UNIVERSIDAD DEL BÍO–BÍO
FACULTAD DE EDUCACIÓN Y HUMANIDADES
DEPARTAMENTO DE CIENCIAS DE LA EDUCACIÓN
ESCUELA DE PEDAGOGÍA EN EDUCACIÓN MATEMÁTICA

INTRODUCCIÓN A LA CRIPTOGRAFÍA

MEMORIA PARA OPTAR AL TÍTULO DE PROFESOR DE ENSEÑANZA MEDIA
EN EDUCACIÓN MATEMÁTICA

AUTORA:
RIOSECO SAN MARTÍN, CONSTANZA ALEJANDRA

Profesores Guías:
Basso Basso, Ivo Roberto
Riquelme Faúndez, Edgardo Andrés

CHILLÁN, 2016

“Dedicado a mi familia pero en especial a mis abuelos, Jorge y Gladys, quienes estuvieron presentes en cada momento, nunca dejaron de confiar en mis capacidades y ahí estaban en los momentos difíciles de mi carrera.

Gracias por todo su apoyo incondicional y por no dejarme bajar los brazos, sin ustedes esto no hubiese sido lo mismo”

INDICE

INTRODUCCION

La criptografía (cripto: oculto, logos: ciencia) es tan antigua como la escritura de hecho surge aproximadamente en la época de los romanos, ya que utilizaban códigos para ocultar sus proyectos de guerras o incluso en las tensiones diplomáticas, donde sólo podían ser descifrados por quienes conocían el código de descifrado del mensaje oculto. Actualmente se guarda, con frecuencia, información tanto de naturaleza médica como financiera en los computadores, y es de vital importancia mantenerla en secreto.

Se considera la criptografía como el nombre genérico con el que se designan dos disciplinas opuestas y a la vez complementarias:

→ Criptografía: Se ocupa del estudio de los algoritmos y sistemas que se utilizan para proteger información y dotar de seguridad. En forma más clara, se encarga de construir los procedimientos para cifrar, es decir para ocultar información confidencial.

→ Criptoanálisis: Es el opuesto a la criptografía, su objetivo es buscar el punto débil de los criptosistemas[1] para así reducir o eliminar la seguridad que teóricamente aporta este. Es decir, rompe dichos

[1] Criptosistema: se define como la quíntupla **(m,C,K,E,D)**, donde:

- **m:** conjunto de todos los mensajes sin cifrar (texto plano) que pueden ser enviados.
- **C:** conjunto de todos los posibles mensajes cifrados.
- **K:** representa el conjunto de claves que se pueden emplear en el Criptosistema.
- **E:** conjunto de transformaciones de cifrado o familia de funciones que se aplica a cada elemento de **m** para obtener un elemento de **C**.
- **D:** conjunto de transformaciones de descifrado, inverso a **E**.

procedimientos para cifrar con el fin de recuperar la información oculta.

Debemos tener en cuenta que fue considerada un arte, hasta que Claude Shannon realiza estudios sobre la Teoría de la Información (1948) y posteriormente con la publicación de su trabajo "*La Teoría de las Comunicaciones Secretas*" en 1949, en donde sugería utilizar operaciones múltiples que mezclaran transposiciones y sustituciones con cada letra del alfabeto; pero estos códigos son fáciles de romper pues pueden ser probados todos los posibles valores hasta obtener un mensaje coherente y comprensible. Por esto, la Criptografía dejó de considerarse un arte y fue considerada como una ciencia

La criptografía sólo forma parte de una comunicación secreta. Donde se requiere secreto para la comunicación, es porque existe desconfianza o peligro de que el mensaje transmitido sea interceptado por un enemigo. Este enemigo, si existe, utilizará todos los medios a su alcance para descifrar esos mensajes secretos mediante un conjunto de técnicas y métodos que constituyen una ciencia conocida como criptoanálisis. Al conjunto de ambas ciencias, criptografía y criptoanálisis se le denomina criptología.

Al ser considerada como una ciencia, existen ciertos métodos o procedimientos que nos permiten descifrar estos códigos que ocultan un mensaje en la actualidad, en este trabajo se presentará el método desarrollado en 1978 por R. L. Rivest, A. Shamir y L. Adleman y que es conocido como el MÉTODO RSA por las iniciales de sus autores.

CAPITULO I

En primer lugar debemos conocer los orígenes, respondiendo a la pregunta ¿Qué es la Criptografía? ¿Qué tan antigua es? Luego abordaremos el avance que tiene desde los años 400 a.C, pasando por la época Medieval y por la Europea que se divide en dos fases: la primera hasta el Renacimiento y la segunda del Renacimiento a la Segunda Guerra Mundial. Finalmente, destacaremos a Alan Turing un gran criptoanalista de ese tiempo.

1.1 Orígenes de la Criptografía

La criptografía surge aproximadamente en los orígenes del hombre, desde que este aprendió a comunicarse o incluso podemos mencionar que es tan antigua como la escritura. Por este motivo tuvo que encontrar medios que le permitieran asegurar parte de sus comunicaciones, o mejor dicho necesitaba mantener sus mensajes con cierta confidencialidad. El principio fundamental de la criptografía, es mantener una comunicación entre dos personas de forma que sea incomprensible por el resto.

Era considerada un arte, lo que solo duró hasta que Claude Shannon (1916 – 2001 matemático, ingeniero eléctrico y criptógrafo estadounidense), en 1949 publicó la “Teoría de las comunicaciones secretas”, la que fue aplicada por la NBS (National Bureau of Standars) de Estados Unidos para desarrollar el sistema criptográfico DES (Data Encryption Standard). Así es como la criptografía comenzó a considerarse como una ciencia aplicada,

pero ¿Por qué aplicada? Por la relación que tiene con otras ciencias, como la aritmética, estadística, teoría de números, teoría de la información y la teoría de la complejidad computacional.

Hay que tener bien claro que la criptografía corresponde sólo a una parte de la comunicación secreta. Cuando nos referimos a mantener una comunicación secreta, es porque existe desconfianza o peligro de que el mensaje que está siendo transmitido sea interceptado por un enemigo. Como este enemigo existe, va a utilizar todos los medios que tenga a su alcance para lograr descifrar los mensajes secretos mediante un conjunto de técnicas y métodos que constituyen una ciencia conocida como CRIPTOANÁLISIS. Entonces al conjunto de ambas ciencias, CRIPTOGRAFÍA y CRIPTOANÁLISIS se le denominan CRIPTOLOGÍA.

Desde el Antiguo Egipto hasta la era digital, los mensajes cifrados han sido parte importante de la Historia, arma de militares, diplomáticos y espías, son la mejor defensa de las comunicaciones y datos que recorren por Internet. No debemos olvidar que el hombre desde la antigüedad se las ha ingeniado en garantizar la confidencialidad de las comunicaciones.

