?).

análisis de proceso de estudio con la idoneidad didáctica (?, ?). Sobre esta misma línea de investigación está la visión del Dr. Godino en trabajos como Ingeniería Didáctica basada en el enfoque ontológico-semiótico (?, ?); así que queda pendiente realizar una comparación sistemática entre ambos enfoques. Sin embargo, dicha comparación no es objeto de estudio en este trabajo.

7.1. Conclusiones

Por último, con base en nuestras hipótesis logramos el objetivo general, el cual consistía en realizar un proyecto de Criptografía. Como objetivos particulares, logramos mejorar las prácticas argumentativas en matemáticas de los estudiantes, los cuales se reflejaron tanto en los trabajos por escrito como en los exámenes parciales, reposiciones o final que se realizaron en el curso de Álgebra Superior II[4].

La interacción entre los estudiantes y el profesor fue sumamente estrecha. Como consecuencia, los alumnos adquirieron confianza para comunicar sus ideas, seguido de la responsabilidad del proceso de estudio. Cabe señalar que como resultado que no consideramos, cada equipo mostró una actitud profesional en la manera de expresar sus ideas en las exposiciones; logramos observar que ellos se adjudicaron el significado de la educación superior y la vida profesional o laboral.

Deseo subrayar que sin la interacción cercana del profesor con los estudiantes, suponemos que el objetivo de transformar los errores académicos y organizacionales de los estudiantes difícilmente se hubieran llevado de forma exitosa, así como lograr de manera consciente la autonomía del aprendizaje.

Para terminar, consideramos que este tipo de propuestas en la educación superior en estudiantes en Matemáticas, Ciencias de la Computación y Actuaría tiene como consecuencias la autonomía del proceso de estudio, el cual tiene un grado de importancia significativo, sin embargo para tener mejores resultados es necesario considerar los espacios físicos y el número de alumnos involucrados.

[4]Tuvimos estudiantes que los resultados de sus reposiciones y final, respectivamente, mejoraron consideradamente después de realizar sus exposiciones del proyecto de Criptografía. Entrevistamos a estos alumnos y confesaron que la realización del proyecto les ayudó a comprender mejor temas que se les dificultó durante la clase.

Universidad Nacional Autónoma de México

FACULTAD DE CIENCIAS

Álgebra Superior II

Proyecto de Investigación "Criptografía"

Grupo 4041
Profesor: Alejandro Javier Díaz-Barriga Casales
Ayudantes: Adriana León Montes
Eric Alberto Santiago Martínez

Aguilar Barajas Gerardo Damián
Alcántara Ortíz Rocío Aremi
Blancas Tokunaga Marco Antonio
García González Alejandra
García Vázquez David Arturo
Guzmán Cruz Angélica
Maldonado Rodríguez Alan
Quintanar García Montserrat

INDICE

Cifrados Clásicos

Cifrado de César.

El cifrado de César es uno de los primeros métodos de cifrado conocidos. Históricamente, Julio César lo usó para enviar órdenes a sus generales en los campos de batalla. En general, consistía en escribir el mensaje con el alfabeto utilizado comúnmente que estaba formado por las letras del mismo alfabeto latino normal desplazadas tres posiciones a la derecha (*fig. 1)*. Mostrando nuestro abecedario actual (considerando el americano de 26 caracteres), el cifrado César puede también utilizarse como un recurso de encriptación sencillo.

Abecedario original.	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z
	↓ Al aplicar el cifrado.																									
Abecedario cifrado.	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C

Fig. 1

Ahora que se vio la aplicación del cifrado (que fue el recorrer el abecedario tres espacios a la derecha), veamos un ejemplo sencillo (*fig. 2)*. Es necesario aclarar que los mensajes no deben incluir espaciado, ya que eso implicaría añadir otro carácter al – en este caso – abecedario; es decir, incluir el carácter de "espacio" que se incluiría para el recorrido de todos los símbolos de nuestro conjunto de caracteres a cifrar.

Mensaje original.	A	T	A	C	A	R	A	L	A	M	A	N	E	C	E	R
	↓ Al cifrar el mensaje.															
Mensaje cifrado.	D	W	D	F	D	U	D	O	D	P	D	Q	H	F	H	U

Fig. 2

Se puede observar, que al analizar detenidamente el ejemplo (*fig. 2)*, puede ser descifrado fácilmente haciendo el desplazamiento inverso con cada letra del mensaje (que se mostrara en lenguaje matemático su forma de cifrar y descifrar en las siguientes páginas). Aunque para el resto de la gente que incidentalmente pudiese llegar a ver el mensaje cifrado carecerá de sentido para estos.

Además de esto puede notarse que el cifrado es inseguro – por su facilidad para descifrar -, pero en la época de Julio Cesar este encriptado era confidencial y poco común que la población en general tuviera conocimiento de lo que pudiera ser un "cifrado".
Es importante mencionar que 1500 años después, un cifrado similar al de Julio Cesar fue utilizado por la reina María Estuardo de Escocia, para conspirar junto con los españoles contra su prima Isabel I (en realidad, fue incitada a conspirar por agentes al servicio de Isabel I). Los mensajes cifrados de María fueron fácilmente descencriptados mediante sencillos análisis estadísticos por los agentes de Isabel I y así quedó al descubierto la conspiración de la reina escocesa siendo ejecutada el 8 de Febrero de 1587. Después de esto, el cifrado de Cesar quedo definitivamente descartado como método de encriptado seguro para los gobernantes del mundo. Al día de hoy, los cifrados usados por los Estados para preservar sus secretos han mejorado considerablemente[1].
Los fundamentos matemáticos del cifrado de César son una aplicación de la aritmética modular; la cual está determinada por la siguiente función (*fig. 3*) (de igual forma se hará instancia del dominio, condominio y regla de correspondencia).

Definición. *Sea* Σ *un alfabeto. Un esquema de cifrado o criptosistema es una quintupla* $(M, \Gamma, K, E, \Delta)$, *donde*:

- M, *conocido como el espacio de mensajes, es el conjunto de posibles mensajes que se pueden fomar con los caracteres del alfabeto* Σ.
- Γ, *el espacio de mensajes cifrados, es el conjunto de todos los posibles mensajes cifrados.*
- K, el espacio de llaves, es el conjunto de todas las posibles llaves.
- $E = \{E\kappa : \kappa \in K\}$ *es una familia de funciones* $E\kappa : M \to \Gamma$ *en la que cada elemento se llama* función de cifrado.
- $\Delta = \{\Delta\kappa : \kappa \in K\}$ *es una familia de funciones* $\Delta\kappa : \Gamma \to M$ *en la que cada elemento se llama* función de descifrado.
- *Para cada* $\varepsilon \in K$, $\exists \delta \in K$ *tal que* $\Delta\delta(E\varepsilon(\mu)) = \mu \quad \forall \mu \in M$.

Fig. 3

Una vez vista la definición general, en nuestro caso particular del abecedario original, se tiene el siguiente enunciado (*fig. 4*).

A cada letra del alfabeto español se le asigna un número entero según su posición en el alfabeto.
Por lo que el espacio de mensajes es $M = \{0,1,\dots,26\}$, *el espacio de mensajes cifrados o criptogramas es* $\Gamma = \{0,1,\dots,26\}$ *y el espacio de llaves es* $K = \{0,1,\dots,26\}$. *Por ultimo, las funciones de cifrado y de descifrado quedan*

[1] Kahn, David: *The Codebreakers.* La "Biblia" de las cifras y códigos. Un exhaustivo análisis de la historia de la criptografía, desde el antiguo Egipto hasta la década de los 60's, en casi 1200 páginas. Una nueva edición en 1997 añade un capitulo que resume las novedades de los últimos años.

Ahora, si se modifica la clave secreta, es decir, el alfabeto original y los lugares que recorre cada letra, se modificaría la función en el sentido del conjunto al cual estemos inmersos cambiaria dependiendo el número de caracteres que tenga el alfabeto. Además, la operación utilizada en la función también cambiaria dependiendo de los lugares que desplazamos cada letra y hacia dónde. De forma general:

$$f(x) \equiv (x + n) \; mod \; s$$

donde:

- "x" es el número correspondiente a la letra del alfabeto original,
- "n" es el número de lugares desplazados (con la aclaración de que "n" estaría en $\mathbb{Z}$ en caso de que los lugares se recorren hacia la izquierda)
- "s" es el número de caracteres en el alfabeto original.

