Benemérita Universidad Autónoma de Puebla

Facultad de Ciencias de la Computación

Sistema de Criptografía de curvas elípticas para Resguardar Información del SS de la FCC

Tesis presentada para obtener el título de:
Licenciatura en Ingeniería en Ciencias de la Computación

Presenta:
Brianda Yareli Cruz Guerrero

Asesores de Tesis:
Dr. Héctor David Ramírez Hernández

Dr. Roberto Contreras Juárez

Febrero 2018

Dedicatoria

Dedicada a mis padres quienes fueron el principal cimiento para la construcción de mi vida profesional y personal sentando en mi las bases de responsabilidad, respeto y superación. A mi mamá Natividad Ramos Cruz (†) y a mi abue Angeles Matus Cubas (†) por su amor incondicional, historias maravillosas y lecciones de vida.

Brianda Yareli Cruz Guerrero.

Agradecimientos

Quiero agradecer al Dr. Héctor David Ramírez Hernández, por la paciencia, tiempo y apoyo que me brindó durante la realización de este trabajo, así como por ser un excelente profesor y persona conmigo.

A la M.C. Nelva Betzabel Espinoza Hernández, por ser una excelente maestra y un gran ser humano, y por dedicarle tiempo a mi trabajo y apoyarme con sus observaciones.

Tambien quiero agradecer a la M.C. Marcela Rivera Martínez y al Dr. Roberto Contreras Juárez quienes se tomaron el tiempo de leer este trabajo y así ayudarme con observaciones.

Quiero agradecer enormemente a mi familia, a mi mamá Othonna Guerrero Ramos, por ser mi guia y mi inspiración, por apoyarme a lo largo de mi vida, por los consejos y valores, por todo eso que me llevó a ser quien soy hoy en día, por creer en mi pero más que nada por quererme siempre. A mi papá Pedro Cruz Matuz, por estar siempre que lo necesito, por los consejos, apoyo y confianza que siempre me ha demostrado, por el ejemplo de perseverancia, trabajo y constancia, este trabajo se lo debo a ustedes.

A mis hermanos Herón Simey Cruz Guerrero por ser el mejor hermano mayor, y a Eder Jarim Cruz Guerrero, por que desde el primer día me enseño una nueva manera de amar, por que se convirtio en mi impulso y motivacion para dar lo mejor de mi en todos los aspectos de mi vida.

A mi papá Herón Guerrero Cano, por su amor incondicional, y consejos que me han

servido a lo largo de mi vida.

A mi prima Aranza Lilibeth Guerrero Ramos, por estar ahí en los momentos importantes, por esos juegos de niñas y esas platicas de adultos, por ser más que mi prima, mi hermana y mi mejor amiga.

A mis tios, Elaine Yareli Guerrero Ramos, Dalila Guerrero Ramos y Nelson Guerrero Ramos, por su apoyo, cariño, platicas, enseñanzas y sobre todo por ser unas personas maravillosas.

A mis amigos, Karen Leticia Vázquez Flores, Gerardo Flores Petlacalco y Christopher Jesús Ruís Escapita, por esos días de proyectos, tardes inolvidables y risas interminables, por estar ahí en los buenos momentos y sobre todo en los malos, por hacer inolvidable esta etapa de mi vida.

Gracias a todos, por el apoyo y comprensión que me dieron, por estar conmigo durante tanto tiempo, por eso y más siempre tendrán un lugar especial en mi corazón.

Brianda Yareli Cruz Guerrero.

Índice general

Dedicatoria I

Agradecimientos II

Índice de figuras V

Índice de algoritmos VII

Introducción 2

1. Estado del Arte 5

1.1. Criptografía Simétrica 6

1.1.1. Criptografía Simétrica por Bloques 6

1.2. Criptografía Asimétrica 6

1.2.1. Diffie-Hellman 7

1.2.2. ElGamal 7

2. Historia 8

2.1. Escítala Lacedemonia 9

2.2. Atbash 10

2.3. Alberti 11

2.4. Vigénere 12

2.5. Enigma 14

2.6. Cifrado de Matrices 15

3. Desarrollo Matemático 18

3.1. Curvas Elípticas Sobre $\mathbb{R}$ . . . 19
3.2. Suma de Puntos . . . 22
3.3. Aritmética Modular . . . 24
3.3.1. Inverso Multiplicativo Modular . . . 24
3.3.2. Residuos Cuadráticos . . . 25
3.3.3. Raíz Cuadrada Modular . . . 26
3.4. Curvas Elípticas sobre un grupo finito GF(p) . . . 26

4. Algoritmos del Sistema **31**
4.1. Euclides Extendido . . . 31
4.1.1. Algoritmo de Euclides Extendido . . . 32
4.2. Suma de Puntos . . . 33
4.2.1. Algoritmo Suma de Puntos . . . 34
4.3. Suma de Puntos K veces . . . 34
4.3.1. Algoritmo Suma de Puntos$K$ veces . . . 35
4.4. Intercambio de Claves . . . 36
4.4.1. Algoritmo Diffie-Hellman . . . 36
4.5. Algoritmo Raíz Cuadrada . . . 38
4.5.1. Símbolo de Jacobi . . . 39
4.6. Codificacion En Curvas Elípticas . . . 40
4.6.1. Algoritmo Codificación Bajo Curvas Elípticas . . . 40
4.7. ElGamal . . . 41
4.7.1. Algoritmo ElGamal . . . 41
4.8. Decodificación . . . 43

5. Resultados **44**
5.1. Elementos del Sistema . . . 44
5.1.1. Base de Datos . . . 45
5.2. Aplicación Web . . . 45
5.2.1. Aplicación Web Final . . . 46

Conclusiones **51**

Bibliografía **52**

Índice de figuras

2.1. Escítala Lacedemonia 9
2.2. Cifrado de Atbash 10
2.3. Cifrado de Julio Cesar 11
2.4. Cifrado de Alberti 12
2.5. Matriz Vigénere 13
2.6. Cifrado de Vigénere 13
2.7. Máquina Enigma 14
2.8. Alfabeto 15
2.9. Matriz A 16

3.1. E1:$y^2 = x^3 - 6x + 1$ 20
3.2. E1:$y^2 = x^3 - 5x + 6$ 20
3.3. Representación gráfica de la suma de dos puntos 23

5.1. Modelo Entidad Relación DB 45
5.2. Vista General de la Aplicación Web 46
5.3. Inscripción Ejemplo 47
5.4. Inscripción Ejemplo 47
5.5. Inscripción Ejemplo 47
5.6. Tabla Alumno 48
5.7. Tabla Dependencia 48
5.8. Tabla Familiar 48
5.9. Tabla Programa 49
5.10. Login 49

5.11. Periodos 49
5.12. Alumnos Inscritos 50

Índice de algoritmos

1. Algoritmo de Euclides 32
2. Inverso Multiplicativo 32
3. Algoritmo Suma de Puntos 34
4. Algoritmo Suma de Puntos k veces 35
5. Intercambio de Claves Diffie-Hellman 37
6. Raíz Cuadrada Modular 38
7. Símbolo de Jacobi 39
8. Codificación Bajo Curvas Elípticas 40
9. ElGamal 42
10. Decodificación 43

Introducción

La criptografía de curvas elípticas es una herramienta que apoya a los desarrolladores y empresas que manejan información confidencial, a partir de los fundamentos matemáticos que la respaldan. En este trabajo, se pretende diseñar e implementar un sistema que utilice el algoritmo de cifrado ElGamal para llevar a cabo el almacenamiento encriptado de la información de estudiantes que se inscriben al Servicio Social (SS) de la Facultad de Ciencias de la Computación (FCC), para garantizar la confidencialidad y la integridad de los datos.

Objetivo General

Desarrollar e implementar un sistema utilizando la teoría de curvas elípticas que brinde los servicios de seguridad, autenticación, integridad y confidencialidad de la información de los estudiantes que se inscriben al Servicio Social de la Facultad de Ciencias de la Computación.

Objetivos Específicos

- Cifrar la información mediante ElGamal.
- Brindar a los usuarios una alternativa práctica para enviar su información cuando se inscriben al SS.

Antecedentes del Proyecto

La criptografía se puede definir como el arte o la ciencia de cifrar y descifrar información, utilizando por ejemplo técnicas matemáticas que hagan posible el intercambio de mensajes de manera que sólo puedan ser leídos por las personas a quienes van dirigidos. La finalidad de la criptografía es garantizar el secreto en la comunicación y asegurar que la información que se envía sea auténtica, es decir, que el contenido del mensaje enviado no haya sido modificado en su tránsito.

Los criptosistemas clásicos son aquellos que usan una única clave para cifrar y descifrar los mensajes entre el emisor y el receptor. En 1976 Whitfield Diffie y Martin Hellman revolucionan la criptografía al introducir el concepto de criptosistema asimétrico, que surge como una solución al problema de intercambiar claves privadas por canales inseguros. Los sistemas asimétricos son aquellos en los cuales tanto el emisor como el receptor poseen un par de claves: una de tipo pública y la otra de tipo privada y para enviar mensajes el emisor tiene que cifrar el mensaje con la clave pública del receptor para que así éste sea el único que pueda descifrar el mensaje usando su clave privada. Este novedoso sistema de encriptación, basa su seguridad en las funciones matemáticas cuya solución computacional es difícil ya que aún conociendo los algoritmos para resolverlos, no es factible su ejecución en un tiempo razonable.

La teoría de curvas elípticas conforma una herramienta matemática que brindan a la criptografía la oportunidad de optimizar los algoritmos de cifrado, tal es el caso de ElGamal, mejorando la eficiencia y robustez sin utilizar más recursos computacionales. La criptografía de curva elíptica (CCE), es una variante de la criptografía asimétrica basada en las matemáticas de las curvas elípticas que puede ser más rápida y usar claves más cortas que los métodos como el Rivest, Shamir y Adleman (RSA), además de proporcionar un nivel de seguridad equivalente.

Metodología

El proyecto se desarrolla iniciando con la investigación del estado del arte y de la historia de la criptografía y también algunos conceptos matemáticos.

Durante la implementacion de este proyecto se implementaron todos los algoritmos necesarios para la correcta encriptación mediante ElGamal y así construir el sistema que se planteo dentro de los objetivos.

Para alcanzar los objetivos planteados se dividirá este trabajo en varios capítulos.

Capítulo 1. Investigación del estado del arte, aquí se describen algunos avances en los tipos de criptografía.

Capítulo 2. Dentro de éste capítulo se muestra un breve recorrido por la historia de la criptografía, desde los primeros métodos criptográficos, hasta los usados recientemente con incursión matemática dentro de ellos.