La criptografía es el arte de encubrir los mensajes con signos convencionales, que sólo pueden cobrar algún sentido a través de una clave secreta que nace en conjunto con la escritura. Lo que podemos encontrar en las tablas cuneiformes, y en los papiros muestran que los primeros egipcios, hebreos, babilonios y asirios conocieron y aplicaron sus recónditas técnicas para ocultar sus mensajes. Actualmente el desarrollo de los sistemas informáticos y de las redes de comunicación, establecen los criptogramas.

1.2 Línea de Tiempo

a) Criptografía Antigua:

Disputas militares, religiosas y comerciales promovieron desde tiempos remotos el uso de escrituras secretas o mensajes secretos. Ya los antiguos egipcios usaron métodos criptográficos.
Por ejemplo, los sacerdotes egipcios utilizaron la escritura hierática (jeroglífica) que era claramente incomprensible para el resto de la población. Los antiguos babilonios también utilizaron métodos criptográficos en su escritura cuneiforme.

Aproximadamente en el 400 a.C, los espartanos montan el primer sistema de criptografía por transposición denominado SCITALA. Esta se caracteriza por ser un palo o bastón en el cual se enrollaba en espiral una tira de cuero. Sobre esa tira se escribía el mensaje en columnas paralelas al eje del palo. La tira desenrollada mostraba un texto sin relación aparente con el texto inicial, pero que podía leerse volviendo a enrollar la tira sobre un palo del mismo diámetro que el primero.

El método la SCITALA era considerablemente sencillo, como también lo era el que estableció JULIO CESAR, basado en la sustitución de cada letra por tres puestos más allá en el alfabeto denominado cifrado de César, el cual consiste en un tratamiento matemático basado en asignar a cada letra un número $(A = 00,\ B = 01, C = 02, \dots Z = 25)$, considerando un alfabeto de 26 letras, la transformación criptográfica en términos matemáticos se puede explicar por la congruencia, es decir:

$$C \equiv M + 3 \ (mod\ 26)$$

$M, corresponde\ a\ la\ letra\ del\ mensaje\ original\ .$
$C, letra\ correspondiente\ a\ M\ pero\ en\ el\ mensaje\ cifrado.$

Este algoritmo es tan básico que ni siquiera posee clave, lo que se reduce a una simple resta de 3 números del orden de las letras del criptograma del alfabeto.

Ejemplo:

Asumamos el alfabeto de 26 símbolos como el siguiente:

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
00	01	02	03	04	05	06	07	08	09	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25

Vamos a cifrar el mensaje **PAZ**

Usando el algoritmo tenemos:

1. Reemplazamos el valor de la primera letra, es decir P equivale a 15
2. Realicemos la operación

$$C \equiv (15 + 3)(mod\ 26) \Rightarrow C \equiv (18)(mod\ 26)$$

3. El numero obtenido es 18 lo que corresponde a la letra S
4. De igual forma efectuamos lo mismo para las letras siguientes.

Finalmente obtenemos los siguientes:

P	S
A	D
Z	C

Así el mensaje codificado es **SDC** y el descodificado es **PAZ**.

- ## El método de Polybios

Se denomina así, gracias a un escritor griego (Grecia, 200 a.C – 118 a.C) que poseía el mismo nombre. Su método consistía en colocar las letras del alfabeto en una red cuadrada de $5x5$, el cifrado se basaba en corresponder cada letra del alfabeto a un par de letras que indicaba la fila y columna.

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

Ejemplo:

DESEAMOS LA PAZ

Lo que se convertirá en: **ADAEDCAEAACBCDDC CAAA CEAAE**

Al introducir al tablero de Polybios números, obtenemos lo siguiente:

	1	2	3	4	5
1	A	B	C	D	E
2	F	G	H	I, J	K
3	L	M	N, Ñ	O	P
4	Q	R	S	T	U
5	V	W	X	Y	Z

De esta forma cada letra está representada por dos números, por el de su fila y por el de su columna. Así, $H = (2, 3)$; mientras que en el caso de la N y Ñ poseen la misma numeración, quedando de la siguiente forma:
$N = (3,3), \tilde{\text{N}} = (3,3)$.

Aplicando lo anterior el mensaje **DESEAMOS LA PAZ** se transforma en la siguiente codificación numérica:

$$1415431511323443\ 3111\ 351155$$

Hasta ahora hemos visto tres métodos o sistemas en que los que se basa la criptografía (SCITILA, CIFRADO DE CESAR Y POLYBIOS), los que hacen uso tanto de la transposición y sustitución.

En el caso del cifrado de César y el método de Polybios son ejemplos de sustitución, lo que significaba que a cada una de las letras del mensaje original tiene una correspondencia fija con el mensaje cifrado. En cambio el Scitala espartana es un claro ejemplo de transposición, es decir las letras simplemente se cambian de posición o se transponen, así las letras pasan a ser las mismas tanto en el texto original como en el cifrado.

b) Criptografía Medieval.

Gracias a lo simple que es la sustitución, se mantuvo presente a lo largo del primer milenio de nuestra era, considerado en aquella época como una sustitución indescifrable. En 1987 se realiza un redescubrimiento en la ciudad de Bagdad, cuando **Al-Kindi**[2] publica el tratado más importante llamado "Sobre el desciframiento de mensajes criptográficos".

En breves dos párrafos Al Kindi plantea el cómo resolver los enigmas criptográficos:

"Una manera de resolver un mensaje cifrado, si sabemos en qué lengua está escrito, es encontrar un texto llano escrito en la misma lengua, suficientemente largo, y luego contar cuantas veces aparece cada letra. A la letra que aparece con más frecuencia la llamamos "primera", a la siguiente en frecuencia la llamaremos "segunda"....y así hasta que hayamos cubierto todas las letras que aparecen en nuestro texto. Luego observamos el texto cifrado que queremos resolver y clasificamos sus símbolos de la misma manera. Encontramos el símbolo que aparece con mayor frecuencia y lo sustituimos por la "primera" de nuestro texto, hacemos lo mismo con la "segunda" y así sucesivamente, hasta que hayamos cubierto todos los símbolos del criptograma que queremos resolver".[3]

[2] Su nombre original es Abu Yusuf Yaqub ibn Ishaq al-Sabbah Al-Kindi (801-873), de procedencia árabe. Se destacó por ser un importante filósofo árabe y un estudioso de las Ciencias y por publicar más de 300 escritos

[3] En el libro de Simón Singh (pág. 36-41) se puede ver un ejemplo resuelto siguiendo las normas de Al Kandi.