Además de esto para poder encriptar y desencriptar un mensaje la función de cifrado debe ser biyectiva con el propósito de evitar errores ya que la codificación y decodificación de un mensaje debe ser única. Para que la función sea biyectiva debe cumplir los siguientes requisitos:

- No puede haber dos letras en el abecedario original que tengan la misma transformación para el código.
- No puede haber letras en el abecedario original que no tengan su transformación en el código.
- No puede haber letras del código que no se correspondan con alguna letra del abecedario original.

Una vez visto este pequeño análisis acerca de las condiciones necesarias, consideraremos un ejemplo sencillo.
Se tiene la siguiente tabla (*fig. 6*). Es importante volver a mencionar que el orden que se tomará el abecedario debe ser estricto para la codificación.

A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S
1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19
T	U	V	W	X	Y	Z	.	:	;	,	¿	?	¡	!	(	)	“	”
20	21	22	23	24	25	26	27	28	29	30	31	32	33	34	35	36	37	38

Fig. 6

La clave secreta que se va a utilizar será mover dos espacios hacia atrás cada símbolo. De modo que la función correspondiente para encriptar será:

$$f(x) \equiv x - 2 \; \; mod \; 38$$

Por ejemplo, si consideramos el símbolo A, al cual se le fue asignado el número 1, entonces:

$$f(1) \equiv (1 - 2) \; mod \; 38$$

$$\Rightarrow f(1) = (-1) \mod 38$$
$$= 37$$

Esto quiere decir que el símbolo **A** será encriptada a la posición 37, es decir el símbolo **"**.
Ahora, la función que servirá para desencriptar será $f^{-1}(x)$, en este caso:

$$f^{-1}(x) \equiv (x + 2) \mod 38$$

Por ejemplo, si tenemos un símbolo encriptado con el símbolo **J**, y observamos que este símbolo tiene asignado el número 10 *(fig. 6)*, lo que quiere decir que:

$$f^{-1}(10) \equiv (10 + 2) \mod 38$$
$$\Rightarrow f^{-1}(x) \equiv (12) \mod 38$$

Lo que implica que el símbolo desencriptado corresponde al carácter de **L**. Muy bien

Textos Cifrados (y su descifrado).

A continuación veremos dos textos que se encuentran cifrados con el encriptado de César; el primero, que fue el asignado por la ayudantía de la clase y el segundo que es un texto de libre albedrio.

Texto Cifrado

Sainu ky ru wak yk ng kyixozu gikxig jk ruy vrgikxky e ruy yalxosoktzuy jkr uvou. Ruy ´edzgyoy e nuxxuxky jk Jk Waotike e ruy vgxgjoy gxzoloiokry jk Hgajkrgoxk yut iutykxbgjuy k otzkxvxkzgjuy iut zgr gxzk wak ruy ngik otsuxzgrky, e kr satju iutuik g lutju rg hkrrkfg, kr zkxxux e kr soyzkxou jk kyuy uyiaxuy xkotuy jutjk kr yu¯ngjux ky zxgtyvuxzgju. Vkxu gatwak sainu ky ru wak yk ng nghrgju, totm´ut nushxk ng uygju zujgb´ıg jkzgrrgx rg tgzaxgrkfg jk ruy lgtzgysgy wak ktzutiky yk xkbkrgt kt rg sktzk, u jk yamkxox rg joxkiio´ot jk ruy otgajozuy igsotuy vux iaeu gjuxtgju e kd´ozoiu iaxyu yk bk oxxkyoyzohrksktzk rgtfgju kr gjoizu. Kr iguy xkvzgtzk N.V. Rubkixglz e Krofghkzn Hkxqkrk.

$$f(x) \equiv (x - 6)$$

Texto Descifrado

Mucho es lo que se ha escrito acerca de los placeres y los sufrimientos del opio. Los éxtasis y horrores de De Quincey y los *paradis artificiels* de Baudelaire son conservados e interpretados con tal arte que los hace inmortales, y el mundo conoce a fondo la belleza, el terror y el misterio de esos oscuros reinos donde el soñador es transportado. Pero aunque mucho es lo que se ha hablado, ningún hombre ha osado todavía detallar la naturaleza de los fantasmas que entonces se

Programa implementado para el criptado de César.

Para facilitar un poco más la forma de utilizar el encriptado de César, se implementa el siguiente programa, haciendo los comentarios necesarios.

```
package cifradodecesar;
import java.util.Scanner;
public class CifradoDeCesar {
public static void main(String[] args) {
Scanner tec= new Scanner(System.in);
    String frase1, frase2;
    int clave;          /* variable de desplazamiento */
    frase2="";          /* mensaje cifrado */
    String min= "abcdefghijklmnopqrstuvwxyz";
    String may ="ABCDEFGHIJKLMNOPQRSTUVWXYZ";
    System.out.println("Introduce una frase : ");
    frase1= tec.nextLine();
    System.out.println("Introduce tu clave: ");
    clave = tec.nextInt();
    for(int i=0; i< frase1.length(); i++){  /* recorre la frase 1 */
      for(int j=0; j< min.length(); j++){  /* recorre cada una de las letras y las
comparamos con                                    los
abecedarios */
          if(frase1.charAt(i)== min.charAt(j)){  /* .charAt nos devuelve el valor
char del índice. */
           if(j + clave >= min.length()){          /* permite darle vueltas al
alfabeto */
              frase2 += min.charAt((j + clave) % min.length());  /* 40 % 25= 15 */
           }
           else{
              frase2 += min.charAt(j + clave);
           }
          }
          /* análogo para el otro alfabeto */
          else if(frase1.charAt(i)== may.charAt(j)){
           if(j + clave >= may.length()){
              frase2 += may.charAt((j + clave) % may.length());
           }
            else{
              frase2 += may.charAt(j + clave);
            }
          }
      }
    }
    System.out.println(frase1);
    System.out.println(frase2);
} }
```

Textos Cifrados (y su descifrado).

A continuación veremos un texto que se encuentra cifrado con el encriptado de decimado, el cual fue asignado por la ayudantía de la clase (*fig. 10*). Primero se propondrá la siguiente encriptación:

Abecedario a cifrar									
a	á	b	c	C	d	e	f	g	h
0	1	2	3	4	5	6	7	8	9
i	í	j	k	l	m	n	ñ	o	ó
10	11	12	13	14	15	16	17	18	19
P	q	r	s	t	u	v	w	x	y
20	21	22	23	24	25	26	27	28	29
z	:	,	-	!	¡	U	Q		
30	31	32	33	34	35	36	37		

Función

$$f(x) \equiv (3x) \mod 38$$

$$\Rightarrow mcd(37,3) = 1$$

$$\Rightarrow 37 = 3(12) + 1$$

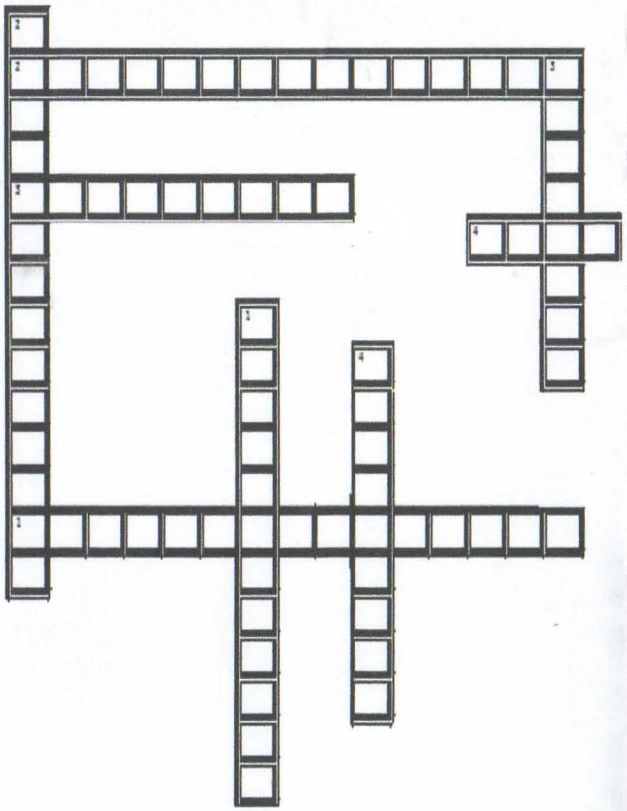
$$\Rightarrow 3 = 1(3) + 0$$

Abecedario cifrado									
a	á	b	c	C	d	e	f	g	h
a	c	e	h	j	m	o	q	t	w
i	í	j	k	l	m	n	ñ	o	ó
z	-	U	á	C	f	i	k	n	ó
p	q	r	s	t	u	v	w	x	y
r	u	x	:	!	Q	b	d	g	í
z	:	,	-	!	¡	U	Q		
l	ñ	p	s	v	y	,	¡		

Fig. 10

En la actualidad la criptografía ha pasado de ser una actividad reservada y exclusiva a convertirse en una necesidad del mundo moderno, la criptografía forma parte de la vida cotidiana. Con el uso de la computadora, y más aún con la llegada de Internet, fue indispensable el uso de herramientas automatizadas para la protección de archivos y otro tipo de información almacenada en la computadora, algunas de estas herramientas son los cortafuegos, los Sistemas Detectores de Intrusos y el uso de sistemas criptográficos .