Capítulo 3. Se sabe que en la criptografía con curvas elípticas, los conceptos matemáticos son muy importantes, es por eso que en este capítulo se presentan las definiciones y conceptos importantes para comprender el proceso que se realizó durante el proyecto.

Capítulo 4. En este capítulo se describen los algoritmos utilizados para realizar el proceso de encriptado dentro del sistema.

Capítulo 5. En este capítulo se muestran los resultados finales del sistema, desde la aplicación web, hasta el resultado final del proceso de encriptación en la base de datos.

Capítulo 1

Estado del Arte

Desde siempre las personas tienen la necesidad de ocultar información y se ha incrementado considerablemente con la llegada de los equipos de cómputo. A lo largo de la historia se han utilizado diferentes estrategias que han ayudado a ocultar la información que no se quiere que sean vistas por entes no autorizados. Sin embargo, el avance tecnológico en un mundo globalizado hace más vulnerable cualquier clase de información.

La evolución de la tecnología implica un número creciente de problemas y riesgos estratégicos relacionados con las actividades de las empresas en la web y de prácticamente cualquier usuario que haga uso de este recurso, ya que toda clase de interacciones que se realizan a través de la red y toda clase de información que se ingresa puede ser visible o pública para cualquier entidad.

Desafortunadamente, la mayoría de los usuarios que interactúan con el internet piensan que su información está a salvo de cualquier alteración o robo y que es confidencial para todo el mundo.

En este capítulo, presenta el estado del arte con el objetivo de conocer los tipos de sistemas criptográficos que se tienen hoy en día.

1.1. Criptografía Simétrica

La criptografía simétrica es aquella que usa un método matemático para cifrar y descifrar un mensaje, este tipo de criptografía utiliza únicamente una llave para realizar el proceso, así el mensaje únicamente se descifra con la única llave existente, este tipo de criptografía garantiza confidencialidad, pero al querer compartir el mensaje con otro usuario deberá crearse una nueva llave y el número de llaves aumenta conforme aumenten los usuarios con quienes se comparta el mensaje.

1.1.1. Criptografía Simétrica por Bloques

La información se divide en bloques de tamaño fijo (8, 16 bytes) y se aplica un algoritmo de cifrado a cada bloque, los modos de operación son los siguientes:

- ECB: Cada bloque es cifrado de forma independiente [6].
- CBC: Cada bloque es mezclado con la cifra del bloque previo, después se cifra utilizando la llave [6].

1.2. Criptografía Asimétrica

Estos sistemas se caracterizan por utilizar dos claves, una pública y otra privada utilizadas para encriptar y desencriptar la información, la clave pública está disponible para todos y la privada es sólo conocida para el usuario.

Los modos de operación son los siguientes:

- Encripción: El mensaje es encriptado usando la clave pública del receptor y se desencripta usando la clave privada del receptor, garantizando la confidencialidad del mensaje [6].
- Autenticación: El mensaje es encriptado usando la clave privada del emisor y se desencripta usando la clave pública del emisor. Esto garantiza la autenticidad

del emisor y la integridad del mensaje enviado [7].

1.2.1. Diffie-Hellman

El sistema de intercambio de claves de Diffie-Hellman fue el primer sistema criptográfico de clave pública que se conoció que permite acordar claves entre dos usuarios y está basado en el problema del algoritmo discreto (PLD)[1].

Tiempo después Rivest, Shamir y Adleman desarrollaron el primer sistema criptográfico de clave pública y el cual se continúa usando hasta el día de hoy basado en el modelo Diffie-Hellman, pero utilizando el problema de factorización de enteros (IFP) [5].

1.2.2. ElGamal

En 1985 apareció el sistema criptográfico de ElGamal una variante basada en el PLD [2]. En ese mismo año Neal Koblitz y Victor Miller propusieron de manera independiente la criptografía de curvas elípticas (CCE) [3, 4], cuya seguridad computacional también se basa en el problema del Logaritmo Discreto. Como los puntos racionales de una curva elíptica forman un grupo abeliano más complicado que las unidades de un cuerpo finito, el problema del logaritmo discreto en curvas elípticas es más difícil que el problema del logaritmo discreto en cuerpos finitos. Sin embargo, trabajar con curvas elípticas permite el uso de claves más pequeñas así como mantener el mismo nivel de seguridad, que se traduce en ahorro de banda en las redes de comunicación, consumo de memoria, tiempo y capacidad de procesador.

Capítulo 2

Historia

A lo largo del tiempo el hombre ha tenido la necesidad de enviar y recibir mensajes con contenido confidencial. Gracias a esto nació la criptografía que en primera instancia fue sólo conocida como un arte pero eventualmente fue evolucionando hasta lograr una relación con las matemáticas con lo que se logra reconocer a la Criptografía como una ciencia.

Criptología, del griego Krypto: "oculto" y logos: "estudio" es conocida como la ciencia que estudia la escritura de mensajes "secretos".

La Criptología tiene 3 ramas: Criptografía, Criptoanálisis y Esteganografía.

1. **Criptografía**: Arte de escribir con clave secreta o de un modo enigmático. Ésta rama se encarga de estudiar los métodos que convierten el mensaje en otro con el propósito de que nadie ajeno al emisor y receptor puedan tener acceso al mensaje.

2. **Criptoanálisis**: Arte y técnica de descifrar lo escrito en clave. Se refiere a estudiar los métodos que se utilizan para descifrar el mensaje encriptado. Se dice que ésta es la ciencia opuesta pero complementaria de la Criptografía.

3. **Esteganografía**: La esteganografía trata el estudio y aplicación de técnicas que permiten ocultar mensajes u objetos dentro de otros, llamados portadores,

de modo que no se perciba su existencia.

En éste capítulo se expondrán los inicios y la evolución de las técnicas de la criptografía.

2.1. Escítala Lacedemonia

Los primeros mensajes de los que se tiene conciencia tienen lugar en el siglo V antes de Cristo, provenientes de Esparta y gracias a la invención de la Escítala Lacedemonia (Figura 2.1)

Este método aunque simple resultó muy efectivo. Consistía en poseer un cilindro con medidas y diámetro específicos, posteriormente se enredaba una cinta de papiro y se escribía el mensaje que se quería mandar a lo largo del cilindro, es decir, de forma horizontal. El éxito de este método consistía en que si se desenredaba del cilindro la cinta de papiro sólo se podrían observar letras en desorden o palabras sin sentido.

La cinta ya con el mensaje encriptado era mandada con un mensajero al receptor, así mismo, el receptor debería tener un cilindro de las mismas medidas del emisor para poder enredar la cinta de papiro en su cilindro y así tener acceso al mensaje con claridad.

Figura 2.1: Escítala Lacedemonia

Aunque ahora al analizarlo se llega a la conclusión de que si se acomoda la cinta de alguna manera en especial se podría leer el mensaje con facilidad. Éste método es

muy importante pues fué pionero de la Criptografía.

2.2. Atbash

Siguiendo con los cifrados simples durante los años 500-600 a.C se encuentra el cifrado de Atbash de origen Hebreo. Con éste cifrado se conoce el primer cifrado de sustitución y es mejor conocido por sus aplicaciones bíblicas (Figura 2.2).

Este método consiste en asignar a la primera letra del alfabeto la última de éste, es decir, tomando como ejemplo el alfabeto romano, a la letra 'A" que es la primera letra del alfabeto le asignamos la letra "Z" que es la última, y así sucesivamente hasta tener todas las asignaciones.

Este proceso es encriptando carácter por carácter, después de obtener el alfabeto es fácil, por cada letra del mensaje en claro, el mensaje encriptado se obtiene con la asignación de las letras como se muestra en el siguiente ejemplo:

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

Figura 2.2: Cifrado de Atbash

1. Paso 1: Se tóma una a una las letras del mensaje en claro.

2. Paso 2: Se busca la letra asignada en el alfabeto.

3. Paso 4: Conforme se realizan los pasos siguientes se escribe el resultado que será el mensaje en claro.

Ejemplo 1 ***Mensaje en claro****: HOLA MUNDO*
Mensaje Cifrado*: SLOZÑFNWL*

Julio César

El siguiente método de cifrado que se menciona es una aportación Romana. Este método toma el nombre de Julio César pues él lo usaba para enviar mensajes con órdenes a los generales en batalla, este método consistía en crear un alfabeto encriptado a raíz del alfabeto en claro haciendo una asignación pero desplazándose 3 posiciones a la derecha y así poder encriptar el mensaje. Para hacer el proceso de desencriptación se hace el procedimiento inverso, es decir, hacer un desplazamiento de 3 posiciones pero a la izquierda, como se muestra en la imagen (Figura 2.3).

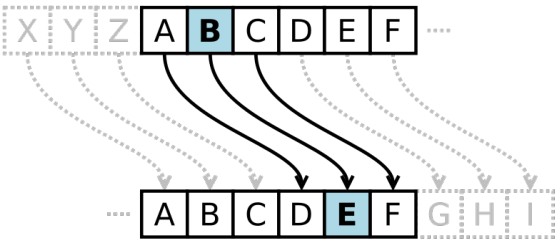


Figura 2.3: Cifrado de Julio Cesar

Aparentemente, hoy en día podemos juzgarlo como un cifrado muy simple y fácil de penetrar, pero en la época de Julio César era una forma muy segura de mandar mensajes al campo de batalla.

Gracias a este método nacieron algunos otros que tomaron como base este cifrado añadiéndole un poco más de seguridad al quitar el número fijo de posiciones que se tenían que desplazar para obtener el alfabeto cifrado, así para obtener el mensaje en claro el receptor debería conocer el número "n" de posiciones de desplazamiento.

2.3. Alberti

En 1466 nació el cifrado de Alberti o cifrado de discos. Este método consiste en dos discos de diferente tamaño que giran independientemente el uno del otro, cada disco tenía inscrito el abecedario, el cifrado se hacía mediante una clave que, en este caso

es una dupla de letras, la primera letra hacía referencia al disco más grande y la segunda al más pequeño, el mensaje en claro se leía de acuerdo al disco exterior.