Lo anterior se logra facilitar a través de las frecuencias relativas de las letras y de algunas palabras frecuentes, para ello observa las siguientes tablas respectivamente:

Letras de alta frecuencia		Letras de frecuencia media		Letras de frecuencia baja	
Letra	Frecuencia %	Letra	Frecuencia %	Letra	Frecuencia %
e	16,78	r	4,94	y	1,54
a	11,96	u	4,80	q	1,53
o	8,69	i	4,15	b	0,92
l	8,37	t	3,31	h	0,89
s	7,88	c	2,92	El resto de las letras: g,f,v,w,j,z,x,k tienen frecuencias inferiores a 0.5% y se pueden considerar por tanto "raras":	
n	7,01	p	2,76		
d	6,87	m	2,12		

Palabras más frecuentes		Palabras de dos letras		Palabras de tres letras		Palabras de cuatro letras	
Palabra	Frecuencia (por diezmil)	Palabra	Frecuencia (por diezmil)	Palabra	Frecuencia (por diezmil)	Palabra	Frecuencia (por diezmil)
de	778	de	778	que	289	para	67
la	460	la	460	los	196	como	36
el	339	el	339	del	156	ayer	25
en	302	en	302	las	114	este	23
que	289	se	119	por	110	pero	18
y	226	un	98	con	82	esta	17
a	213	no	74	una	78	años	14
los	196	su	64	mas	36	todo	11
del	156	al	63	sus	27	sido	11
se	119	es	47	han	19	solo	10
las	114						

Considerando las tablas anteriores podemos realizar un pequeño resumen sobre algún texto:

- ✓ Las vocales ocuparán alrededor del 47% del texto.
- ✓ Las vocales e y a poseen cierta seguridad, porque destacan por sobre las demás. De hecho, entre las dos ocupan el 25% del mensaje.
- ✓ En las letras de alta frecuencia se aprecia un 68% del total.
- ✓ Las consonantes más frecuentes: $l, s, n;\ d$ (alrededor del 30%).
- ✓ Las seis letras menos frecuentes: v, ñ, $j, z, x;\ k$ (poco más del 1%).
- ✓ Las palabras más frecuentes (de, la, el, en) que ocuparán el 30% del texto.

Recordemos que el análisis de frecuencias, fue desarrollada en primera instancia por los árabes cuando buscaban la frecuencia de las palabras que aparecían en el Corán para ilustrar la cronología de las palabras del Profeta.

Ejemplo:

Descifremos la siguiente frase célebre de Galileo Galilei:

TATIG NK KTIUTZXGJU ATG VKXYUTG ZGT OMTUXGTZK WAK TU YK VAKJG GVXKTJKX TGJG JK KRRG

Primero se debe contar las letras que aparecen en el mensaje secreto. Aquellas con mayor frecuencia le asignamos las letras A ó E (destacan en la tabla anterior); entonces las letras más repetidas son la $G\ y\ K$, correspondiendo a las letras A ó E.

El siguiente grupo de letras a encontrar es $O, L, S, N; D$ y así sucesivamente con las demás letras para poder leer el mensaje original**.**

De esta forma el mensaje descifrado es:

NUNCA HE ENCONTRADO UNA PERSONA TAN IGNORANTE QUE NO SE PUEDA APRENDER NADA DE ELLA.

c) Criptografía Europea hasta el Renacimiento.

- **Precursores Europeos:**

El monje franciscano Roger Bacon (1220 – 1292) escribió el primer libro europeo donde se refiere al uso de la criptografía, denominado La Epístola sobre las obras de arte secretas y la nulidad de la magia, aquí describen siete métodos distintos para mantener en secreto los mensajes.

Las personas se dedicaban en su gran mayoría a la criptografía ya que estaban conscientes que los análisis de frecuencia eran vulnerables al momento de ser cifrados. Así es como utilizaron dos cifrados que permitían combatir contra el estudio de frecuencias, estos son: los homófonos y las nulas. Los primeros trabajan con los alfabetos normales (26 letras), pero se añaden algunas letras nuevas como: ♦ ♣ ♥ ♠ que corresponden a las letras con mayor frecuencia. En cambio en el segundo cifrado se incluyen al mensaje original algunas letras con falta de significado y que no obstruyen su comprensión, conviene utilizar las letras nulas aquellas que tiene poco frecuencia para no alterar el mensaje.

Ejemplo:

Cifrado Homófonos.	**Cifrado Nulo.**
Al cifrar el siguiente texto: **el río está limpio** se convierte en: F♣ ♠KZ FIDG ♣BMTKS. Utilizando un alfabeto por sustitución[4].	Cifrar el siguiente mensaje: **lla pazz no hha sidto ffirdmadoa**, cuando el mensaje llegue a su destino el descifrador no tiene problemas para recuperar el mensaje original: **LA PAZ NO HA SIDO FIRMADA.**

En esta época la criptografía se basaba netamente en cifrados mono - alfabéticos, lo que se refiere a que la sustitución clave, una vez elegida, no es modificada hasta terminar el cifrado del mensaje. No debemos olvidar que también existían cifrados mediante dos o más alfabetos, donde se iban alternando letra a letra con el fin de confundir al criptoanalista.

Lo anterior dio paso a un gran salto cualitativo por el hecho de pasar de cifrados mono – alfabéticos a cifrados poli – alfabéticos, donde se destaca León Battista Alberti (1402 – 1472) por crear la primera máquina criptográfica que consiste en dos discos centrados que giran en forma independientes, con el fin de obtener en cada giro un alfabeto de transposición. Él es considerado el abuelo de la criptología.

[4]

Alfabeto original	a	a	b	c	d	e	e	f	g	h	i	i	j	k	l	m	n	o	o	p	q	r	s	t	u	v	w	x	y	z
Alfabeto cifrado	G	V	♦	X	C	♥	F	P	A	W	K	B	N	E	♣	M	L	Z	S	T	Q	♠	I	D	Y	O	R	J	U	H

También existía la idea de reforzar los cifrados mono – alfabéticos a través de los códigos[5], el objetivo es sustituir una palabra o varias por un determinado código.

Ejemplo:

Al cifrar el texto: Capturar al rey de Francia y atravesar el rio Sena.

Flandes = ⊕	Rey de Francia = ⊗	Reina de Inglaterra =	
Río Sena = ℵ	Reina de Escocia = Φ	Almirante = ϑ	Capturar =13
Matar = 34	hoy = 45	mañana = 56	atravesar = WD

Obtenemos como mensaje 13-⊗-WD-ℵ codificado.