Se ha vuelto tan importante el cifrado en empresas como Apple y Google, en sus últimos sistemas operativos han incorporado el cifrado de datos.

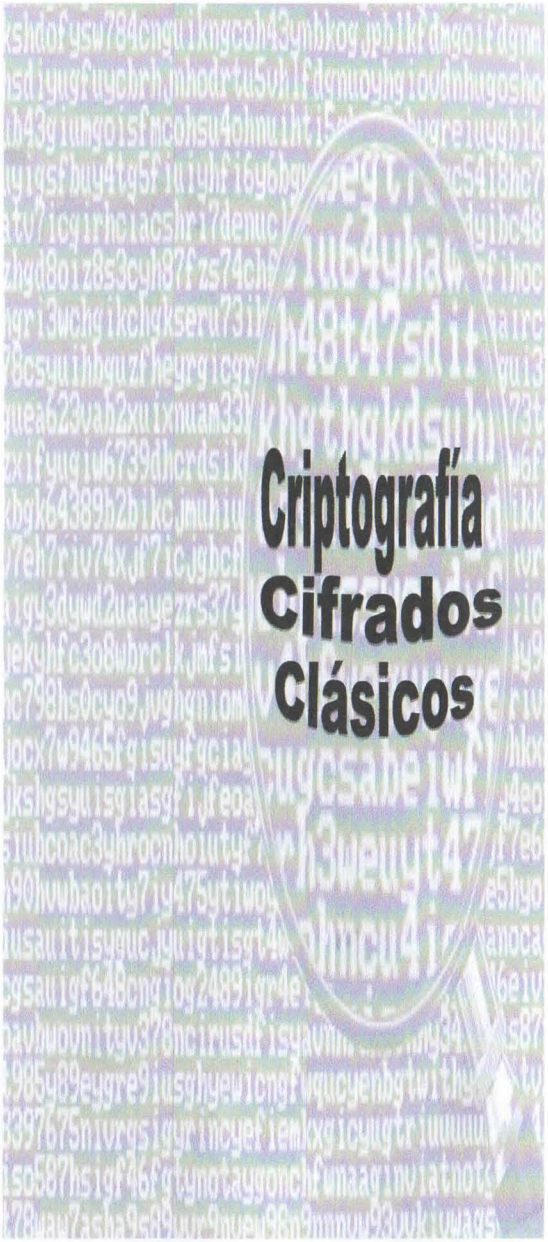


VERTICA L

1.-Ciencia que se encarga de descifrar mensajes .
2.- Mezcla la transposición y permutación.
3.-Es una de las cuatro condiciones para el cifrado de César.
4. Para poder encriptar y desencriptar se debe cumplir con que la función sea_____.

HORIZONTAL

1.-Para este método de cifrado se debe cumplir que en su función para encriptar sus componentes "n" y "s" sean primos relativos.
2.-Actualmente la criptografía forma parte de_____.
3.- Etapa de la historia en que desaparece la criptografía.
4.-Éste cifrado hereda las mismas condiciones que el cifrado Decimado y César.



Equipo Pichones

Universidad Nacional Autónoma de México

Facultad de Ciencias

Proyecto de Investigación

Criptografía

Equipo 2^3

Aguirre Pessina María Ximena

Cabrera Ramírez Gabriel Omar

Córdova Amezcua Pamela

Dosal Trujillo José Alejandro

Freyre Mendoza Raúl

Nazará Sosa Emilio Ayub

Santillán Aparicio Eluid Daniel

Zúñiga Pérez Diana Belén

16 de mayo del 2016.

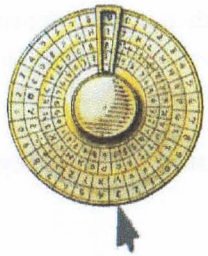
Apéndice

Evolución de la criptografía (método sustitución)

1. Atbash

2. Cifrado de Cesár

3. Cifrado de Alberti



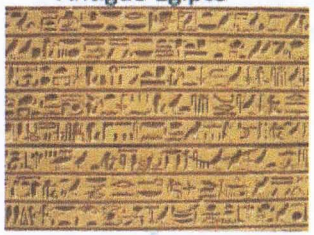
de

4. Cifrado de Vigenere

5. Cifrado Vernam

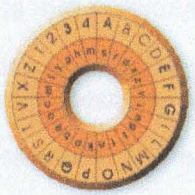
Cifrados relevantes para el desarrollo de los métodos de criptografía.

a. Jeroglíficos Antiguo Egipto



b. Escítala Espartana

c. Tablero Polybio



d. Cifra Playfair

e. Máquina Enigma

Aportaron en la historia al Cifrado

a. En Antiguo Egipto los jeroglíficos se toman como los primeros ejemplos de "escritura oculta".

b. Alrededor del año 400 a.C. los espartanos se enviaban mensajes ocultos entre tropas militares, ellos utilizaban una de las primeras prácticas que se conocen de criptografía, llamada Escítala Espartana.

   La Escítala consistía una vara de madera en el que se enrollaba una tira de cuero. Sobre esta tira se escribía el mensaje que se quería ocultar en columnas paralelas al eje del palo. Al desenrollar la tira se muestra un texto aparentemente incoherente con el texto inicial, pero que puede leerse volviendo a enrollar la tira sobre un palo del mismo diámetro que el primero. Así, si el mensajero era interceptado, el mensaje que se encontraba era una serie de caracteres incomprensibles.

c. En el siglo II a.C., el historiador Polybio ideó un código que se basaba en un tablero conocido como "Tablero de Polybio". Así si se quiere cifrar un mensaje se sustituye cada una de las letras que lo forman por el par de letras que le corresponden en el tablero (fila, columna)

d. En el siglo XIX Thomas Jefferson inventó el cilindro o rueda de Jefferson, es compuesto por 26 discos de madera que giran libremente alrededor de un eje central de metal. Las veintiséis letras del alfabeto son inscritas aleatoriamente en la superficie más externa de cada disco de modo que, cada uno de ellos, posea una secuencia diferente de letras. Girándose los discos puédese obtener los mensajes.
e. En 1917 Gilbert Vernam inventó un cifrado basado en un sistema de sustitución a través de un alfabeto binario llamado Libreta de un solo uso.

Cifrados importantes a lo largo de la historia.

1. La Biblia hace referencias al Atbash, un sistema de sustitución de letras que se usaba para cifrar mensajes y que se remonta al año 600 a.C.
2. En el año100 a.C. surge otra aplicación de la criptografía, el primer cifrado por sustitución empleada por el emperador de Roma, Julio César durante la Guerra de Galias, en el que el emperador señala que envió un mensaje al General Cicerón cambiando letras latinas por griegas. Posteriormente, ideó un cifrado simple al que llamó "Cifrado César"
   La técnica utilizada para cifrar un mensaje en el "Cifrado César" era sustituir cada una de las letras del mensaje por aquella que ocupaba tres posiciones más en el alfabeto.
3. En la época del Renacimiento (Siglo XV) Leon Battista Alberti trabajo en un cifrado polialfabético y desarrollo un sistema de codificación mecánico (basado en discos) conocido como el cifrado de Alberti.