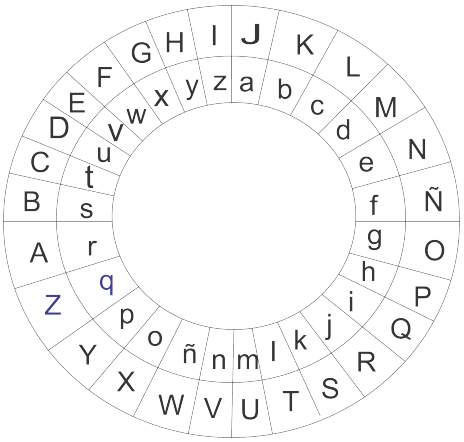


Figura 2.4: Cifrado de Alberti

El proceso se inicia girando los discos hasta empatar la clave, haciendo coincidir las letras de los dos discos, y así se obtiene el alfabeto cifrado para así cifrar y descifrar el mensaje, como se puede observar en el siguiente ejemplo.

Ejemplo 2

- *Clave: Zq*
- *Mensaje en claro: HOLA MUNDO*
- *Mensaje cifrado: ygcrdmeug*

2.4. Vigénere

El siguiente método es más complejo que los que se presentaron anteriormente, con este comenzamos a notar la relación que mantienen la criptografía y las matemáticas y se trata del Cifrado de Vigénere.

En este método se hace uso de las matrices, se tiene una matriz de $n \times n$ con el alfabeto y también una clave. Este método es carácter por carácter.

	A	B	C	D	E	F	G	H	I
A	A	B	C	D	E	F	G	H	I
B	B	C	D	E	F	G	H	I	A
C	C	D	E	F	G	H	I	A	B
D	D	E	F	G	H	I	A	B	C
E	E	F	G	H	I	A	B	C	D
F	F	G	H	I	A	B	C	D	E
G	G	H	I	A	B	C	D	E	F
H	H	I	A	B	C	D	E	F	G
I	I	A	B	C	D	E	F	G	H

Figura 2.5: Matriz Vigénere

En el primer renglón dentro del alfabeto se toma en cuenta sólo las letras de la clave y de forma vertical las letras del mensaje en claro, al hacer la intersección de la clave y el mensaje se obtiene el mensaje encriptado como se muestra en la siguiente imagen (Figura 2.6).

Figura 2.6: Cifrado de Vigénere

2.5. Enigma

El siguiente método es uno de los más conocidos a lo largo de la historia, se trata de la máquina ENIGMA. Hablando un poco de su historia se sabe que tuvo un papel muy importante durante la segunda guerra mundial, fué inventada por el ingeniero alemán Arthur Scherbius[11] quien para la realización de los mecanismos para que la máquina lograra la encriptación tomó como base el cifrado de Vigénere.

Figura 2.7: Máquina Enigma

Hablando del proceso de cifrado de Enigma, se comenzará diciendo que es una máquina electromagnética, es decir, tiene una parte eléctrica y otra mecánica, consistía en una máquina de escribir común y corriente con un tablero iluminado aunque en este caso las teclas eran interruptores que al presionarlas activaban tres cilindros rotatorios que se encontraban dentro de la máquina.

Para cifrar el mensaje se requerían dos personas para operar a Enigma, el que tecleaba colocaba la clave de cifrado en las clavijas de los rotores y la segunda persona anotaba las letras del panel iluminado. El mensaje se cifraba con ayuda de los tres cilindros que estaban conectados al teclado con 26 cables este proceso era tan eficaz gracias a que el primer cilindro giraba un veintiseisavo de vuelta con cada pulsación, así las posiciones de las conexiones cambiaban, el segundo cilindro giraba una vez cada que el primer cilindro giraba 26 veces y el tercer cilindro giraba hasta que el segundo terminara los 26 giros como el funcionamiento de un reloj, además de esto los cilindros podían intercambiar posiciones todo esto para hacer un encriptado casi imposible de descifrar.

Enigma fué descifrada debido a que los operadores repetían las claves de cifrado, por lo que encontraron un patrón en los mensajes[12].

2.6. Cifrado de Matrices

Uno de los métodos que en la actualidad se siguen usando es el cifrado con matrices, este método consiste en asignarle al alfabeto un número (Figura 2.8), con el mensaje en claro obtenemos una matriz renglón, se toma en cuenta que el emisor debe tener la matriz A y el receptor A^{-1}, para obtener el mensaje cifrado se multiplica cada matriz renglón por la matriz A, con este proceso se obtiene el mensaje cifrado, para que el receptor obtenga el mensaje en claro deberá aplicar como primer paso eliminación Gauss-Jordan para obtener A^{-1}, luego se divide el mensaje cifrado en matrices renglón de n elementos y se multiplican por la matriz inversa que se obtuvo, como se observa en el siguiente ejemplo:

0	-	6	F	12	L	18	Q	24	W
1	A	7	G	13	M	19	R	25	X
2	B	8	H	14	N	20	S	26	Y
3	C	9	I	15	Ñ	21	T	27	Z
4	D	10	J	16	O	22	U	-	-
5	E	11	K	17	P	23	V	-	-

Figura 2.8: Alfabeto

Se muestra el proceso de encriptado mediante multiplicación de matrices.

Mensaje en claro: HOLA MUNDO

Declaramos la matriz A de $n \times n$:

$$A = \begin{pmatrix} 1 & 2 & -2 & 1 \\ 1 & 1 & 1 & 3 \\ -1 & -1 & 1 & 4 \\ 1 & 1 & -1 & 5 \end{pmatrix}$$

Figura 2.9: Matriz A

También se tiene el mensaje en claro con la asignación del alfabeto (2.8):

$(8, 16, 12, 1), (0, 13, 22, 14), (4, 16, 0, 0)$

Para la codificación se deberá recordar que multiplicaremos cada matriz renglón por la matriz A y así obtener la matriz renglón codificada:

$$\text{Matriz Renglón}\begin{pmatrix} 8 & 16 & 12 & 1 \end{pmatrix} \text{ x } \begin{pmatrix} 1 & 2 & -2 & 1 \\ 1 & 1 & 1 & 3 \\ -1 & -1 & 1 & 4 \\ 1 & 1 & -1 & 5 \end{pmatrix} = \begin{pmatrix} 13 & 21 & 11 & 109 \end{pmatrix}$$

$$\text{Matriz Renglón}\begin{pmatrix} 0 & 13 & 22 & 14 \end{pmatrix} \text{ x } \begin{pmatrix} 1 & 2 & -2 & 1 \\ 1 & 1 & 1 & 3 \\ -1 & -1 & 1 & 4 \\ 1 & 1 & -1 & 5 \end{pmatrix} = \begin{pmatrix} 5 & 5 & 21 & 197 \end{pmatrix}$$

$$\text{Matriz Renglón}\begin{pmatrix} 4 & 16 & 0 & 0 \end{pmatrix} \text{ x } \begin{pmatrix} 1 & 2 & -2 & 1 \\ 1 & 1 & 1 & 3 \\ -1 & -1 & 1 & 4 \\ 1 & 1 & -1 & 5 \end{pmatrix} = \begin{pmatrix} 20 & 24 & 8 & 52 \end{pmatrix}$$

Con esto se obtiene el mensaje encriptado: $(13, 21, 11, 109, 5, 5, 21, 197, 20, 24, 8, 52)$

Se observa el proceso de desencriptación con ayuda de A^{-1}.

Se obtiene la matriz inversa:

$$A^{-1} = \begin{pmatrix} -1 & 0 & -1 & 1 \\ 1 & \frac{1}{2} & \frac{5}{9} & -\frac{17}{18} \\ 0 & \frac{1}{2} & \frac{1}{9} & -\frac{7}{18} \\ 0 & 0 & \frac{1}{9} & \frac{1}{9} \end{pmatrix}$$

Para realizar la desencriptación multiplicamos cada matriz renglón que nos dió el proceso de encriptación por la matriz inversa A^{-1} para obtener cada matriz renglón con el número de cada letra según nuestro alfabeto (Figura 2.8).

$$\text{Matriz Renglón}\begin{pmatrix} 13 & 21 & 11 & 109 \end{pmatrix} \text{ x } \begin{pmatrix} -1 & 0 & -1 & 1 \\ 1 & \frac{1}{2} & \frac{5}{9} & -\frac{17}{18} \\ 0 & \frac{1}{2} & \frac{1}{9} & -\frac{7}{18} \\ 0 & 0 & \frac{1}{9} & \frac{1}{9} \end{pmatrix} = \begin{pmatrix} 8 & 16 & 12 & 1 \end{pmatrix}$$

$$\text{Matriz Renglón}\begin{pmatrix} 5 & 5 & 21 & 197 \end{pmatrix} \text{ x } \begin{pmatrix} -1 & 0 & -1 & 1 \\ 1 & \frac{1}{2} & \frac{5}{9} & -\frac{17}{18} \\ 0 & \frac{1}{2} & \frac{1}{9} & -\frac{7}{18} \\ 0 & 0 & \frac{1}{9} & \frac{1}{9} \end{pmatrix} = \begin{pmatrix} 0 & 13 & 22 & 14 \end{pmatrix}$$

$$\text{Matriz Renglón}\begin{pmatrix} 20 & 24 & 8 & 52 \end{pmatrix} \text{ x } \begin{pmatrix} -1 & 0 & -1 & 1 \\ 1 & \frac{1}{2} & \frac{5}{9} & -\frac{17}{18} \\ 0 & \frac{1}{2} & \frac{1}{9} & -\frac{7}{18} \\ 0 & 0 & \frac{1}{9} & \frac{1}{9} \end{pmatrix} = \begin{pmatrix} 4 & 16 & 0 & 0 \end{pmatrix}$$

Y con este proceso se descifrr el mensaje con ayuda de la tabla del alfabeto (Figura 2.8).

Mensaje cifrado: $(13, 21, 11, 109, 5, 5, 21, 197, 20, 24, 8, 52)$
Mensaje en claro: HOLA MUNDO

Capítulo 3

Desarrollo Matemático

Es necesario entender algunos conceptos básicos para comprender el desarrollo del proyecto, en este capítulo se presentarán las definiciones que ayudarán más adelante a comprender las operaciónes realizadas para el criptoanálisis.

Se les llama curvas elípticas por que están formadas por ecuaciones cúbicas parecidas a las utilizadas para calcular la circunferencia de una elipse y constituyen un grupo Abeliano.

Las propiedades de estas curvas son muy útiles dentro de la criptografía.