Si bien se puede considerar que los códigos son más seguros para codificar pero a la misma vez es imprescindible redactar un libro con códigos, que lo más probable tendría cientos de páginas. Además este libro debería ser distribuido tanto a embajadores como a militares, y en caso que este libro llegue a manos de los criptoanalistas se produciría una catástrofe. Por este motivo los criptógrafos comprendieron las dificultades de los cifrados por códigos, por lo que se decidieron utilizar en sus mensajes sistemas híbridos y de nomencladores[6].

[5] Técnicamente, un código se define como una sustitución al nivel de las palabras o frases codificadas

[6] Un nomenclátor es un sistema de codificación que se basa en el alfabeto cifrado, el cual se utiliza para codificar la mayor parte del mensaje, y en una lista limitada de palabras o frases codificadas.

d) Criptografía en Europa: Desde el Renacimiento hasta la Segunda Guerra Mundial.

- **Blaise Vigenere:**

En el siglo XVI Vigenere, desarrollo la teoría de la criptología poli – alfabética, transformándose su nombre en uno de los métodos más famosos de sustitución poli – alfabética, actualmente recibe el nombre de “tablero de Vigenere”. Este radica en la disposición de un alfabeto de 26 letras de Cesar. Además se incorpora al cifrado una palabra clave para mantener protegido el mensaje que se repite en forma constante a lo largo de todo el mensaje a cifrar.

Antes de conocer como cifrar un mensaje, debemos saber cómo funciona el tablero Vigenere (ver página siguiente): donde cada fila representa un alfabeto distinto y cada columna constituye el cifrado de las letras, por ejemplo consideremos la fila 4 que representa al alfabeto E donde la letra K se transforma en la letra O, de esta forma se logra cifrar el mensaje deseado.

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

NOTA

El alfabeto A (fila 0) no sufre ninguna modificación ya que corresponde al abecedario original, es decir la letra B va seguir siendo B y así sucesivamente.

Entonces para cifrar un mensaje se deben seguir los siguientes pasos:

- ✓ Buscar una palabra clave fácil de recordar.
- ✓ Bajo el texto original se escribe la palabra clave tantas veces sea necesario.
- ✓ Ahora cada letra del texto original está asociado a cada letra de la palabra clave, lo que a su vez corresponde a un alfabeto distinto.

Ejemplo:

Consideremos la palabra clave: **AZUL**.

El texto a codificar es: **EL EJÉRCITO ESTÁ PREPARADO**.

E	L	E	J	E	R	C	I	T	O	E	S	T	A	P	R	E	P	A	R	A	D	O
A	Z	U	L	A	Z	U	L	A	Z	U	L	A	Z	U	L	A	Z	U	L	A	Z	U

Usando el tablero de Vigenere, tenemos que la primera letra del mensaje (E) corresponde al alfabeto A donde la letra E se transforma en E, luego el alfabeto Z la letra L se transforma en K, en el alfabeto U la letra E se transforma en Y, en el alfabeto L la letra J se transforma en U…. En forma análoga obtenemos la codificación de cada una de las letras del texto según el alfabeto correspondiente.

Finalmente el texto a codificar queda de la siguiente forma:

EK YUEQWTTN YDTZ JCEOUCACI

Cabe descartar que este sistema fue ignorado por bastante tiempo aproximadamente por casi dos siglos. Algunas de las causas por las cuales no se utilizaba este método puede ser por el uso extendido, por parte de los criptógrafos, por cifras mono – alfabéticas y por sobre todo la dificultad de utilizar las cifras poli – alfabéticas.

- ## El Código Morse.

No es considerado una forma criptográfica, por lo que no trata de ocultar un mensaje. Pero si es considerado un alfabeto alternativo que permite transmitir mensajes de manera más simple. Para poder transmitir un mensaje secreto utilizando este tipo de código se necesita que el telegrafista lo codifique antes de remitirlo.

No podemos olvidar que la tabla de Vigenere se convirtió en las mejores formar de asegurar los mensajes secretos.

Cabe mencionar que cada una de las letras del abecedario representa un código Morse y lo mismo ocurre con los dígitos, como se muestra a continuación:

Símbolos del código Morse Internacional

SIGNO	CÓDIGO	SIGNO	CÓDIGO	SIGNO	CÓDIGO	SIGNO	CÓDIGO
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	--..		
1	.----	2	..---	3	...--	4	....-
5	.....	6	-....	7	--...	8	---..
9	----.	0	-----				

- ## Charles Babbage

Charles Babbage (1791 – 1871) considerado un genio del siglo XIX, matemático inglés y científico informático. Fue la primera persona que tuvo la idea de lo que hoy conocemos como computador, aproximadamente en 1820 se interesó por las distintas herramientas que permitían calcular; aquí es donde la condesa Ada Byron (Hija del poeta Lord Byron) lo ayudó económicamente para desarrollar dos calculadoras o máquinas de números.

La primera consistía en un dispositivo que resolvía ecuaciones polinómicas por el método diferencial y la segunda era una máquina analítica donde solucionaba cómputos en general. Las dos máquinas eran en su totalidad mecánicas, por que usaban ejes, engranajes y poleas para poder obtener los cálculos. No debemos olvidar que ningunas de las dos máquinas logró construirlas completamente.

Hacia el año 1854, fue capaz de descifrar la llamada cifra de Vigenere. Este descubrimiento fue utilizado por los ejércitos ingleses en le Guerra de Crimea, permitiéndoles cierta ventaja sobre los métodos criptográficos de su enemigo: el ejército Ruso. Por esta razón, sus hallazgos en criptografía se ocultaron hasta su muerte y lograron ser publicados recién el siglo XX.

- ## La cifra del barón Lyon Playfair

Este cifrado fue inventado aproximadamente en el año 1845, por su amigo Charles Wheatstone, pero el procedimiento de este tipo de cifrado se le atribuye al científico Lyon Playfair. Se usaba principalmente en comunicaciones telegráficas secretas.

Consiste en separar el texto original en diagramas y realizar el cifrado mediante una matriz alfabética de $5x5$ donde encontramos las 26 letras del alfabeto, además se empleaba una palabra clave lo que permitía mayor seguridad al mensaje.

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

Matriz de Playfair original (sin clave)

Pero, ¿En qué consiste el cifrado de la Matriz de Playfair?

En primer lugar se incorpora al principio de la matriz la palabra clave que permite obtener una mayor seguridad y luego el resto de las letras del alfabeto en orden.

Observación

Las letras de la palabra clave se deben sustituir al momento de incorporar las letras del abecedario que faltan, para que no se repitan y éste este completo.

Ahora se debe seguir los siguientes pasos:

1. El mensaje original se debe dividir en diágrafos, es decir en pares de letras.
2. Las letras de los diágrafos tienen que ser diferentes, en caso contrario hay que incorporar un x con el fin de romper con la igualdad.