Clave Secreta: desplazamiento de 8 posiciones en el alfabeto

Título: Inmortalidad. Autor: Amado Nervo. **No, no fue tan efímera la historia de nuestro amor: entre los folios tersos del libro virginal de tu memoria, como pétalo azul está la gloria doliente, noble y casta de mis versos.** **No puedes olvidarme: te condeno a un recuerdo tenaz. Mi amor ha sido lo más alto en tu vida, lo más bueno; y sólo entre los légamos y el cieno surge el pálido loto del olvido.** **Me verás dondequiera: en el incierto anochecer, en la alborada rubia, y cuando hagas labor en el desierto corredor, mientras tiemblan en tu huerto los monótonos hilos de la lluvia.** **¡Y habrás de recordar! Esa es la herencia que te da mi dolor, que nada ensalma. ¡Seré cumbre de luz en tu existencia, y un reproche inefable en tu conciencia y una estela inmortal dentro de tu alma!**	"Vw, vw ncm biv mníumzi ti pqabwzqi lm vcmabzw iuwz: mvbzm twa nwtqwa bmzawa lmt tqjzw dqzwqvit lm bc umuwzqi, kwuw xmbitw ihct mabi ti wtwzqi lwtqmvbm, vwjtm g kiabi lm uqa dmzawa. Nw xcmlma wtdqlizum: bm kwnlmvw i cv zmkcmzlw bmvih. Uq iuwz pi aqlw tw uia itbw mv bc dqli, tw uia jcmvw; g aótw mvbzm twa tmwiuwa g mt kqmvw aczwm mt xitqlw twbw lmt wtdqlw. Um dmzia lwvlmycqmzi: mn mt qvkqmzbw ivwkpmkmz, mv ti itjwzili zcjqi, g kcivlw piwia tijwz mn mt lmaqmzbw kwzzmlwz, uqmnbzia bqmujtiv mv bc pcmzbw twa uwvóbwnwa pqtwa lm ti ttcdqi. ¡G pijzia lm zmkwzliz! Mai ma ti pmzmvkqi ycm bm li uq lwtwz, ycm vili mvaitui. ¡Amzm kcujzm lm tch mn bc mfqabmvkqi, g cv zmxzwkpm qvmnijtm mn bc kwvkqmvkqi g cvi mabmti qvuwzbit lmvbzw lm bc itui!"

Decodificación del texto indicado, se adjunta *clave secreta*.

Clave secreta: Desplazamiento de 6 posiciones en el alfabeto.

Método para descifrarlo: Nos percatamos de que había letras dobles en el texto (rr,xx) y en el lenguaje castellano solo existen "rr" y "ll" como letras dobles, "rr" no podía ser igual a "rr", entonces "ll" debía ser "rr"; la distancia de "l" a "r" son 6 caracteres, igual de "r" a "x", proponiendo esa clave como la correcta, solo aplicamos la inversa, desplazándonos 6 a la izquierda en el cifrado César.

¿Qué pasa si todos los equipos juntan su texto desencriptado?: Obtendríamos la mayor parte del texto "El caos Reptante" de Lovecraft , al primer equipo le tocó aproximadamente un párrafo del texto, al siguiente equipo la continuación y así hasta aproximadamente tres cuartas partes del texto de Lovecraft; por cierto

Demostración: Consideremos las funciones:

$$h(m)=m+b \bmod n$$ (Cifrado César)

$$g(m)=am \bmod n$$ (Cifrado Decimado)

Si realizamos la composición de estas dos funciones obtenemos:

$$h(g(m))=(am)+b \ mod \ n$$

P.D. h∘g es biyectiva
Sabemos que h es biyectiva y como mcd(a,n)=1 g también lo es, en particular son *inyectivas*

$$Entonces \ a=b \rightarrow h(a)=g(b) \ y \ g(a)=g(b)$$

$$Entonces, se \ cumple \ a=b \rightarrow \ g(a)=g(b) \rightarrow h(g(a))=h(g(b))$$

Por lo tanto es *inyectiva*.
También h y g son suprayectivas y

$$h:Z \rightarrow Z \quad y \quad g:Z \rightarrow Z$$

Y tenemos que para todo **x** en Z existe un **y** también en Z tal que h(y)=x
Y para todo **y** en Z existe un w también en Z tal que g(w)=y

Tenemos que

$$h \ o \ g:Z \rightarrow Z$$

Entonces por lo anterior, para todo **x** en Z existe un **y** para el que existe un **w** tal que h(y)=x -> h(g(w))=x
Por lo tanto, es *suprayectiva*.
Por lo tanto es *biyectiva.*

Como se probó que este método es *biyectivo*, entonces debe existir una *función inversa* para descifrar un texto.
Notemos que si renombrados a f(m) como c, tenemos la ecuación

$$c=(am+b) \bmod n$$

Si despejamos c de esta ecuación, obtenemos:

$$m=(c-b)a^{-1} \bmod n$$

Proponemos la función:

$$f(c)=(c-b)a^{-1} \bmod n$$

Para ser la función que desencripte un texto.

Nota: no se debe confundir a^{-1} con 1/a, en este caso a^{-1} representa el inverso multiplicativo en aritmética modular, esto es:

$$(a \cdot a^{-1}) \bmod n = 1$$

Ejemplo: Consideremos el texto que encriptamos anteriormente SIPISAL. Y supongamos que conocemos la clave a=5

CÓDIGO DE ENCRIPTACIÓN

ORIGINAL																								
A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z
CÓDIGO																								
M	T	A	H	O	V	C	J	Q	X	E	L	S	Z	G	N	U	B	I	P	W	D	K	R	Y	F

y b=8Asignamos a cada letra su valor numérico correspondiente:

S	I	P	I	S	A	L
18	8	15	8	18	0	11

Se sustituye cada número en la función anterior.
Es este caso $a^{-1}=21$

(S)	(18-8)(21) mod 26 =2	(C)
(I)	(8-8)(21) mod 26 =0	(A)
(P)	(15-8)(21) mod 26 =17	(R)
(I)	(8-8)(21) mod 26 =0	(A)
(S)	(18-8)(21) mod 26 =2	(C)
(A)	(0-8)(21) mod 26 =-12 => 14	(O)
(L)	(11-8)(21) mod 26 = 11	(L)

2	0	17	0	2	14	11
C	A	R	A	C	O	L

Vemos que efectivamente obtuvimos la palabra encriptada.

Se puede ver que en algunos casos pueden resultar números negativos, en estos casos le sumamos n al número obtenido para obtener el resultado correcto, en el ejemplo anterior al ser n=26 se le sumó 26 a -12 para obtener el resultado correcto que es 14.
Esto se debe a cómo funcionan las congruencias modulares, se tiene que si

$$m \equiv (c-b)a^{-1} \bmod n$$

también lo es

$$m \equiv (c-b)a^{-1}\ (n+(c-b))\ \bmod n$$

(≡ representa congruencia modular)

A continuación se presenta un ejemplo de un texto cifrado y uno descifrado utilizando el método afín, con un valor a=7, b=12.; en ambos se utilizaran estos valores

4. Algunos métodos de Criptografía moderna

A mediados del siglo XIX se hizo muy popular un sistema de criptografía donde ya no se trataría que el producto fuera un mensaje donde el orden de las letras no tiene coherencia. Parte de estos sistemas se les conocen como códigos.

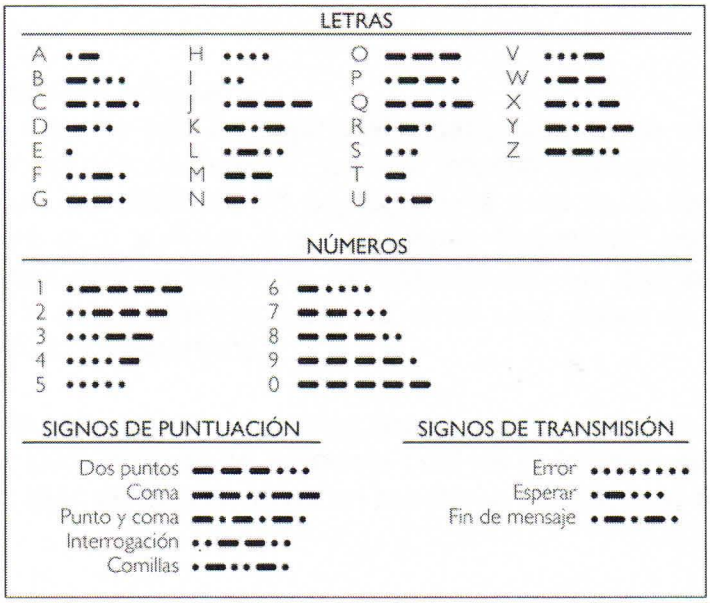
Una de las características de los cifrados clásicos es que lo que buscaban cambiar era las letras por otras letras del mismo abecedario. En términos más formales; esto se escribiría como f:E→E donde E es el sistema de escritura y f es la función encriptar el mensaje, y sí x∈**E** entonces x es una letra.