Definición 3.1 *Un grupo Abeliano es un conjunto G con una operacion $(G*)$ que cumple las siguientes propiedades.*

1. *Operación Interna*
   Definimos operación interna como:

$$\forall\,(a,b)\ \in G : a * b\ \in\ G$$

2. *Asociativa*
   Se dice que $(G*)$ es asociativa si:

$$\forall\,(a,b,c) \in G : a * (b * c) = (a * b) * c$$

3. *Existencia del elemento Neutro*
   Se dice que tiene la existencia de un neutro si:

$$\exists\, un\, e \in G : (a * e) = (e * a) = a$$

4. *Todo elemento de G tiene su inverso*
   Definimos el inverso como:

$$\forall\, a \in G \exists\, un\, a^{-1} \in G : a * a^{-1} = a^{-1} * a = e$$

5. *Conmutativa*
   Se dice que es conmutativa si:

$$\forall\, (a, b) \in G : (a * b) = (b * a)$$

3.1. Curvas Elípticas Sobre $\mathbb{R}$

Definición 3.2 *Una curva elíptica sobre* $\mathbb{R}$ *es el conjunto de puntos del plano (x,y), que cumplen la siguiente ecuación:*

$$y^2 = x^3 + ax + b \tag{1}$$

Los coeficientes a y b caracterizan únivocamente cada curva.

Las siguientes ecuaciones son ejemplos de curvas elípticas.

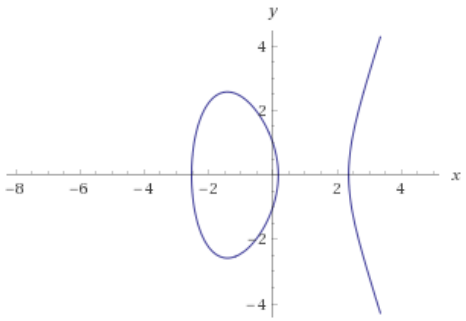


Figura 3.1: E1:$y^2 = x^3 - 6x + 1$

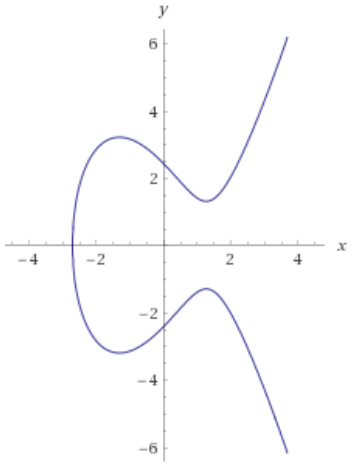


Figura 3.2: E1:$y^2 = x^3 - 5x + 6$

Si $x^3 + ax + b$ no tiene raíces múltiples, entonces la curva correspondiente, aunado con el punto especial ∞, llamado punto en el infinito, más la operación suma que se definirá más adelante, se denominará grupo de curva elíptica E($\mathbb{R}$). Hay que recalcar que ∞ es un punto imaginario situado por encima del eje de abscisas a una distancia infinita, y que por lo tanto no tiene un valor concreto.

Viendo ahora que si $x^3 + ax + b$ no tiene raíces múltiples, entonces se cumple que $\Delta = 4a^3 + 27b^2 \neq 0$. A Δ se le llamará el discriminante de la curva elíptica.

Proposición 1 *Si la expresión $x^3 + ax + b$ tiene raíces múltiples, entonces $\Delta = 4a^3 + 27b^2 = 0$.*

Demostración 1 *Supongamos que la expresión $x^3 + ax + b$ tiene raíces múltiples. Esto implica que*

$$x^3 + ax + b = (x - q)^2(x - r)$$

Desarrollando el segundo término:

$$(x - q)^2(x - r) = (x^2 - 2qx + q^2)(x - r) = x^3 - 2qx^2 - rx^2 + q^2x + 2qrx - q^2r$$

Igualando los coeficientes del mismo grado se tienen la siguientes relaciones:

$$-2q - r = 0$$

$$q^2 + 2qr = a$$

$$-q^2r = b$$

Despejando r en la primera igualdad y sustituyendo su valor en las dos restantes se obtiene:

$$r = -2q$$

$$a = q^2 + 2q(-2q) = q^2 - 4q^2 = -3q^2$$

$$b = -q^2(-2q) = 2q^3$$

elevando al cubo la segunda expresión y al cuadrado la tercera expresión obtenemos:

$$a^3 = -27q^6$$

$$b^2 = 4q^6$$

Despejando q^6 de ambas expresiones e igualando tenemos:

$$q^6 = \frac{a^3}{-27} = \frac{b^2}{4}$$

Lo cual implica que:

$$4a^3 = -27b^2,$$

esto es,

$$4a^3 + 27b^2 = 0.$$

3.2. Suma de Puntos

Sean $P(x_p, y_p)$ y $Q(x_q, y_q)$ puntos de una curva elíptica definida sobre $\mathbb{R}$. Se define la suma entre P y Q de la siguiente manera:

- Si P y Q son puntos distintos los cuales no son negativos uno del otro, se tiene la inclinación de la línea a través de P y Q, de la forma:

  $$m = \frac{y_p - y_q}{x_p - x_q},$$

  y se puede expresar la suma $P + Q = R$ como sigue:

  $$x_R = m^2 - x_P - x_Q,$$

  $$y_R = -y_P + m(x_P - x_Q).$$

- Sumar P consigo mismo se tiene: $P + P = 2P = R$. Cuando $y_P \neq 0$,

  $$m = \frac{3x^2 + a}{2y_P},$$

  $$x_R = m^2 - 2x_P,$$

  $$y_R = -y_P + m(x_P - x_R).$$

Geométicamente hablando, las reglas de la adición pueden ser establecidas de la siguiente manera:

1. El negativo de un punto P es el punto con la misma coordenada en x (abscisa), pero con coordenada y (ordenada negativa), ($P = (x, y)$ entonces - $P = (x, -y)$). Se debe notar que estos 2 puntos se representan como una

línea vertical y además que $P + (-P) = P - P = \infty$. Recordando que a ∞ se le llama punto cero o punto en el infinito.

2. Para sumar dos puntos distintos P y Q se traza una línea que pase por ambos puntos y se tiene que interceptar con la curva en un tercer punto denominado R. Se puede apreciar que R es el único punto de intersección a menos que la línea trazada sea tangente a la curva en cuyo caso se tiene que P o Q son tangentes a dicha curva, se necesita definir la adición de estos tres puntos como $P + Q = -R$. Esto es $P + Q$ será reflejada sobre eje de las abscisas del tercer punto de intersección. La siguiente figura ilustra esta construcción.

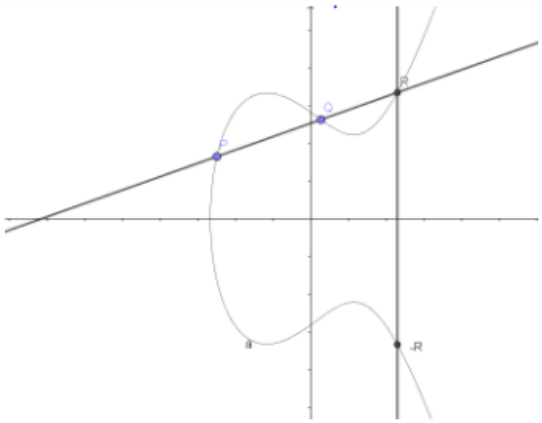


Figura 3.3: Representación gráfica de la suma de dos puntos

3. Considerando el caso donde $x_P = x_Q$, pero $y_P \neq y_Q$; por lo que $Q = -P$. La línea a través de P y $-P$ es una línea vertical, por lo tanto intersecta a la curva en ∞. Por lo tanto, en este caso $P + (-P) = \infty$.

4. En el caso en el que $P = Q$, se traza una línea tangente a la curva y encuentra otro punto de intersección $-R$. entonces $P + P = 2P = R$.

5. Finalmente, suponiendo que $Q = \infty$. La línea a través de P e ∞ es una línea vertical que intersecta a la curva elíptica en el punto P' que es la reflexión de P a través del eje x. Cuando se refleja P' a través del eje x para obtener

$R = P + Q$ se regresa al punto P.
Por lo tanto:

$$P + \infty = P,$$

para todos los puntos P sobre la curva elíptica.

3.3. Aritmética Modular

Se puede definir a la aritmética modular como la rama de las matemáticas que ayuda a la Criptografía, permite realizar cálculos complejos, es un sistema aritmético para clases de equivalencia de números enteros llamados clases de congruencia.[8]

Se le llama también congruencia, equivalencia o aritmética de reloj pues los números dan la vuelta haciendo analogía al reloj hasta alcanzar un valor llamado módulo.[9]

Para este proyecto se define al Grupo Abeliano como el campo GF(p), donde, p es un número primo.

Definición 3.3 *Sea m un entero positivo, donde $a, b \in \mathbb{Z}$. Se define $a \equiv b \pmod{m}$ si y sólo si m divide a $(a - b)$*

Proposición 2

- *$a \equiv b \pmod{m}$ entonces a y b dejan el mismo resto cuando son divididos por m.[10]*
- *La relación de congruencia $\pmod{m}$, es una relación de equivalencia en $\mathbb{Z}$.*

Ejemplo 3 *Con GF(5), se dice que $12 \equiv 7 \pmod{5}$,pues 5 divide a la resta de 12-7, esto es, 5 divide a 5.*

3.3.1. Inverso Multiplicativo Modular

Se sabe que el inverso multiplicativo de un número real distinto de 0 se puede calcular de una forma sencilla, por ejemplo el inverso multiplicativo de 4 es $\frac{1}{4}$ ya que $4 * \frac{1}{4} = 1$.

Definición 3.4 *Dados un entero a y un primo p el inverso multiplicativo de a* (mód p) *es un entero x entre 1 y p-1 tal que,* $xa \equiv 1$ (mód p)*. Se debe tener en cuenta que el inverso multiplicativo de a* (mód p) *existe si y sólo si a y p son enteros coprimos, es decir, si mcd(a,p)=1.*

Dentro de la aritmética modular el inverso multiplicativo así como el máximo común divisor (mcd) se obtiene con ayuda del algoritmo de Euclides Extendido (Algoritmo 1) para obtener tanto el inverso como el máximo común divisor.

En la operación modular el problema radica en encontrar un x tal que:

$$xa \equiv 1 \pmod{p}$$

entonces si $mcd(a, p) = 1$ se sabe que existe un x e y tal que:

$$a \cdot x + n \cdot y = 1 \, en \, GF(p)$$

se tiene que $a \cdot x = 1$ (mód p). El algoritmo realizado para obtener el inverso se estudiara más adelante.

3.3.2. Residuos Cuadráticos

Definición 3.5 *Sea* $a \in GF(p)$*. El elemento a es residuo cuadrático módulo p si existe un x en GF(p) tal que* $x^2 \equiv a$ (mód p)*. Se denota al conjunto de todos los residuos cuadráticos como* Q_p *y el de los residuos no cuadráticos como* $\overline{Q_p}$

Para obtener el conjunto de los residuos cuadráticos Q_p y los no cuadraticos $\overline{Q_p}$, se hace uso del Símbolo de Legendre definido a continuación.