Hay que tener claro que pueden surgir los siguientes casos:

i. Cuando las letras del diágrafo están en igual fila y diferente columna, se debe desplazar cada letra una columna a la derecha. Si la letra se ubica al final de la fila, se reemplaza por la que está al principio.
   Matemáticamente: $(a_{ij}, a_{ik}) \Rightarrow (a_{ij}+1, a_{ik}+1)$

ii. Si las dos letras del diágrafo están en la misma columna y en diferente fila, debemos desplazar cada letra una columna hacia abajo. Si la letra se ubica al final de la columna, se reemplaza por la que está al principio.
Matemáticamente: $(a_{ik}, a_{jk}) \Rightarrow (a_{(i+1)j}, a_{(j+1)k})$

iii. Finalmente si los diágrafo están en diferente fila y columna, la operación matemática es la siguientes: $(a_{ki}, b_{js}) \Rightarrow (a_{ks}, b_{ji})$

Ejemplo:

Clave: **MAR**

Mensaje original: **SE HA MAREADO HOY**

Diágrafos del mensaje: **SE – HA – MA – RE – AD – OH – OY.**

La matriz Playfair es:

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

→ **SE** (ambas letras están en distinta fila y columna) transformándose en **QF**

→ **HA** (ambas letras están en distinta fila y columna) transformándose en **EC**

→ **MA** (las letras están en la misma fila pero diferente columna) transformándose en **AR**

→ **RE** (ambas letras están en distinta fila y columna) transformándose en **AF**

→ **AD** (ambas letras están en distinta fila y columna) transformándose en **ME**

→ **OH** (ambas letras están en la misma columna pero diferente fila) transformándose en **UO**

→ **OY** (ambas letras están en distinta fila y columna) transformándose en **NZ.**

Así el mensaje codificado toma la siguiente forma:

QF – EC – AR – AF – ME – UO – NZ.

- ## La cifra ADFGVX

La primera Guerra Mundial fue una guerra a gran escala, por lo que se necesitó de audacia para codificar mensajes en forma rápida y efectiva. Es por esto que la famosa cifra ADFGVX es una mezcla de métodos de

sustitución y transposición, lo que hace que los desciframientos sean evidentemente complicados.

¿Cómo se cifra mediante ADFGVX?

Se debe disponer de las 26 letras del alfabeto y de los diez dígitos distribuidos en una matriz de $6x6$, las filas y columnas van encabezadas por las sucesivas letras **A D F G V X**. El orden de letras y números es en forma aleatoria pero se debe informar aquel orden, al receptor del mensaje.

Ejemplo:

	A	D	F	G	V	X
A	0	Q	9	Z	7	C
D	M	U	1	H	F	2
F	4	8	W	N	R	G
G	L	6	V	T	P	A
V	Y	3	D	5	E	K
X	J	S	I	O	B	X

El mensaje cifrado se obtiene sustituyendo cada letra correspondiente a la fila y columna de la letra que está siendo codificada. Por ejemplo el numero 4 es sustituido por las letras FA y la letra K por el par de letras VX.

Entonces al codificar el siguiente mensaje: **ENVÍEN MUNICIONES**, queda de la siguiente forma:

VVFGGFXFVVFGDADDFGXFAXXFXGFGVVXD.

Solo hasta el momento hemos visto un cifrado por sustitución, lográndose descifrar por un análisis de frecuencia. Ahora la fase de transposición consiste en utilizar una palabra clave, por ejemplo la palabra clave es **WHISKY**; las letras de la palabra clave se escriben en el comienzo de la cuadricula (en la parte superior) y el mensaje anteriormente codificado se escribe en filas hacia el lado quedando de la siguiente manera:

W	H	I	S	K	Y
V	V	F	G	G	F
X	F	V	V	F	G
D	A	D	D	F	G
X	F	A	X	X	F
X	G	F	G	V	V
X	D	A	A	A	A

Como en los últimos 4 espacios de la última fila quedaban libres del mensaje cifrado, se rellenan con A.

Finalmente ordenamos la palabra clave en orden alfabético en conjunto con sus columnas correspondientes, es decir:

H	I	K	S	W	Y
V	F	G	G	V	F
F	V	F	V	X	G
A	D	F	D	D	G
F	A	X	X	X	F
G	F	V	G	X	V
D	A	A	A	X	A

Ahora leemos columna a columna el mensaje cifrado:

VFAFGD FVDAFA GFFXVA GVDXGA VXDXXX FGGFVA

Si se deseara cifrar el anterior mensaje mediante el código Morse, existe un gran porcentaje de que el mensaje sea descifrado por el hecho que contiene solamente 6 letras.

El 2 de Junio de 1918, el criptoanalista Georges Painvin, fue capaz de descifrar un mensaje mediante la cifra de ADFGVXX.

- ## Auguste Kerckhoffs y sus reglas

No debemos olvidar que la Primera Guerra Mundial se caracterizó por el uso de la criptografía. El holandés Auguste Kerckhoffs, estudió los distintos sistemas criptográficos, lo que se logra visualizar en su artículo titulado “La Cartografía Militar” donde menciona que estos sistemas cumplen ciertas reglas, que son las siguientes:

1. No existe ninguna forma de recuperar el texto original a partir del criptograma. (seguridad en el primer ataque)
2. Los sistemas criptográficos deben estar compuestos por dos tipos de información:

a) Pública: familia de algoritmos que definen el sistema criptográfico.
b) Privada: conocida solo por el usuario y es particular.

3. La clave deber ser fácil de recordar y de poder modificar.
4. La comunicación entre el criptograma y los medios de transmisión habituales deben ser posibles.
5. La complejidad del proceso de descodificación del mensaje o texto original depende exclusivamente del costo proporcional al secreto que se desea guardar.

Las reglas recién planteadas están referidas a las reglas militares aceptadas mundialmente.

• Alan Turing.

Nace en 1912 en Londres, se destacaba por tener un carácter retraído. En 1936 conoce a Gödel y Von Newman, transformándose en colaborador de este último. En 1948 alcanzó el puesto de profesor en la Universidad de Manchester.

Durante la Segunda Guerra Mundial, fue solicitado por el gobierno inglés para trabajar en Bletchley Park, a donde se ejecutaban trabajos criptográficos para destruir los códigos de las famosas máquinas Enigma

que utilizaban los alemanes para cifrar mensajes. Turing destacó por su trabajo y por crear la máquina BOMBE, que consistía en descifrar códigos nazis, lo que fue fundamental en el desarrollo de la Guerra.