En los códigos el modo de encriptar era de otra naturaleza, consistía en tener miles de frases, palabras, sílabas o letras y asociar un conjunto de números, símbolos, palabras e incluso frases diferentes a cada una de ellas, a este nuevo conjunto se le llama Grupo código.

Ejemplos:

- Los códigos de radio militares, su grupo código es un código numérico, si se mandaba "77" esto querría decir "mantenerse alerta". Análogamente todos los códigos que se usan para la policía bomberos y paramédicos que tanto se escuchan en las películas adoptan este estilo.

- El código morse; en este el alfabeto tiene asociado un pequeño conjunto de rayas y puntos los cuales tienen un significado rítmico donde un punto es un golpeteo rápido y una raya un tiempo más largo, llegaron con la invención del telégrafo gracias a Samuel Morse en el siglo XIX.



Curiosamente también fue creado en estados unidos el "Acme Comodity Phrase and Code" el cual era un libro donde le asignan a 100000 frases comunes un

Se tienen dos sujetos los cuales quieren mandar un mensaje por un medio inseguro, en los sistemas clásicos, conocer la llave para cifrar el mensaje era el mismo para poder descifrarlo, entonces se necesita una llave para cifrar el mensaje y otra para descifrarlo, a este tipo de criptografías se les llama asimétricas, aun así hay criptografías asimétricas donde conocer la llave proporciona toda la información necesaria para conocer la llave de descifrado, el cifrado de llave pública tendría que ser uno donde la llave es conocida pero no da la información suficiente para conocer la llave de descifrado; al existir una criptografía de este estilo suceden cosas muy curiosas.

- Todas las sujetos del sistema poseen los medios necesarios para cifrar mensajes y descifrar los mensajes que son para ellos con su propia llave secreta

- Para todos es muy difícil obtener en un tiempo razonable las llaves secretas de los demás

4.1.1. Logaritmo discreto

Es la base de este tipo de sistema, se observó que hay procesos fáciles hacía una dirección, y el inverso se vuelve difícil, el logaritmo discreto es uno de ellos; sea Zp con **p** primo, entonces Zp es un campo finito, elevar números a una potencia en un campo finito es fácil.

Pero la pregunta ¿a qué número se debe elevar x para que de y en Zp? Ya no tiene una respuesta fácil, el problema se vuelve tanto más grande cuando el tamaño del campo aumenta.

En los reales, la pregunta tiene solución siempre que el argumento y la base sean positivos, pero en Zp puede incluso que la pregunta no tenga solución, por ejemplo:

$$3^x=7 \bmod 13 \text{ no tiene solución}$$

¿Pero cómo utilizar el logaritmo discreto si se quiere encriptar letras?

Mediante un código numérico por el cual se pueda asociar a cada letra un número, así como en las computadoras se asocia un código binario o un código ASCII, de este modo la palabra Hola, se leería 484F4C41 en sistema hexadecimal, de esta manera se logra una conversión de palabras a números, y principalmente el método de llave pública es un método computacional.

Existen maneras complicadas para que dados dos sujetos que se quieren comunicar, obtengan una llave común para descifrar sus mensajes, la cual esté relacionada con sus llaves secretas, sin que ninguno conozca la llave del otro, si hubiera un tercero que hubiera presenciado todo, para obtener el descifrado del mensaje el sujeto tendría que resolver el logaritmo discreto en un campo muy

grande, y en cuyo caso un programa de computadora tardaría mucho, cabe destacar que ya se conocen números primos tan grandes, uno el cual tiene más de 22 millones de dígitos, donde tratar de resolver este problema en un campo de ese tamaño se vuelve una tarea humanamente imposible.

No sobra mencionar que este no es uno de los sistemas de encriptado más complejos que existan, en conclusión, la humanidad ha llegado a una gran complejidad a la hora de esconder un mensaje, y de una elegancia tal que la manera de esconderlo puede ser conocido pero aun así tratar de conocer el mensaje se convertiría en una tarea irresoluble comparado con la capacidad humana.

Conclusiones

Conclusiones

En base al objetivo de este proyecto se puede observar que los métodos de cifrado han evolucionado a la par con la humanidad desde el antiguo Egipto hasta la actualidad y seguirá desarrollándose de acuerdo a las necesidades del hombre.

Los cifrados han tenido una evolución constante debido a que el ser humano tiene la necesidad de transmitir de una forma eficaz y segura su información, llegando a la época en la que la sociedad se desarrolla actualmente donde el manejo de datos y el intercambio de información es más rápido y sencillo provocando que esta esté al alcance de cualquiera; debido a esto, los cifrados tienen que ser modificados y cada vez son más complejos permitiendo así que la información sólo pueda ser vista por el emisor y por la persona a la que está dirigida sin temor a que un tercero pueda acceder a ella.

A lo largo de esta investigación se puede notar que a la par con los métodos para encriptar se han ido también desarrollando las maneras para descifrar la información; de ahí que se tenga la necesidad de ir modificando los cifrados. Mientras no se encuentre una fórmula general para encontrar primos, los cifrados actualmente utilizados seguirán siendo eficaces; sin embargo en un futuro se prevé que las formas de encriptar no sólo se van a basar en cifrados

FACULTAD DE CIENCIAS

UNIVERSIDAD NACIONAL AUTÓNOMA DE MÉXICO

"UNA INTRODUCCIÓN GENERAL A LA CRIPTOGRAFÍA"

PROYECTO FINAL

ÁLGEBRA SUPERIOR II

Autores: André Daniel Navarrete Escobedo

Celia Concepción Hueto Pérez

Elmer Tovar Acosta

Silvestre Calderón Román

Introducción:

La necesidad del ser humano por comunicarse en secreto nos ha seguido desde tiempos ancestrales aumentando su campo de acción en cada conflicto bélico y diferencia diplomática. Con nuestro historial tan desafortunadamente grande de guerras y guerrillas calientes y frías no es de extrañarse que la criptografía haya evolucionado de manera tremenda, tanto que los cifrados antiguos parecen (y a veces son) juegos de niños.

El objetivo primordial de éste material es proporcionarle al lector una visión generalizada de cómo se sucedieron estos procesos, así como la aplicación práctica de cada uno de ellos. Siempre intentando cuidar y mantener claro el punto de vista matemático.

Es un trabajo generado de estudiantes para estudiantes, esperando que quienes quieran sumergirse en el mar del conocimiento criptográfico encuentren en el presente texto un buen remojón de pies con el que empezar a tentar las aguas.

Sin embargo, como mencionamos anteriormente, el proyecto tendrá un enfoque matemático, razón por la cual es necesario introducir conceptos y demostraciones, si el lector es aficionado a las matemáticas pero no desde el punto de vista formal encontrara en las primeras páginas de nuestro texto una gran introducción a las demostraciones matemáticas, algo que para muchos es difícil de asimilar en primera instancia, pero si el lector no entra en esta categoría o es de esas personas que sienten cierto odio a la materia no hay razón para preocuparse, gran parte del contenido matemático, y por esta gran parte nos referimos a las demostraciones, puede ser colocado en segundo término, en particular las primeras páginas que parecerán sofocantes a primera vista pero no son más que resultados sencillos puede ser revisada solo por encima leyendo los conceptos para así poder entrar al tema principal del trabajo, la criptografía.

Antecedentes:

Nociones de criptología

La criptología (del griego krypto y logos, significa estudio de lo oculto) es la ciencia que trata los problemas teóricos relacionados con la seguridad en el intercambio de mensajes en clave a través de algún canal de comunicaciones.
Esta ciencia se divide en dos ramas: La criptografía, ocupada del cifrado de mensajes en clave y del diseño de criptosistemas, y el criptoanálisis, que trata de descifrar los mensajes, de romper el criptosistema. Cuando hablamos de criptografía hablaremos de dos textos, el original al o texto claro, y del texto cifrado o en clave.