Definición 3.6 *Sea p un primo impar y a un entero. El símbolo de Legendre se define:*

$$\frac{a}{p} = \begin{cases} 0 & si \; \frac{p}{a} \\ 1 & si \; a \in Q_p \\ -1 & si \; a \in \overline{Q_p} \end{cases} \tag{2}$$

Ejemplo 4 *Si p=7 el conjunto Q_p esta conformado por 1,2,4 ya que:*

$$1^2 \equiv 1 \pmod 7$$

$$2^2 \equiv 4 \pmod 7$$

$$3^2 \equiv 2 \pmod 7$$

$$4^2 \equiv 2 \pmod 7$$

$$5^2 \equiv 4 \pmod 7$$

$$6^2 \equiv 1 \pmod 7$$

el conjunto $\overline{Q_p}$ está conformado por 3,5 y 6

3.3.3. Raíz Cuadrada Modular

Dentro de las operaciones que se pueden realizar en la aritmética modular se encuentra la raíz cuadrada, usada para el proceso de encriptación con curvas elípticas la cual se calcula con ayuda de la siguiente definición.

Definición 3.7 *Sea $a \in Q_p$. Si $x \in GF(p)$ tal que $x^2 \equiv a \pmod p$, entonces x es la raíz cuadrada modular de $a \pmod p$.*

El número de raíces de $a \pmod p$ se determina mediante la obtención de los Residuos Cuadráticos, es decir:

Si p es un número primo y $a \in Q_n$, a tiene exactmante dos raíces cuadradas módulo p distintas en caso contrario a tiene más de dos raíces.

3.4. Curvas Elípticas sobre un grupo finito GF(p)

Trabajar criptografía con curvas elípticas sobre los números reales se puede volver lento e inexacto, debido a los errores de redondeo que puedan existir. En la práctica,

el trabajo de criptografía se lleva a cabo con curvas elípticas sobre el campo finito GF(p) pertenecientes a los campos primos y GF(2^m) pertenecientes a los campos binarios. Este trabajo se centra en las curvas elípticas sobre el campo finito GF(p), con p un número primo.

Recordando que el campo GF(p) usa los numeros del 0 al $p-1$ en cómputo final se obtiene el módulo de p.

Una curva elíptica definida sobre el campo de GF(p), denotada por E(GF(p)), puede estar formado por las variables a y b dentro del campo GF(p). Las curvas elípticas incluyen todos los puntos de (x, y) que satisface la ecuación de una curva elíptica módulo p. esto es, una curva elíptica sobre GF(p) tiene por ecuación:

$$y^2 \pmod p = (x^3 + ax + b) \pmod p, \tag{3}$$

donde a,b $\in$ GF(p).

De manera analógica, si x^3+ax+b contiene factores no repetidos o equivalentemente si $aq^3+27b^2 \pmod p$ no es 0, entonces la curva elíptica se puede utilizar para formar un grupo. Una curva elíptica sobre el grupo GF(p) tiene los puntos correspondientes en la curva elíptica, junto con un punto especial ∞, al cual se le llama punto en infinito o punto cero.

Ejemplo 5 *Considerando la curva elíptica sobre GF(7), con $a = 3$ y $b = 4$, la ecuación de la curva elíptica es $y^2 = x^3 + 3x + 4$. Los puntos que pertenecen a esta curva son:(0,2),(0,5),(1,1),(1,6),(2,2),(2,5),(5,2),(5,5),(6,0) incluyendo a ∞.*

Las reglas para la adición son equivalentes a las que se describieron para el caso de las curvas elípticas definidas para los números reales:

1. $P_1 + \infty = P_1$
2. Si $P_1 = (x_1, y_1)$, entonces $-P_1 = (x_1, -y_1)$.
3. Sean $P_1 = (x_1, y_1)$ y $P_2 = (x_2, y_2)$ puntos de la curva elíptica con $P_1, P_2 \neq \infty$. Entonces si $x_1 = x_2$ pero $y_1 = y_2$ o $P_1 = P_2$ y $y_1 = 0$ entonces $P_1 + P_2 = \infty$.

en otro caso $P_1 + P_2 = P_3 = (x_3, y_3)$ con

$$x_3 = m^2 - x_1 - x_2,\ y_3 = m(x_1 - x_3) - y_1$$

$$m = \begin{cases} \frac{3x^2+a}{2y}\ si\ x_1 = x_2 \\ \frac{y_2-y_1}{x_2-x_1}\ si\ x_1 \neq x_2 \end{cases} \tag{4}$$

Ejemplo 6 *En el grupo de la curva elíptica definida por* $y^2 = x^3 + 3x + 4$ *sobre GF(7), ¿cuál es el resultado de* $P + Q$*, donde P=(0,2) y Q=(1,6)?, ¿y de 2Q?.*

El proceso se comienza de acuerdo a los visto en la sección suma de puntos (Sección 3.2), como primer paso se obtiene m*, se observa que* P *y* Q *son diferentes y que* $x_1 \neq x_2$ *a demás es importante recordar que se trabaja con aritmética modular por lo tanto todas las operaciones deberán ser realizadas módulo* p *entonces,*

$$m = \frac{y_2 - y_1}{x_2 - x_1},$$

$$m = \frac{6 - 2}{1 - 0}$$

$$m = \frac{4}{1},$$

en este punto se debe obtener el inverso multiplicativo del denominador,en nuestro caso el inverso multiplicativo de 1 *es* 1*,*

$$4 \times 1 = 4$$

$$m = 4$$

Se sustituye m *en la ecuación para obtener* x_3*, entonces*

$$x_3 = m^2 - x_1 - x_2,$$

$$x_3 = 4^2 - 0 - 1,$$

$$x_3 = 2 - 6 = 3$$

Se sustituyen los valores encontrados en la ecuación para obtener y_3,

$$y_3 = m(x_1 - x_3) - y_1$$

$$y_3 = 4(0 - 3) - 2$$

$$y_3 = 4(4) - 2$$

$$y_3 = 2 - 2 = 0$$

Así se encuentra el punto $P + Q = R$, *donde,* $R = (3, 0)$.

Para el caso de $2Q$, *se obtiene la variable* m, *en este caso el punto a sumar es el mismo, es decir, se quiere obtener* $2Q$, *entonces nuestra variable* m *se obtiene de la siguiente forma:*

$$m = \frac{3x^2 + a}{2y}$$

$$m = \frac{3(1^2) + 3}{2(6)}$$

$$m = \frac{6}{5}$$

Se obtiene el inverso multiplicativo de 5 *que es* 3,

$$3 \times 6 = 18 = 4$$

$$m = 4$$

Se Sustituye m *en la ecuación para obtener* x_3,

$$x_3 = m^2 - 2(x_Q)$$

$$x_3 = (4)^2 - 2(1)$$

$$x_3 = 2 - 2 = 0$$

Se sustituyen los valores encontrados en la ecuación para obtener y_3,

$$y_3 = -y_Q + m(x_Q - x_3)$$

$$y_3 = -6 + 4(1 - 0)$$

$$y_3 = -6 + 4 = -2 = 5$$

Así se encuenntra el punto $Q + Q = 2Q = R$*, donde,*$R = (0, 5)$.

La curva elíptica E(GF(p)) dotada de la operación suma definida anteriormente forma un Grupo Abeliano.

Capítulo 4

Algoritmos del Sistema

Una vez que se estableció la base matemática usada en este proyecto, para la correcta realización del proyecto en este capítulo se muestran los algoritmos usados durante la encriptación realizada para el sistema Web final.

4.1. Euclides Extendido

En el capítulo anterior se describió el Algoritmo de Euclides Extendido como el método que nos permite calcular el mcd y el inverso multiplicativo dentro de la aritmética modular, ahora se muestra el algoritmo de este método.

Es importante tener en cuenta que este algoritmo es una ligera modificación del algoritmo de Euclides que nos permite, además de encontrar el mcd y expresarlo como una combinación lineal, calcular el inverso multiplicativo. Debemos dejar en claro que éste número no siempre existe y se podrá obtener si y sólo si el $mcd(a, p) = 1$.

El pseudocódigo para la implementación del algoritmo es el siguiente:

4.1.1. Algoritmo de Euclides Extendido

Algoritmo 1 Algoritmo de Euclides

Entrada: p, a

1: $mod = p$

Salida: $d = mcd(p, a), x, y$

2: **si** $b = 0$ **entonces**

3: $p = p, x = 1, y = 0$

4: **devolver** d, x, p

5: **fin si**

6: $x_2 = 1, x_1 = 0, y_2 = 0, y_1 = 1$

7: **mientras** $a > 0$ **hacer**

8: $q = \frac{p}{a}, r = p - qa, x = x_2 - qx_1, y = y_2 - qy_1, p = a, b = r, x_2 = x_1, x_1 = x, y_2 = y_1, y_1 = y$

9: **fin mientras**

10: $d = p, x = x_2, y = y_2$

11: **devolver** d, x, y

Gracias al Algoritmo de Euclides (Algoritmo 1) se obtiene la representación del mcd como $Px + Ay = 1$, entonces al obtener el valor de y obtenemos el inverso modular, recordando que todas las operaciones son modulares por lo que para obtener el inverso se agregan las siguientes líneas al pseudocódigo del algoritmo.

Algoritmo 2 Inverso Multiplicativo

Salida: inv=y

1: **mientras** inv < 0 **hacer**

2: inv=inv+mod

3: **fin mientras**

4: **mientras** inv $>= 0$ **hacer**

5: inv=inv−mod

6: **fin mientras**

7: **devolver** d, x, y, inv

Para que se aprecie mejor el algoritmo se dan algunos valores para obtener los el $mcd, x, y, inverso$, la salida del programa se muestra a continuación.

Ejemplo 7 *Suponiendo los siguientes parámetros para el ejemplo:*

- *Primer número p:* 73
- *Segundo número a:* 11

La salida del programa fué:

El mcd$(73, 11) = 1$
$x = -3$
$y = 20$
Combinación lineal: $73(-3) + 11(20) = 1$
Inverso modular: 20

4.2. Suma de Puntos

Ahora se explica el proceso de la Suma de Puntos, gracias a esta operación se obtiene un punto base que es importante para el proceso de encriptación.

Se xplicará brevemente como trabaja el algoritmo.