Turing se inspira en el décimo problema de Hilbert:

"*Dada una ecuación diofántica*[7] *con cualquier número de incógnitas y con coeficientes numéricos racionales enteros: Idear un proceso de acuerdo con el cual pueda determinarse, en un número finito de operaciones, si la ecuación es resoluble en números racionales enteros"*.

Para construir la famosa máquina de Turing, que sentó las bases de los computadores actuales.

Gracias a su importante rol en le II Guerra Mundial se realizó la película *"The Imitation Game":*

En el invierno de 1952, ingresan al hogar de Alan Turing, interpretado por Benedict Cumberbatch, con el fin de indagar un robo; fue arrestado por ser homosexual lo que es considerado una ofensa criminal.

Pero los oficiales no tenían la mínima idea a quien estaban llevando tras las rejas al pionero de la informática actual. Se destacó por descifrar el código de la exitosa máquina Enigma de los alemanes en la Segunda Guerra Mundial, permitiendo salvar miles de vidas y lograr acortar esta guerra.

[7] Ecuación diofantica: ecuación algebraica que tiene dos o más incógnitas.

La película, ha ganado el OSCAR al mejor guion fue dirigida por el noruego Morten Tyldum, retrata a uno de los genios del siglo XX, el mismo que ayudó a descifrar la máquina Enigma y el mismo que fue condenado a la castración química para evitar la cárcel por su homosexualidad (ver linkografia).

En 1953, fue arrestado y sometido a un tratamiento hormonal por su homosexualidad. Y en 1954 fue encontrado muerto por la ingesta de cianuro.

No podemos olvidar que fue considerado el padre de la computación y el 2012 (año de la informática) se le otorga el homenaje de DOODLE[8].

.

[8] El famoso buscador (google) conmemora el 100 aniversario del nacimiento de Alan Turing, precursor de la informática moderna y considerado uno de los padres de la computación, cifrando su nombre en la famosa máquina de Turing.

CAPITULO II

Antes de entrar de lleno en que son y el funcionamiento de los CRIPTOSISTEMAS debemos describir y recordar cada concepto matemático con sus propiedades que permiten cifrar y descifrar mensajes, como lo es la aritmética modular en el cifrado de Cesar.

2.1 Divisibilidad y MCD

Definición Divisibilidad:

Sea $a, b \in \mathbb{Z}; a \neq 0$. Se dice que a divide a b o que b es divisible por a si y solo si existe $k \in \mathbb{Z}$ tal que:

$$k \cdot a = b$$

- Se anota $a \mid b$ para indicar la divisibilidad.
- Cuando no hay divisibilidad se anota $a \nmid b$

Proposición:

Si $a, b \, y \, c \in \mathbb{Z}$, tenemos:

a) $a/b \wedge b/c \Rightarrow a/c$

b) $a/b \Rightarrow ac/bc, con\ c \neq 0$

c) $a/b \wedge b/a \Rightarrow a = \pm b$

d) $a/\pm 1 \Leftrightarrow a = \pm 1$

e) $c/a \wedge c/b \Rightarrow c/(ax + by),\ para\ todo\ x, y \in \mathbb{Z}$

Ejemplo:

$$c/a \wedge c/b \Rightarrow c/(a^2 + b^2), con\ x = a\ ; y = b$$

$$c/a \wedge c/b \Rightarrow c/ab,\ con\ x = b; y = 0$$

Máximo Común Divisor (MCD)

Definición:

Sea $a, b \in \mathbb{Z}$, ambos no nulos. El máximo común divisor (MCD) de $a\ y\ b$ es un entero positivo d tal que:

- $d/a \wedge d/b$
- Si $k/a \wedge k/b \Rightarrow k/d$

Es decir d es el mayor de los divisores comunes entre $a\ y\ b$. Se anota como $mcd(a, b)$.

Teorema de Euclides:

Si $a, b \in \mathbb{Z}; b > 0$ entonces existen únicos enteros $q \wedge r$ tal que:

$$a = bq + r\ ; 0 \leq r < b$$

Los enteros $q \wedge r$ reciben el nombre de cociente y residuo, respectivamente.

Cálculo del mcd mediante el Algoritmo de Euclides:

Sean a , b números positivos y supongamos que $a > b$

$$a = q_1\, b + r_1, \quad 0 \leq r_1 < b$$

$$b = q_2\, r_1 + r_2; \quad 0 \leq r_2 < r_1$$

$$r_1 = q_3\, r_2 + r_3; \quad 0 \leq r_3 < r_2$$

$$\vdots \qquad\qquad \vdots \qquad\qquad \vdots$$

$$r_{k-2} = q_k\, r_{k-1} + r_k; \quad 0 \leq r_k < r_{k-1}$$

$$r_{k-1} = q_{k+1}\, r_{k-1} + 0$$

Proposición:

$$mcd\,(a, b) = r_k$$

Demostración: ver página 5 en [6]

Ejemplo:

Encuentre el $mcd\,(348, 136)$ utilizando el algoritmo de Euclides

Solución:

$$348 = 136 \cdot 2 + 76$$

$$136 = 76 \cdot 1 + 60$$

$$76 = 60 \cdot 1 + 16$$

$$60 = 16 \cdot 3 + 12$$

$$16 = 12 \cdot 1 + 4$$
$$12 = 4 \cdot 3 + 0$$

Por lo tanto el $mcd\ (348, 136) = 4$

Algoritmo de Euclides Extendido:

Sea $a\ , b$ números positivos, entonces la ecuación:

$$ax + by = mcd(a, b)$$tiene solución

Ahora escribamos el mcd cómo combinación lineal de $a\ y\ b$, es decir

$d = ax_0 + by_0$. Utilizando sustitución regresiva para encontrar x_0; $y_0$en el ejemplo anterior

$$4 = 16 + (-1)[12]$$
$$4 = 16 + (-1)[60 + (-3)16]$$
$$4 = 4 \cdot\ 16 + (-1)[60]$$
$$4 = 4 \cdot\ [76 + (-1)] + (-1)60$$
$$4 = 4 \cdot\ 76 + (-4)60 + (-1)60$$
$$4 = 4 \cdot\ 76 + (-5)60$$
$$4 =\ 4 \cdot 76 + (-5)[136 + (-1)76]$$
$$4 = 4 \cdot 76 + (-5)136 + (5)76$$
$$4 = 9 \cdot 76 + (-5)76$$
$$4 = 9 \cdot\ [348 + (-2)(136)] + (-5)136$$
$$4 = 9 \cdot 348 + (-18)136 + (-5)136$$
$$4 = 9 \cdot 348 + (-23)136$$

Así obtenemos $x_0 = 9\,, y_0 = -23$

Por lo tanto $4 = 348 \cdot 9 + 136 \cdot (-23)$

Primos Relativos

Definición:

Sean $a \wedge b$ enteros no nulos. Se dice que $a \wedge b$ son primos relativos, si y solo si $mcd(a,b) = 1$

Ejemplo: $mcd(73,25) = 1$

Corolario: $a \wedge b$ son primos relativos, si y solo si existen $x_0,\ y_0 \in \mathbb{Z}$ tal que $ax_0 + by_0 = 1$

Se pueden obtener primos relativos usando:

Proposición

Si $d = (a,b) \Rightarrow (a/d\,,\ b/d) = 1$

Demostración: ver página 7 en [6].