La estenografía por su parte trata de ocultar la existencia del mensaje, es decir que no importa que todos puedan leerlo siempre y cuando solo el destinatario será capaz de comprenderlo. Esta es la principal diferencia entre estenografía y criptografía.

Un poco antes mencionamos el término "criptosistema" que no es más que una quíntupla de siglas (P, C, K, E, D). Donde se cumplen las siguientes condiciones:

1. P es el conjunto de todos los posibles textos claros.
2. C es el conjunto de todos los posibles textos cifrados.
3. K es el conjunto de todas las claves que podemos utilizar.
4. E es el conjunto de funciones de encriptado, e: P→C para cada e en E, las cuales deben ser biyectivas.
5. D el conjunto de funciones para des encriptar, d: C→P para cada d en D.

Para cada clave en K existe una función de encriptado e_k en E y una de des encriptado d_k en D tales que $d_k(e_k(x)) = x$ para cada x en P, en otras palabras, son funciones "inversas".

En esta sección de criptografía clásica, trabajaremos con dos tipos de cifrados en los que con facilidad se abarcan la gran mayoría de los cifrados de la época: Transposición y sustitución.
En los cifrados por sustitución tenemos que cada una de las letras del mensaje tiene una correspondencia fija en el mensaje cifrado, ejemplos de este son el método de Polybios, o el cifrado de César.
Mientras que en los cifrados por transposición las letras simplemente cambian de sitio, por lo que las letras del texto cifrado son las mismas que las del texto claro.

Definición: Sean a, b en Z_n decimos que b es el inverso de a si y solo si

$$ab \equiv 1 \, mod \, n$$

Afirmación: Sea x en Z_n, x tiene inverso multiplicativo en Z_n si y solo si $mcd\ (x,n)\ = 1$

Demostración: Supongamos "x" tiene inverso multiplicativo en Zn es decir existe "y" en Z_n tal que
$xy \equiv 1 \, mod \, n$ Por definición de congruencia
$n|xy - 1$ Por definición de "dividir a" existe un s en Z tal que
$ns = xy - 1$ Es equivalente a
$xy - ns = 1$ y esto nos implica $mcd(x,n) = 1$

Ahora supongamos $mcd(x,n) = 1$
Entonces existen s,t en Z tales que $xs + nt = 1$ de donde
$nt = 1 - xs$ Entonces
$n|1 - xs$ por definición de congruencia
$xs \equiv 1 \, mod \, n$ Por definición de inverso multiplicativo s es inverso multiplicativo de x en Z_n.

Afirmación: El inverso es único.

Demostración:
Supongamos a, b, x en Z_n tales que
$ax \equiv bx \equiv 1 \, mod \, n$
$ax \equiv bx \, mod \, n$ Por definición de congruencia
$n|ax - bx$
$n|x(a - b)$ pero $mcd\ (x,n)\ = 1$ por lo tanto $n|a - b$ y por definición de congruencia
$a \equiv b \, mod \, n$

Entonces ya tenemos la función, solo habría que dar ciertas reglas de tal manera que la función sea biyectiva y no haya problemas al descifrar.

Si a = 2 tenemos:

Original	a	b	c	d	e	f	g	h	i	j	k	l	m	n	o	p	q	r	s	t	u	v	w	x	y	z
Cifrado	a	c	e	g	i	k	m	o	q	s	u	w	y	a	c	e	g	i	k	m	o	q	s	u	w	y

Aquí el problema es que en determinado momento se vuelven a repetir las letras, por ejemplo en el alfabeto original a la b le toca la c pero también a la o, es decir la función no es biyectiva, por lo que no nos sirve para cifrar mensajes. Cabe destacar que: $mcd\ (2,26) = 2$

Ahora si a = 3 tenemos:

Ejercicio de cifrado:

Teniendo la regla para saber si nos sirve el cifrado o no, proponemos el valor de "a" como 5. Como $mcd\ (5, 26) = 1$ entonces, según nuestro criterio debería funcionar para cifrar el mensaje:

Original	a	B	c	D	e	f	g	H	i	j	k	l	m	n	o	p	q	r	s	t	u	v	w	x	y	z
Cifrado	a	F	k	P	u	z	e	J	o	t	y	d	i	n	s	x	c	h	m	r	w	b	g	l	q	v

Ahora notemos que $21 * 5 = 105$ y además $105 = 26 * 4 + 1$ por lo que $105 \equiv 1\ mod\ 26$, en otras palabras 21 es el inverso multiplicativo de 5 en Z_{26}, con los resultados anteriores tenemos que nuestra congruencia para descifrar es: $x = 21y\ mod\ 26$.

La función es biyectiva, por lo que podemos proceder a cifrar el texto dado:

Allí se escondió él mismo y se puso a rondar y a acechar. Pronto llegaron corriendo las perdices, encontraron el grano y se fueron metiendo en el saco una detrás de otra. Cuando ya había una buena cantidad dentro el gato tiró de la cuerda, cerró el saco corriendo hacia allí y les retorció el pescuezo. Luego se echó el saco a la espalda y se fue derecho al palacio del rey.

Ese texto, queda cifrado como:

Addó mu umksnpos úd iomis q mu xwms a akukjah. Xhsnrs ddueahsn kshhounps dam xuhpokuh,

Unksnrahsn ud ehans q mu zwuhsn iurounps un ud maks wna purám pu srha. Kwanps qa jafóa wna

Fwna kanropap punrs ud ears rohs pu da kwuhpa, kuhhs ud maks kshhounps jakóa addó q dum hurshkos ud xumkwuvs. Dwues mu ukjs ud maks a da umxadpa q mu zwu puhukjs ad xadakos pud huq.

Cifrado Afín

El cifrado afín no es más que un caso particular de los cifrados por sustitución, a la vez que es una generalización de los cifrados vistos anteriormente.
En este cifrado restringimos nuestras funciones de encriptación a las que tienen la forma:

$$e(x) \equiv ax + b\ mod\ 26$$

Donde $0 \leq a, b < 26$
De forma más general, si nuestro alfabeto tiene n letras y cada una le asignamos un valor numérico comenzando desde el 0 las funciones tienen la forma

Si ahora tomamos su residuo módulo 26, así nuestro alfabeto original se convertiría en:

Letra	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z
Res. mod 26	1	4	7	10	13	16	19	22	25	2	5	8	11	14	17	20	23	0	3	6	9	12	15	18	21	24
L. Cód.	B	E	H	K	N	Q	T	W	Z	C	F	I	L	P	R	U	X	A	D	G	J	M	P	S	V	Y

Con esto un mensaje como: "no procrastinar más" se convierte en:

"pr uarhabdgzpba lbd"

Donde el procedimiento fue:

Para $n = 13(letra\ n)$ $13 * 3 + 1 = 40$ luego $40/26 = 26 * 1 + 14$ entonces

$$(13 * 3 + 1 \equiv 14\ mod\ 26)$$

Para o $(14 * 3 + 1 \equiv 17\ mod\ 26)$ Y procedemos de forma análoga para las demás letras.

Como mencionamos antes el módulo de la congruencia con la que trabajemos dependerá del número de elementos que tenga nuestro alfabeto, y este mismo modulo se utilizará al descifrar, proceso del que hablaremos ahora.
En nuestro ejemplo al aplicar la función a $n = 13$ obtuvimos $y = 14$, entonces para descifrar necesitamos resolver la congruencia:
$3x + 1 \equiv 14\ (mod\ 26)$ Que es equivalente a
$3x \equiv 13(mod\ 26)$
$3x \equiv 39\ (mod\ 26)$ como mcd $(3,26) = 1$ podemos dividir entre 3(multiplicar por el inv. Multiplicativo de 3)
$x \equiv 13\ (mod\ 26)$ Que efectivamente era lo que buscábamos.
Sin embargo este método no sería practico al tratar de descifrar textos largos por lo que necesitamos una manera de simplificarlo, para lo cual necesitaremos mos ciertos resultados acerca de Z_n, los cuales introducimos en la sección anterior y no son otra cosa más que las condiciones necesarias para que un x en Z_n tenga inverso multiplicativo.