Para realizar el cálculo necesitamos una curva elíptica de la forma $y^2 = x^3 + ax + b$ la cual debe estar definida dentro de un grupo $GF(p)$ con p primo, con esto se asegura tener un punto $P(x, y)$ perteneciente al grupo y obtener otro igual que pertenece a la curva, el cual se denota como $r(x, y)$.

Para esta operación se tienen dos fórmulas que ayudarán al proceso de obtener el punto $K(x, y)$, cabe resaltar que para éste punto todas las operaciones realizadas son modulares.

Sea p, q un punto dentro de una curva elíptica dada por una ecuacion del tipo $y^2 = x^3 + ax + b$, para sumar dos puntos diferentes $p(x, y)$ y $q(x, y)$ utilizamos la siguiente fórmula.

$$m = \frac{(y_p - y_q)}{(x_p - x_q)} \tag{1}$$

$$x_r = m^2 - x_p - x_q \tag{2}$$

$$y_r = -y_p + m(x_p - x_r) \tag{3}$$

Si se requiere sumar dos veces el mismo punto es decir $p(x,y)+p(x,y) = 2p$ tenemos la siguiente fórmula

$$m = \frac{(3xp^2 + a)}{(2y_p)} \tag{4}$$

$$x_r = m^2 - 2x_p \tag{5}$$

$$y_r = -y_p + m(x_p - x_r) \tag{6}$$

4.2.1. Algoritmo Suma de Puntos

El siguiente algoritmo calcula la suma de puntos de dos puntos iguales o diferentes.

Algoritmo 3 Algoritmo Suma de Puntos

Entrada: p(x,y),q(x,y),a
Salida: r(x,y)

1: **si** $px \neq q_x$ y $q_x \neq q_y$ **entonces**
2: $\Delta = \frac{(y_p - y_q)}{(x_p - x_q)}$
3: $x_r = \delta^2 - 2x_p$
4: $y_r = -y_p + \Delta(x_p - x_r)$
5: **devolver** r(x,y)
6: **fin si**
7: **si** $px = q_x$ y $q_x = q_y$ y $y_x \neq 0$ **entonces**
8: $\Delta = \frac{(3xp^2+a)}{(2y_p)}$
9: $x_r = \delta^2 - 2x_p$
10: $y_r = -y_p + \Delta(x_p - x_r)$
11: **devolver** r(x,y)
12: **fin si**

4.3. Suma de Puntos K veces

Parece importante destacar que este procedimiento se realiza de izquierda a derecha al momento de seguir la representación del numero K en binario.

Se necesita una curva elíptica del tipo $y^2 = x^3 + ax + b$ la cual debe estar definida dentro de un grupo $GF(p)$ con p primo, con esto se asegura tener un punto $p(x, y)$ perteneciente al grupo y obtener otro igual que pertenece a la curva, el cual se denota como $K(x, y)$, con K perteneciente al grupo $GF(p)$.

4.3.1. Algoritmo Suma de Puntos$K$ veces

Ahora vemos que dentro de nuestro sistema de encriptación eventualmente vamos a necesitar sumar un punto$k - veces$ es decir $p+p+...+p$ un número k de veces. Para obtener el punto kp podemos hacer uso del siguiente algoritmo.

Algoritmo 4 Algoritmo Suma de Puntos k veces

Entrada: p(x,y),k,a,g

Salida: k(x,y)

1: convertimos a k en binario
2: tomamos como punto inicial $pi(0, 0)$
3: **para** $i = tamao\,del\,binario$ hasta $i = 0$ **hacer**
4: **si** $digito[i] = 0$ **entonces**
5: puntos=$SumadePuntos(p, pi, a, g)$
6: **fin si**
7: **si** $digito[i] = 1$ **entonces**
8: puntos=$SumadePuntos(p, pi, a, g)$
9: puntos=$SumadePuntos(p, puntos, a, g)$
10: **fin si**
11: **fin para**
12: **devolver** puntos(x,y)

Ejemplo 8 *Supongamos los siguientes parámetros para el ejemplo:*

- *Curva elíptica:* $y^2 = x^3 + 34x + 25$
- *GF(p):* 73

- *Punto base* (x, y)*:* $P(8, 15)$
- *K:*75

La salida del programa fue:

$75 \times P(8, 15) = (57, 35)$

4.4. Intercambio de Claves

Éste punto es importante dentro del sistema pues como se menciona, se usa un sistema asimétrico por lo cual es necesario realizar un intercambio de claves entre el emisor y el receptor, para esto se utiliza el método de Diffie-Hellman, este método realiza el intercambio de claves utilizando curvas elípticas.

4.4.1. Algoritmo Diffie-Hellman

Se considera al emisor y al receptor como usuarios A y B respectivamente, entonces suponiendo que el usuario A requiere enviar un mensaje al usuario B se sigue el siguiente procedimiento.

1. El usuario A selecciona un valor aleatorio dentro del grupo GF(p) al cual se llamará nA y envia al usuario B el punto $PA = nA * GF(p)$
2. El usuario B selecciona un valor aleatorio dentro del grupo GF(p)al cual se llamará nB y envia al usuario A el punto $PB = nB * GF(p)$
3. En este punto el usuario A debe generar una clave secreta la cual llamará K donde $K = nA * PB$
4. El usuario B a su vez genera su clave privada $K = nB * PA$

Para poder realizar el proceso es necesario contar con una curva elíptica del tipo $y^2 = x^3 + ax + b$ y un punto $p(x, y)$ definidos sobre el grupo con el cual se trabajará.

Romper este esquema es prácticamente imposible pues el ataque deberá ser capaz de obtener las claves K por lo que deberá intentar obtener el grupo GF(p) y a su vez el punto p lo que hace muy seguro a este método.

Algoritmo 5 Intercambio de Claves Diffie-Hellman

Entrada: $p(x, y), a, g$
Salida: nA, nB, KA, KB

1: Se obtienen los valores aleatorios nA y nB
2: Se verifica que nA y nB sean valores permitidos
3: $mcdA$=EuclidesExtendido, $mcdB$=EuclidesExtendido
4: **si** $mcdA = 1$ y $mcdB = 1$ **entonces**
5: PA=Algoritmo Suma de Puntos K veces
6: PB=Algoritmo Suma de Puntos K veces
7: Para obtener KA y KB se envian al Algoritmo de Suma de Puntos K veces los datos PA y PB
8: KA=Algoritmo Suma de Puntos K veces (PA)
9: KA=Algoritmo Suma de Puntos K veces (PB)
10: **fin si**
11: **devolver** nA, nB, KA, KB

Ejemplo 9 *Supongamos los siguientes parámetros para el ejemplo:*

- *Curva elíptica:* $y^2 = x^3 + 34x + 25$
- *GF(p):* 73
- *Punto base* (x, y) *:*$P(8, 15)$
- *Clave Secreta A:* 75
- *Clave Secreta B:* 68

La salida del programa fue:

$74 \times P(8, 15) = (57, 35)$
$68 \times P(8, 15) = (25, 41)$
La clave secreta común es: $K = 75(25, 41) = 68(57, 35) = (8, 33)$

4.5. Algoritmo Raíz Cuadrada

Como lo hemos repetido en éste y en capítulos anteriores todas nuestras operaciones son modulares, es por eso que para obtener la raíz cuadrada haremos un proceso diferente al convencional pues ésta raíz es modular. A continuación se muestra el algoritmo para obtener la raíz cuadrada modular y a su vez el algoritmo del símbolo de Jacobi que es necesario para el cálculo de la raíz.

Algoritmo 6 Raíz Cuadrada Modular

Entrada: e,p,a

Salida: r

1: Obtenemos el símbolo de Jacobi l
2: **si** $l = -1$ **entonces**
3: Imprimir"No tiene Raíz"
4: **fin si**
5: $t = \frac{(p-1)}{2^s}$
6: Obtenemos el inverso multiplicativo de t con el algoritmo de Euclides extendido
7: $c = b^t \pmod p$, $r = a^{\frac{t+1}{2}} \pmod p$
8: **para** $i = 0$ hasta $i < s - 1$ **hacer**
9: $d = (r^2 a^{-1})^{s-i-1} \pmod p$
10: **si** $d = -1 \pmod p$ **entonces**
11: $r = rc \pmod p$
12: **fin si**
13: $c = c^2 \pmod p$
14: **fin para**
15: **devolver** r

Ejemplo 10 *Supongamos los siguientes parámetros para el ejemplo:*

- *GF(p):* 751
- *Número al que se le quiere sacar raíz:* 255

La salida del programa fue:

Raíz Cuadrada de $255 \pmod 7 51 = 69$

Para comprender mejor el algoritmo anterior debemos tener en cuenta el siguiente algoritmo, el símbolo de Jacobi, ya que es un concepto importante, es necesario para obtener la raíz cuadrada y eventualmente el punto codificado del mensaje en claro.

4.5.1. Símbolo de Jacobi

Este algoritmo ayuda con el cálculo de la raíz cuadrada modular dentro de la aritmética modular, acontinuación mostramos el pseudocódigo.

Algoritmo 7 Símbolo de Jacobi

Entrada: a,n
Salida: s

si $a = 0$ **entonces**
  devolver 0
fin si
si $a = 1$ **entonces**
  devolver 1
fin si
$a_1 = \frac{a}{2^e}$
si e es par **entonces**
  $s = 1$
fin si
si $n = 1 \pmod 8$ o $n = 7 \pmod 8$ **entonces**
  $s = 1$
fin si
si $n = 3 \pmod 8$ o $n = 5 \pmod 8$ **entonces**
  $s = -1$
fin si
si $n = 3 \pmod 4$ y $a_1 = 3 \pmod 4$ **entonces**
  $s = -s$
fin si
devolver s

4.6. Codificacion En Curvas Elípticas

Para llegar a la codificación con ElGamal es necesario mostrar cómo se codifica un mensaje en primera instancia bajo una curva elíptica, esto se hace con la finalidad de que al mensaje que se envía por cada letra contenida dentro de este mensaje le corresponda un punto válido dentro de la curva dada pues esto hace más fácil el trabajo para nuestro algoritmo de cifrado ElGamal.

4.6.1. Algoritmo Codificación Bajo Curvas Elípticas

De la misma manera que en algoritmos anteriores para este debemos tener una curva elíptica del tipo $y^2 = x^3 + ax + b$ y un grupo $G(p)$ con p primo.
Antes de empezar con el algoritmo es importante decir que se codificará bajo el código ASCII, es decir, cada letra del mensaje m tomará el valor de acuerdo a la tabla ASCII.