2.2 Aritmética Modular

Definición:

Sea m un entero positivo, donde $a, b \in \mathbb{Z}$. Se define $a \equiv b\ (mod\ m) \Leftrightarrow m/(a-b)$

Proposición:

a) $a \equiv b\ (mod\ m) \Leftrightarrow a\ y\ b$ dejan el mismo resto cuando son divididos por m.
b) La relación de congruencia $mod\ n$, es una relación de equivalencia en $\mathbb{Z}$.

Nota:

Sea $a \in \mathbb{Z}$, su clase de equivalencia en $mod\ m$ es el conjunto definido por:

$$\bar{a} = \{x \in \mathbb{Z}; x \equiv a\ (mod\ m)\}$$

¿Cuántas clases de equivalencia existen?

Hay m clases: $\{\bar{0}, \bar{1}, \ldots \overline{m-1}\}$

y $\{0, 1 \ldots, m-1\}$ se denomina conjunto completo de representantes.

Ejemplo: En $mod\ 6$.

Sabemos que $\mathbb{Z}_6 = \{0, 1, 2, 3, 4, 5\}$ y por tanto sus clases de equivalencia son $\{\overline{0}, \overline{1}, \overline{2}, \overline{3}, \overline{4}, \overline{5}\}$.

c) Sea $m \geq 1$ un entero fijo:

- Si $a \equiv b\ (mod\ m)$ y $c \equiv d\ (mod\ m)$. Entonces $a + c \equiv b + d\ (mod\ m)$.

- Si $a \equiv b\ (mod\ m)$ y $c \equiv d\ (mod\ m)$. Entonces $ac \equiv bd\ (mod\ m)$

Definición:

Sea $\bar{a}\ y\ \bar{b}$ clases de equivalencia, tenemos que:

- $\bar{a} + \bar{b} = \overline{a + b}$
- $\bar{a} \cdot \bar{b} = \overline{a \cdot b}$

d) Sea $m \geq 1$. Entonces para cualquiera $a, b, c \in \mathbb{Z}$ se desprenden las siguientes propiedades:

- $\bar{a} + \bar{b} = \bar{b} + \bar{a}$
- $(\bar{a} + \bar{b}) + \bar{c} = \bar{a} + (\bar{b} + \bar{c})$
- $\bar{a} + \bar{0} = \bar{0} + \bar{a} = \bar{a}$
- $\bar{a} + \overline{-a} = \overline{-a} + \bar{a} = \bar{0}$

- $\bar{a} \cdot \bar{b} = \bar{b} \cdot \bar{a}$
- $(\bar{a} \cdot \bar{b}) \cdot \bar{c} = \bar{a} \cdot (\bar{b} \cdot \bar{c})$
- $\bar{a} \cdot \bar{1} = \bar{1} \cdot \bar{a} = \bar{a}$
- $\bar{a} \cdot (\bar{b} + \bar{c}) = \bar{a} \cdot \bar{b} + \bar{a} \cdot \bar{c}$

De acuerdo a las propiedades anteriores de la adición y multiplicación, el conjunto de todas las clases de equivalencia $mod\, m$ es un anillo que se denota por $\mathbb{Z}/m\mathbb{Z}$ y se llama anillo cociente.

Ejemplo:

$$\mathbb{Z}/8\mathbb{Z} = \{0 + 8\mathbb{Z}, 1 + 8\mathbb{Z}, 2 + 8\mathbb{Z}, 3 + 8\mathbb{Z}, 4 + 8\mathbb{Z}, 5 + 8\mathbb{Z}, 6 + 8\mathbb{Z}, 7 + 8\mathbb{Z}\}$$

Representando las clases del anillo $(\mathbb{Z}_8, +, \cdot)$

Recordemos

Un anillo $(A, +, \cdot)$ cumple las siguientes propiedades:

- $(A, +)$ grupo abeliano.
- La multiplicación debe ser cerrada
- La multiplicación debe cumplir con la asociatividad.
- La multiplicación distribuye con respecto a la suma.

Además para que sea un anillo conmutativo, la multiplicación debe ser conmutativa. Y para que el anillo tenga unidad, la multiplicación debe poseer neutro.

Consideremos el mismo anillo anterior y sea B un subconjunto no vacío de A.

Se define:

$$B\ es\ sub-anillo\ de\ A \ \Leftrightarrow \begin{cases} a,b \in B \Rightarrow a-b \in B \\ a,b \in B \Rightarrow ab \in B \end{cases}$$

Ejemplo:

$(2\mathbb{Z},+,\cdot)$ Es un sub – anillo $(\mathbb{Z},+,\cdot)$

e) Si $m \geq 1$, entonces $\bar{a} \in \mathbb{Z}/m\mathbb{Z}$ tiene inverso multiplicativo si y sólo si $mcd\,(a,m)=1$

Los identificaremos así:

$$(\mathbb{Z}/m\mathbb{Z})^* = \{\bar{a} \in \mathbb{Z}/m\mathbb{Z} : mcd(a,m)=1\}$$

denominándolo como el grupo de unidades de $\mathbb{Z}/m\mathbb{Z}$

Ejemplo:

$$(\mathbb{Z}/24\mathbb{Z})^* = \left\{\overline{1},\overline{5},\overline{7},\ \overline{11},\ \overline{13},\overline{17},\overline{19},\overline{23}\right\}$$

2.3 Números primos, factorización única y cuerpos finitos

Definición:

Se llama número primo p al número que tiene como único divisores p y 1. Si p no es primo, se denomina como número compuesto.

Teorema Fundamental de la Aritmética:

Todo entero mayor que 1 se puede expresar como producto de números primos, siendo esta la expresión única.

Observaciones:

- Si p es un número primo. Entonces todo elemento distinto de cero en $\mathbb{Z}/p\mathbb{Z}$ tiene un inverso multiplicativo.
- Si p es n número primo, entonces el conjunto $\mathbb{Z}/p\mathbb{Z}$ de enteros $mod\ p$ con adición y multiplicación es un cuerpo.