Con estos resultados a la mano podemos buscar una manera sencilla de descifrar, primero escribimos

$$y \equiv ax + b\ mod\ n$$

Que es equivalente a $y - b \equiv ax\ mod\ n$
como $mcd\ (a,n) = 1$ "a" tiene inverso multiplicativo, digamos c, ahora

multiplicando en ambos lados de la igualdad
$c(y-b) \equiv (c)ax \bmod n$
$c(y-b) \equiv (ca)x \bmod n$ por definición de inverso multiplicativo
$c(y-b) \equiv x \bmod n$
Por lo que esta última congruencia es la que debemos resolver si queremos descifrar nuestro texto. En nuestro ejemplo quedaría como $9(y-1) \equiv x \bmod 26$

A simple vista pareciera que este cifrado es mucho más seguro que los cifrados de sustitución (Cesar y decimado) anteriores, esto es cierto hasta cierto punto, ya que en los cifrados que vimos anteriormente solo había 26 posibles cifrados mientras que en este contamos con 312, pero al igual que los anteriores es vulnerable a un ataque por medio de análisis de frecuencia, para darnos una idea de esto anexamos unas tablas que contienen las 5 letras más frecuentes en 3 idiomas distintos.

Ingles

Letra	Frecuencia (%)
E	12.7
T	9.1
A	8.2
O	7.5
I	7

Español

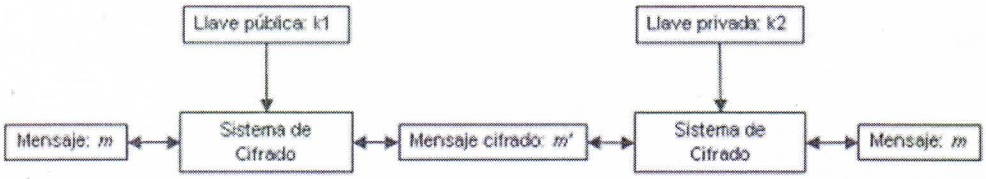
Letra	Frecuencia (%)
E	16.78
A	11.96
O	8.69
L	8.37
S	7.88

Francés

Letra	Frecuencia (%)
E	14.7
S	7.9
A	7.6
I	7.5
N	7

Criptografía Asimétrica

Usando otra vez un diagrama, se puede observar que no existe simetría alguna, de ahí obtiene su nombre este tipo de cifrado.



Lo que se hace es codificar un mensaje con una llave pública llamémosle k1, y se decodifica con la llave privada k2, esto quita el problema que había con la simétrica, pues si yo quiero enviar un mensaje a un gran número de personas, tendría que saber cada una de las llaves de estas personas, pero si esas mismas personas me quieren enviar un mensaje solo es necesario que conozcan mi llave pública, el problema que tiene este tipo es el de la autenticidad de las llaves públicas. Para solucionar este problema, lo que se puede hacer es encriptar asimétricamente la llave pública (k), es decir se usa la llave pública (k´) y una llave privada (p), así aquel que quiera decodificar y recibir un mensaje tendrá que poseer tanto la llave pública(k´) y la llave privada (p), de esta manera se prueba la autenticidad de la llave pública para codificar los mensajes.

Algunos ejemplos de este tipo de criptografía son RSA y El Gamal.

Es natural que con el desarrollo de la criptografía esta necesitara de bases matemáticas más potentes por lo que es momento de desarrollar algunos conceptos importantes en los cifrados modernos.

El pequeño Teorema de Fermat:

Si p es un número primo y p no divide a b, entonces, $p|b^p - b$

Nótese que la conclusión del teorema es equivalente a la congruencia:

$$b^{p-1} = 1 \, mod \, p$$

Dem:

Primero notemos que p no divide a b,2b,3b.....(p-1)b, para demostrar esto supongamos que p/kb para $k < p$, como p no divide a b entonces p/k, lo cual es una clara contradicción.

Para seguir con la demostración veremos que para cada par de enteros tomados de b,2b.....(p-1)b estos no son congruentes modulo p.

Sean j,k enteros menores a p, supongamos que $jb \equiv kb \, mod \, p$ al ser $mcd(b,p) = 1$ multiplicamos por el inverso de b para obtener: $j \equiv k \, mod \, p$, con lo que la única forma de que la congruencia se cumpla es que $j = k$ ya que ambos son menores a p.

Después se escoge aleatoriamente un número e<n tal que mcd (e, (p-1) (q-1)) = 1. Igual que n, el valor de e se hace público. A continuación, se obtiene d, que será el inverso de e módulo (p-1) (q-1). Es decir, d, debe satisfacer la congruencia:

$$de \equiv 1 \, mod \, (p-1)\,(q-1)$$

Aquel que envía el mensaje, puede enviar un mensaje P < n con la congruencia:

$$C \equiv P^e \, mod \, n$$

El receptor, recibe el mensaje cifrado C, que puede desencriptar con la congruencia:

$$P \equiv C^d \, mod \, n$$

Para demostrar que esto funciona, nos apoyaremos en el pequeño teorema de Fermat.:

Tenemos que:

$$de \equiv 1 \, mod (p-1)\,(q-1)$$

Entonces existe un entero k tal que, de = 1 + k(p-1) (q-1). Ahora supongamos, que el texto sin cifrar P es primo relativo de p, entonces por el pequeño teorema de Fermat:

$$P^{p-1} \equiv 1 \, mod \, p$$

Entonces, también tenemos lo siguiente:

$$P^{de} \equiv P^{1+k(p-1)(q-1)} \equiv P(P^{(P-1)})^{k(q-1)} \equiv P * 1 \equiv P \, mod \, p$$

Por otro lado, aunque P no sea primo relativo de p aún tenemos:

$$P^{de} \equiv P \, mod \, p$$

Dado que ambos lados son congruentes con 0 módulo m. Análogamente podemos mostrar que:

$$P^{de} \equiv P \, mod \, q$$

Ahora bien, como p y q son primos relativos, por ser primo cada uno de ellos. Tenemos que:

$$P^{de} \equiv P \, mod \, n$$

Ahora notamos que:

$$C^d \equiv (P^e)^d \equiv P^{de} \equiv P \, mod \, n$$

Y ahí está la prueba de que la desencriptación siempre funciona .

Conclusiones:

Al final de éste trabajo nos hemos encontrado con que a pesar de que la criptografía lleva siglos y siglos de desarrollo, no fue sino hasta tiempos modernos que comenzó a alcanzar un gran auge, tanto que la mayoría de nuestras acciones diarias depende de ella. Nuestras cuentas de redes sociales, banco, la universidad y demás dependen de contraseñas, códigos e información privada que seguimos intentando defender a capa y espada y aun así sale a la luz. Pero todo este desarrollo no ha sido totalmente por su cuenta, la criptografía ha crecido a la par de principalmente otras 2 ciencias: Las matemáticas, más específicamente en la rama llamada teoría de números y la computación, una de las ciencias que avanza a pasos agigantados en la actualidad. Y es que en algún punto la computación avanzara tanto que así como nosotros vemos a los cifrados antiguos como juegos de niños las futuras generaciones verán nuestros criptosistemas "modernos" como algo trivial, por desgracia así como los avances tecnológicos pueden usados para mejorar nuestra seguridad, siempre habrá personas que busquen descifrar los criptosistemas, robar información y así usarla para su beneficio

En una época en la que parece que ya nada se puede mantener en secreto se vuelve aún más imperativo que la seguridad de la información que se transmite por la red sea garantizada. De ahí la importancia del estudio criptográfico.