Algoritmo 8 Codificación Bajo Curvas Elípticas

Entrada: m,M,l,g,h
Salida: p(x,y)

1: Se verifica que $M * h < g$
2: El proceso se hace para cada letra del mensaje m
3: **mientras** $i = 1$ hasta $i = largodem$ **hacer**
4: $x = ascii(h) + j$
5: Se sustituye a x en la ecuación $y^2 = x^3 + ax + b$
6: Se obtiene la raíz cuadrada del resultado de la ecuación
7: Se obtiene el punto $p(x, y)$ donde p es el x encontrado e y es el resultado de la raíz
8: **fin mientras**
9: **devolver** $p(x, y)$

Ejemplo 11 *Supongamos los siguientes parámetros para el ejemplo:*

- *Curva elíptica:* $y^2 = x^3 + 34x + 25$

- *M:* 42
- *h:* 7
- *GF(p):* 460
- *M:* 28
- *h:* 8
- *Mensaje a codificar: TEST*

Mensaje Codificado:
$(148, 13), (34, 64), (141, 50), (148, 13)$

4.7. ElGamal

ElGamal es un cifrado de clave pública basado en curvas elípticas. Este algoritmo es con el cual realizamos el proceso de encriptación carácter por carácter, aquí se hace uso de los algoritmo declarados a lo largo de este capítulo.

4.7.1. Algoritmo ElGamal

Ahora que ya tenemos codificado el carácter con el procedimiento anterior, procedemos a realizar el algoritmo de encriptación de clave pública ElGamal, como parámetros tendremos una curva elíptica de tipo $y^2 = x^3 + ax + b$ y un grupo GF(p) con p primo y un carácter codificado previamente por el algoritmo de Codificación Bajo Curvas Elípticas(Algoritmo 6) es decir el punto $p(x, y)$.

Algoritmo 9 ElGamal

Entrada: $p(x, y)$,curva,grupo,puntoBase(x,y)

Salida: p(x_1, y_1, x_2, y_2)

1: Se obtiene la clave secreta del usuario A y del usuario B
2: cA =Diffie-Hellman
3: cB =Diffie-Hellman
4: Se obtiene la clave publica del usuario A y del usuario B multiplicando $cA * puntoBase$
5: cpA=SumaPuntosKveces
6: cpB=SumaPuntosKveces
7: Así se obtiene el par de claves de cada usuario
8: $A = cA, cpA$
9: $B = cB, cpB$
10: Se obtiene un numero aleatorio k dentro del grupo
11: Se calcula $PO = k * p$ y $PO + K * cpB$
12: Se obtiene la pareja$E = PO(x, y), PO + K * cpB(x, y)$
13: **devolver** E

Ejemplo 12 *Supongamos los siguientes parámetros para el ejemplo:*

- *Curva elíptica:* $y^2 = x^3 + 34x + 25$
- *M:* 42
- *h:* 7
- *GF(p):* 460
- *Clave A:* 3
- *Clave B:* 7
- *Mensaje a codificar: TEST*

Mensaje Codificado:
$((399, 710)(148, 13)), ((67, 83)(34, 64)), ((210, 76)(141, 50)), ((234, 25)(148, 13))$

4.8. Decodificación

El proceso de decodificación se realiza con los puntos obtenidos del cifrado con El-Gamal visto anteriormente, se necesita una curva elíptica del tipo :$y^2 = x^3 + ax + b$, nuestro elemento M y h así como el grupo $GF(p)$, para este proceso se utiliza el siguiente algoritmo.

Algoritmo 10 Decodificación

Entrada: clave$B$,parejadePuntos$PO(x, y), PO + K * cpB(x, y), h$
Salida: carácter

1: Se multiplica la clave privada de B por el primero de los puntos recibidos
2: punto=clave$B * PO(x, y)$
3: Se resta el segundo punto que envió el usuario A menos el punto obtenido $Pe = (PO + K * cpB(x, y)) - punto(x, y)$
4: Se debe recordar que $p(x, y)$ tiene a su negativo $-p(x, -y)$ es decir se puede sustituir la operación resta por la suma del negativo de punto $Pe = (PO + K * cpB(x, y)) + punto(x, -y)$
5: Una vez que se obtiene $Pe(x, y)$ se realiza una división $c = \frac{Pe(x)}{h}$
6: Se obtiene la parte entera de este resultado convirtiéndolo en carácter c
7: **devolver** c

Ejemplo 13 *Supongamos los siguientes parámetros para el ejemplo:*

- *Curva elíptica:*$y^2 = x^3 + 34x + 25$
- *M:*42
- *h:*7
- *GF(p):*460
- *Mensaje a decodificar:* $(148, 13), (34, 64), (141, 50), (148, 13)$

Mensaje Decodificado:
TEST

Capítulo 5

Resultados

Dentro del Servicio Social de la Facultad de Ciencias de la Computación se maneja información sensible de los alumnos inscritos, como nombre, teléfono, dirección, matrícula, etc. para resguardar y asegurar la confidencialidad de esta información se creó una Aplicación Web en la que nos fué posible incorporar el proceso de criptografía con curvas elípticas.

5.1. Elementos del Sistema

Para la construcción del sistema se tomó la decisión de hacer uso del lenguaje PHP (Hypertext Preprocessor)[15], es un lenguaje de código abierto orientado especialmente para el desarrollo Web interpretado del lado del servidor, y de carácter multiplataforma, uno de los lenguajes más usados actualmente para el desarrollo de aplicaciones web, así como del gestor de base de datos MySQL pues el conjunto de estas herramientas nos permite realizar de una manera más sencilla aplicaciones Web[13].

5.1.1. Base de Datos

La base de datos del proyecto se realizó con MySQL, un sistema de gestion de base de datos relacional open source optimizado para equipos de múltiples procesadores, tiene como filosofía principal ser un sistema de gestión de base de datos fiable y eficiente[14]. La Base de Datos (DB) contiene 5 tablas: Alumno, Programa, Dependencia, Familiar, Administrador; dentro de estas tablas se guardarán los datos encriptados, el modelo Entidad relación (ER) se puede observar en la siguiente imagen.

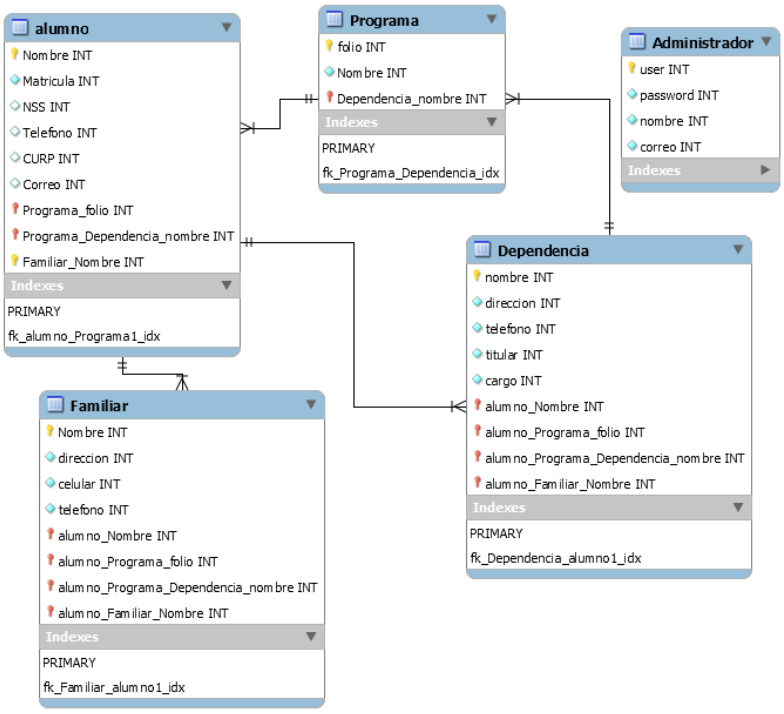


Figura 5.1: Modelo Entidad Relación DB

5.2. Aplicación Web

En esta sección se muestra el estado final de la Aplicación Web junto con el sistema criptográfico realizado para que se puedan visualizar los resultados de la incorpora-

ción del diseño Web y la programación del sistema criptográfico.

5.2.1. Aplicación Web Final

La vista General de la Aplicación Web muestra todo lo que puede realizar el alumno, como verificar los horarios de atención, el proceso de termino del SS, consultar los programas, descargar los formatos necesarios para el término del servicio, visitar la sección de preguntas frecuentes y realizar su inscripción al SS.

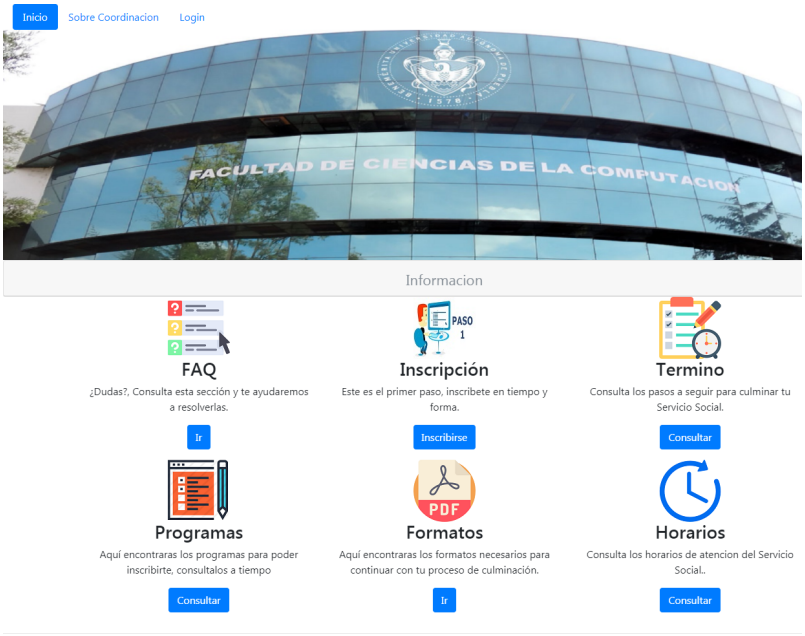


Figura 5.2: Vista General de la Aplicación Web

Inscripción

Dentro del apartado de inscripción es donde el alumno deberá ingresar los datos correspondientes para que se pueda inscribir al SS, los datos que el alumno proporciona se ingresan en un formulario, dicho formulario procesa los datos del alumno.

Los alumnos deberán ingresar todos los datos que se les pide dentro del formulario para poder inscribirse al SS, como se muestra en el siguiente ejemplo.

Figura 5.3: Inscripción Ejemplo

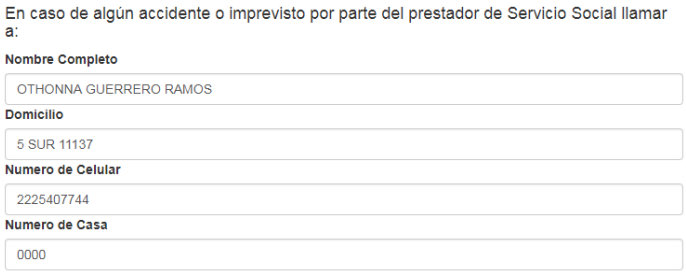


Figura 5.4: Inscripción Ejemplo

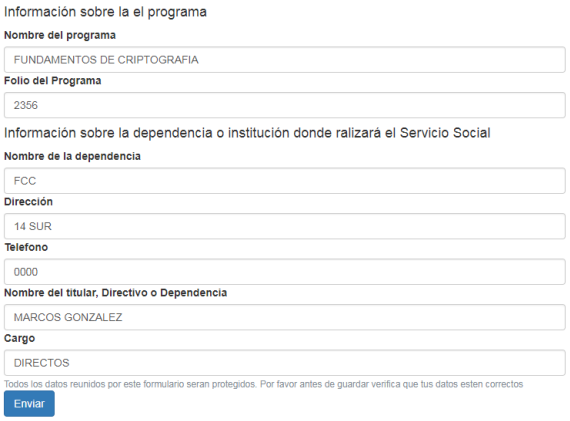


Figura 5.5: Inscripción Ejemplo

Cuando el alumno presiona el botón enviar, el sistema envía campo por campo los datos a la función que encripta, el proceso se realiza carácter por carácter partiendo de la conversión de cada uno de éstos al código ASCII correspondiente, al obtener éste código el proceso de encriptado comienza haciendo uso de los algoritmo descritos en el capítulo anterior, cuando el proceso termina se obtienen las coordenadas del carácter, estas coordenadas se insertan en la base de datos. Este proceso se realiza para todos los campos del formulario llenado por los Alumnos.

En caso de un ataque realizado a la base de datos, los atacantes no podrán visualizar los datos en claro que se enviaron en el formulario, ellos únicamente podrán observar un grupo de números, los mismo que se obtuvieron en el proceso de cifrado y se guardaron en la base de datos. En las siguientes imágenes se visualizan los registros de la base de datos.

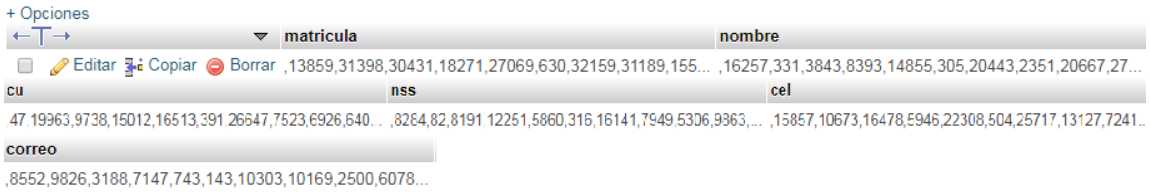


Figura 5.6: Tabla Alumno

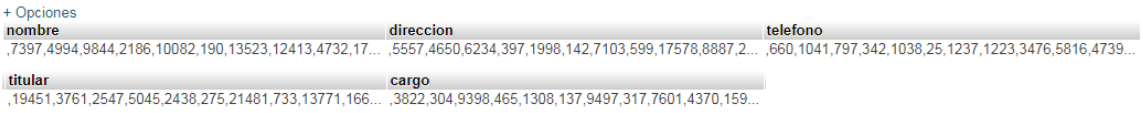


Figura 5.7: Tabla Dependencia

Figura 5.8: Tabla Familiar

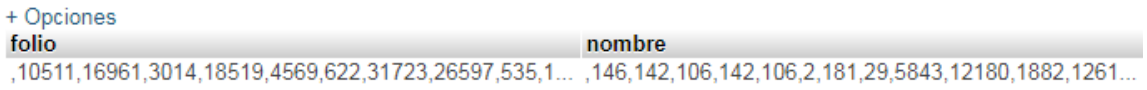


Figura 5.9: Tabla Programa

En la base de datos sólo se mostrarán números, la Coordinadora de Servicio Social es la única que podrá visualizar los datos en claro, para ésto ella tendrá que logearse en la Aplicacion web.

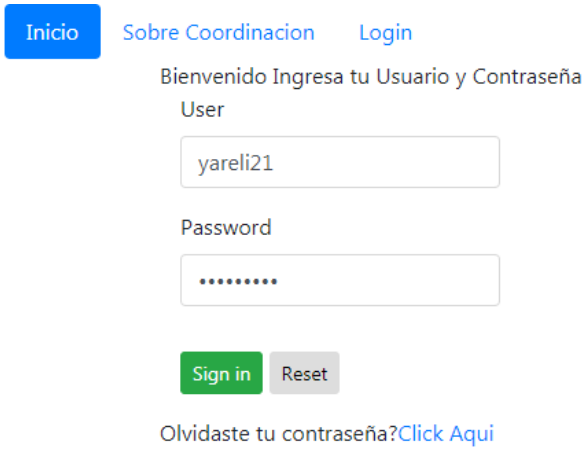


Figura 5.10: Login

Una vez logeada, la Coordinadora tendrá acceso a los 3 periodos de inscripción al Servicio Social: Primavera, Verano y Otoño.

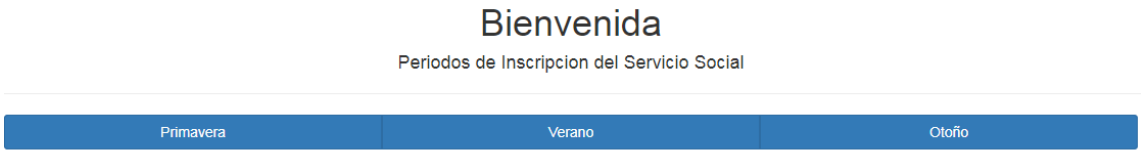
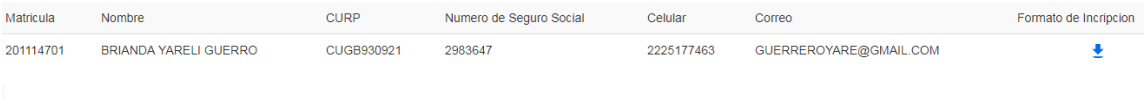


Figura 5.11: Periodos

Cuando la coordinadora seleccione uno de los periodos el sistema selecciona de la base de datos todos los registros y uno por uno los somete al proceso de desencriptado,

como se mencionó éste proceso se realiza carácter por carácter. La coordinadora podrá ver a los alumnos que hasta la fecha de consulta han mandado sus datos para la inscripción, claro está la profesora visualiza los datos de forma clara ya desencriptados.



Matricula	Nombre	CURP	Numero de Seguro Social	Celular	Correo	Formato de Incripcion
201114701	BRIANDA YARELI GUERRO	CUGB930921	2983647	2225177463	GUERREROYARE@GMAIL.COM	

Figura 5.12: Alumnos Inscritos

De esta forma se realiza el proceso de envío de datos, encriptación, resguardo y desencriptación de los datos que se obtienen de los alumnos que se inscriben al Servicio Social.

Conclusiones

Se logró cumplir con los objetivos planteados al inicio de este proyecto, pues se desarrolló satisfactoriamente una aplicación Web capaz de obtener los datos de los alumnos encriptarlos y resguardarlos con la ayuda del sistema criptográfico propuesto.

Se estudiaron y aplicaron los conceptos matemáticos para la correcta realización de los algoritmos de cifrado y descifrado estudiados a lo largo del proyecto, así como aplicar técnicas nuevas de programación.

Cabe destacar que los resultados se obtienen eligiendo parámetros válidos para el correcto funcionamiento de los algoritmos, a lo largo del proyecto se expusieron una serie de características a cumplir, por ejemplo cada parámetro para realizar la encriptación deberá estar contenido dentro del Grupo Abeliano elegido, así como resaltar que el proceso de envío de datos y encriptación se realizan en tiempo real.

Como trabajo a futuro se plantea mejorar las funciones del sistema Web, con funciones que logren ayudar a la Coordinadora del SS a la inscripción de los alumnos, como, generar archivos pdf con los datos del alumno para que la Coordinadora pueda guardarlos y tener un mejor control de los alumnos inscritos, además de subir la aplicación Web y la BD a un servidor para que eventualmente se pueda hacer uso del sistema.

Bibliografía

[1] Diffie, W. & Hellman, M. New directions in cryptography. IEEE transactions on Information Theory, 22(6), pp. 644-654(1976).

[2] ElGamal, T. A public key cryptosystem and a signature scheme based on discrete logarithms. IEEE transactions on information Theory, 31, pp. 469-472(1985).

[3] Koblitz, N. Elliptic curve cryptosystems, Mathematics of computation, 48, pp. 203-209(1978).

[4] Miller, V. Uses of elliptic curves in cryptography. Advances in Cryptology-CCRYPTO'85. Lecture Notes in Computer Science, 218, Springer-Verlag pp. 417-426(1986).

[5] Rivest, A., Shamir, A. & Adleman, L. A method for obtaining digital signatures and public key cryptosistems. Communications of the ACM, 21, pp. 120-126(1987).

[6] Granados Parede, G. Introducción a la Criptografia, pp. 5-8(2006).

[7] Alvarez, B. R.(2004) Avances en criptología y seguridad de la información. Ediciones Díaz Santos.

[8] Gómez Bello, M. La aritmética modular y algunas de sus aplicaciones (Doctoral dissertation, Universidad Nacional de Colombia)(2011),

[9] Custodio, B. M. Descifrado de información mediante internet usando el Teorema Chino de los Restos(2014).

[10] Rioseco San Martín, C. A. Introducción a la criptografía(2016).

[11] Martínez, G. Los crímenes de Oxford. Destino(2004).

[12] Hermosilla, J. C. H.(2012) Breve historia del espionaje. Ediciones Nowtilus SL.

[13] Cobo, Á.(2005). PHP y MySQL: Tecnología para el desarrollo de aplicaciones web. Ediciones Díaz Santos.

[14] Santillán, L. A. C., Ginestá, M. G., $ Mora, Ó. P. (2014). Bases de datos en MySQL. Universitat oberta de Catalunya.

[15] Welling, L., & Thomson, L. (2003). PHP and MySQL Web development. Sams Publishing.