Anexo Informático del César:

Start Page | Cesarin.java | CriptografiaClasica.java

Source | History

```
1   package cesar;
2   public class Cesarin {
3       private String cadena;
4
5       public Cesarin(String cadena){
6           this.cadena = cadena;
7       }
8   public String cifrarCadena(){
9   return traducirCadena("cifrar");
10      }
11
12  public String descifrarCadena (){
13      return traducirCadena("descifrar");
14  }
15
16  private String traducirCadena(String operacion){
17      String cadenaCifrada = "";
18      for (int i = 0; i < cadena.length(); i++) {
19          char caracter = cadena.toLowerCase().charAt(i);
20          if(caracter>=97 && caracter<=122){
21              if(operacion.equals("cifrar")){
22                  if(caracter>='x'){
23                      caracter = (char)('a' + ('z'-caracter));
24                  }else{
25                      caracter+=3;
26                  }
27                  cadenaCifrada+=(char)(caracter);
28              }else{
29                  if(caracter<='c'){
30                      caracter = (char)('z' - (caracter - 'a'));
31                  }else{
32                      caracter-=3;
33                  }
34                  cadenaCifrada+=(char)(caracter);
35              }
36          }else{
37              cadenaCifrada+=caracter;
38          }
39      }
40
41      cadena = cadenaCifrada;
42      return cadena;
43  }
44  public static void main(String[] args) {
45      Cesarin cc = new Cesarin ("En un agujero en el suelo vivia un Hobbit");
46      System.out.println(cc.cifrarCadena());
47      System.out.println(cc.descifrarCadena());
48  }
```

Anexo Informático de otras criptografías clásicas:

```
package decimado;
import java.io.BufferedReader;
import java.io.InputStreamReader;
/**
 * @author celia
 */
public class CriptografiaClasica {
    static String tabla = "abcdefghijklmnÃ±opqrstuvwxyz0123456789";
    private static long inv = 0;
    public static void main(String[] args) {
        try {
            String str, opc;
            String b;
            int opc1, b1;
            BufferedReader teclado = new BufferedReader(new InputStreamReader(System.in)); //LEERA DESDE TECLADO
            System.out.println("Algoritmos por sustituciÃ³n\n\n");
            System.out.println("-------------------------------------");
            System.out.println("\n\nQUE OPCION DESEAS?\n\n 1)Desplazamiento puro\n 2)DecimaciÃ³n pura \n 3)DESPLAZAMIENTO
VARIABLE\n 4)AFIN-AFIN \n 5)VERNAM \n 6)HILL\n 7)SALIR");
            opc = teclado.readLine();//LEEMOS LA OPCION
            opc1 = Integer.parseInt(opc);//HACEMOS EL PARSER
            switch (opc1) {
                case 1:
                    System.out.println("ALGORITMO POR DESPLAZAMIENTO PURO \n\n");
                    desplazPuro();
                    break;
                case 2:
                    System.out.println("ALGORITMO POR DECIMACIÃ“N PURA\n\n");
                    desimPura();
                    break;
                case 3:
                    System.out.println("ALGORITMO POR DESPLAZAMIENTO VARIABLE\n\n");
                    variable();
                    break;
                case 4:
                    System.out.println("ALGORITMO AFIN-AFIN\n\n");
                    afin();
                    break;
                case 5:
                    System.out.println("ALGORITMO VERNAM\n\n");
                    vernam();
                    break;
                case 6:
                    System.out.println("ALGORITMO DE HILL\n\n");
                    hill();
                    break;
                case 7:
                    break;

            }
            //str = teclado.readLine(); //LEEMOS DESDE TECLADO
            //System.out.println("dato guardado en str "+str);

        } catch (Exception err) {
```

```
public static void Desencriptar(String t, int key) {
    String texto = LimpiarCadena(t);
    String res = "";
    for (int i = 0; i < texto.length(); i++) {
        int pos = tabla.indexOf(texto.charAt(i));
        if ((pos - key) < 0) {
            res = res + tabla.charAt((pos - key) + tabla.length());
        } else {
            res = res + tabla.charAt(pos - key);
        }
    }
    System.out.println("\n LA CADENA DESCIFRADA ES: " + res);
}

//DECIMACION PURA ALGORITMO
////////////////////////////////////////////////
public static void desimPura() {

    try {

        String str, opc;
        String b;
        int opc1, b1;
        BufferedReader teclado = new BufferedReader(new InputStreamReader(System.in)); //LEERA DESDE TECLADO

        System.out.println("Algoritmo por decimaciÃ³n pura\n");
        System.out.println("-----------------------------------");
        System.out.println("\nQUE OPCION DESEAS?\n\n 1)CIFRADO\n 2)DESCIFRADO \n 3)SALIR");
        opc = teclado.readLine();//LEEMOS LA OPCION
        opc1 = Integer.parseInt(opc);//HACEMOS EL PARSER
        switch (opc1) {
            case 1:
                System.out.println("CIFRADO\n\n INSERTA LA PALABRA A CIFRAR: \t");
                str = teclado.readLine(); //LEEMOS DESDE TECLADO
                System.out.println("\nINSERTA LA CONSTANTE DE DECIMACIÃ“N: \t");
                b = teclado.readLine();
                b1 = Integer.parseInt(b);
                String cadena = Cifrado(str, b1);
                System.out.println("\n LA CADENA CIFRADA ES: \t" + cadena);
                break;
            case 2:
                System.out.println("CIFRADO\n\n INSERTA LA PALABRA A ENCRIPTADA: \t");
                str = teclado.readLine(); //LEEMOS DESDE TECLADO
                System.out.println("\nINSERTA LA CONSTANTE DE DECIMACION: \t");
                b = teclado.readLine();
                b1 = Integer.parseInt(b);
                Descifrado(str, b1);
                break;
            case 3:
                break;

        }
        //str = teclado.readLine(); //LEEMOS DESDE TECLADO
        //System.out.println("dato guardado en str "+str);

    } catch (Exception err) {
        System.err.println(err);
    }
}
```

```
    public static String Cifrado(String t, int key) {
        String texto = LimpiarCadena(t);
        //aqui se almacena el resultado
        String res = "";
        for (int i = 0; i < texto.length(); i++) {
            //busca la posicion del caracter en la variable tabla
            int pos = tabla.indexOf(texto.charAt(i));
            //realiza el reemplazo
            if ((pos * key) < tabla.length()) {
                res = res + tabla.charAt(pos * key);
            } else {
                res = res + tabla.charAt((pos * key) % tabla.length());
            }
        }
        return res;
    }

    public static void Descifrado(String t, int key) {
        String texto = LimpiarCadena(t);
        String res = "";
        long[] resp = new long[3];
        int mod = 0;

        for (int i = 0; i < texto.length(); i++) {
            int pos = tabla.indexOf(texto.charAt(i));

            resp = euclidesExtendido(key, tabla.length());

            mod = (int) resp[1];


            if ((pos * mod) > tabla.length()) {
                res = res + tabla.charAt((pos * mod) % tabla.length());
            } else {
                res = res + tabla.charAt(pos * mod);
            }
        }
        System.out.println("INVERSO MULTIPLICATIVO: \t" + resp[0] + "\t" + resp[1] + "\t" + mod);//LA QUE DA EL INVERSO MULTIPLICATI
        System.out.println("\n LA CADENA DESCIFRADA ES: " + res);
    }
    //DESPLAZAMIENTO VARIABLE

    public static void variable() {

        try {

          String str, str1, opc;
          String b;
          int opc1, b1;
          BufferedReader teclado = new BufferedReader(new InputStreamReader(System.in)); //LEERA DESDE TECLADO

          System.out.println("Algoritmo por desplazamiento variable\n");
          System.out.println("-------------------------------------");
          System.out.println("\nQUE OPCION DESEAS?\n\n 1)CIFRADO\n 2)DESCIFRADO \n 3)SALIR");
          opc = teclado.readLine();//LEEMOS LA OPCION
          opc1 = Integer.parseInt(opc);//HACEMOS EL PARSER

          switch (opc1) {
              case 1:
                  System.out.println("\n\n INSERTA LA PALABRA A CIFRAR: \t");
                  str = teclado.readLine(); //LEEMOS DESDE TECLADO
                  System.out.println("\n INSERTA LA PALABRA CLAVE (LA VECES QUE SEA NECESARIO PARA COMPLETAR EL ARREGLO DEL MICLA): \t
                  str1 = teclado.readLine(); //LEEMOS DESDE TECLADO
                  cifradoVariable(str, str1);
                  break;
              case 2:
                  System.out.println("CIFRADO\n\n INSERTA LA PALABRA A ENCRIPTADA: \t");
                  str = teclado.readLine(); //LEEMOS DESDE TECLADO
                  System.out.println("CIFRADO\n\n INSERTA LA PALABRA CLAVE (LA VECES QUE SEA NECESARIO PARA COMPLETAR EL ARREGLO DEL M
                  str1 = teclado.readLine();
                  descifradoVariable(str, str1);
                  break;
              case 3:
                  break;

          }
          //str = teclado.readLine(); //LEEMOS DESDE TECLADO
          //System.out.println("dato guardado en str "+str);

      } catch (Exception err) {
          System.err.println(err);
      }
  }
```