Recordemos

$(K, +, \cdot)$ es un cuerpo si y solo si K es un anillo conmutativo, con unidad tal que todo elemento no nulo es invertible.

$\rightarrow (K, +)$ grupo abeliano

$\rightarrow (K^*, \cdot)$ grupo conmutativo.

$\rightarrow$ La multiplicación distribuye respecto de la suma.

- El cuerpo $\mathbb{Z}/p\mathbb{Z}\ (mod\ p)$ tiene solo un número finito de elementos. Este es un cuerpo finito y los denominaremos $\mathbb{F}_p$

  Ejemplo:

  $$\mathbb{Z}/5\mathbb{Z}\ (mod\ 5)$$

  $\mathbb{Z}/5\mathbb{Z} = \{0, 1, 2, 3, 4\}$ es un anillo conmutativo, con unidad y cada elemento distinto de cero es invertible.
  $\therefore$ es un cuerpo.

Teorema de Fermat:

Si p es un número primitivo y a un entero cualquiera, entonces:

$$a^{p-1} \equiv \begin{cases} 1\ (mod\ p); si\ p\ \nmid a \\ 0\ (mod\ p); si\ \ p/a \end{cases}$$

Ejemplo:

$$5^{38} \equiv ?\ (mod\ 11)$$

En primer lugar tenemos que $p = 11\ y\ a = 5\ \therefore p\ no\ divide\ a.$

Así

$$5^{10} \equiv 1\ (mod\ 11)\ /(\ )^3$$
$$5^{30} \equiv 1\ (mod\ 11)\ / \cdot 5^8$$

$5^8 \cdot 5^{30} \equiv 5^8 \ (mod\ 11)$

$5^{30+8} \equiv 5^8 \ (mod\ 11)$

$5^{38} \equiv 5^8 \ (mod\ 11)$

Trabajando con

$$5^2 \equiv 3 \ (mod\ 11) / \ (\ )^2$$
$$5^4 \equiv 9 \ (mod\ 11) / \ (\ )^2$$
$$5^8 \equiv 4 \ (mod\ 11)$$

Finalmente $5^{38} \equiv 4 \ (mod\ 11)$

Del teorema anterior se desprende la siguiente:

- Definición:
  El orden de $a \ (mod\ p)$ es el menor exponente de $k \geq 1$ tal que $a^k \equiv 1 \ (mod\ p)$.
- Proposición:
  Sea p un primo y a un entero no divisible por p. Supongamos que $a^n \equiv 1 \ (mod\ p)$. Entonces el orden de $a \ (mod\ p)$ divide a n. En particular el orden de a divide a $p - 1$.

Teorema

Sea p un número primo. Entonces existe un elemento $g \in \mathbb{F}_p$ cuyas potencias dan todos los elementos de $\mathbb{F}_p{}^*$, es decir:

$$\mathbb{F}_p{}^* = \{1, g, g^2 \ldots, g^{p-2}\}$$

Estos elementos se llamas raíces primitivas de $\mathbb{F}_p{}^*$ o generadores de $\mathbb{F}_p{}^*$, cuyo orden es $p-1$

Ejemplo:

Encontrar los generadores de $\mathbb{F}_5{}^*$.

En primer lugar, sabemos $\mathbb{Z}_5 = \{0, 1,\ 2, 3, 4, \}$

Ahora consideremos la clase de equivalencia del 3 y veamos si genera a $\mathbb{F}_5{}^*$

$3^0 \equiv 1\ (mod\ 5)$
$3^1 \equiv 3\ (mod\ 5)$
$3^2 \equiv 4\ (mod\ 5)$
$3^3 \equiv 2\ (mod\ 5)$

Lo mismo ocurre con la clase de equivalencia del 2, genera todos los elementos de $\mathbb{F}_5{}^*$

Por tanto $\mathbb{Z}_5^*$ posea dos generadores o raíces primitivas, es decir $2\ y\ 3$.

2.4 Exponenciación

Para cifrar o descifrar mensajes en algunos criptosistemas como el RSA, que estudiaremos más adelante necesitamos calcular potencias del tipo:

$$a^k\ (mod\ m)$$

Lo anterior tiene un enfoque directo, como el que sigue:

$$a \equiv a \ (mod\ m)$$
$$a^2 \equiv a_1 \cdot a \ (mod\ m)$$
$$\vdots \qquad \vdots \qquad \vdots$$
$$a^k \equiv a_{k-1} \cdot a \ (mod\ m)$$

Algoritmo para calcular potencias:

Consideremos a, k ; m enteros positivos; entonces $a^k \ (mod\ m)$ se obtiene de la siguiente forma:

a) Calcular k en base binaria

$k = k_0 + k_1 2 + k_2 2^2 + \cdots + k_t 2^t$ con $k_0, k_1 \ldots, k_t \in \{0,1\} \wedge k_t \neq 0$

Ejemplo:

El numero 39 va a ser expresado en base binaria

$$39 = 2^5 + 7$$
$$39 = 2^5 + 2^2 + 3$$
$$39 = 2^5 + 2^2 + 2^1 + 1$$
$$39 = 2^5 + 2^2 + 2^1 + 2^0$$

Entonces:

$39 = 1 \cdot 2^0 + 1 \cdot 2^1 + 1 \cdot 2^2 + 1 \cdot 2^5$

$39 = 1 \cdot 2^0 + 1 \cdot 2^1 + 1 \cdot 2^2 + 0 \cdot 2^3 + 0 \cdot 2^4 + 1 \cdot 2^5$

$39 = 1\ 1\ 1\ 0\ 0\ 1$ esta es base binaria.

b) Calculando las potencias:

$$\begin{aligned} a_0 &\equiv a \ (mod\ m) \\ a_1 \equiv\ a_0^2 &\equiv a^2 (mod\ m) \\ a_2 \equiv\ a_1^2 &\equiv a^{2^2} (mod\ m) \\ \vdots \qquad &\vdots \qquad \vdots \\ a_t \equiv\ a_{t-1}^2 &\equiv a^{2^t}\ (mod\ m) \end{aligned}$$

Observando, logramos notar que para obtener la potencia siguiente, elevamos la potencia anterior al cuadrado y obtenemos la que sigue. Si deseamos llegar de la potencia a_2 a la potencia a_3, consideremos:

$\left(a^{2^2}\right)^2 = \left(a^{2^2}\right) \cdot \left(a^{2^2}\right) = a^{2^2+2^2} = a^{2\cdot 2^2} = a^{2^3}$

$\therefore\ a_3 = a^{2^3}$

c) Calculando $a^k\ (mod\ m)$ usando la fórmula y aplicando propiedades de potencia:

$$\begin{aligned} a^k &= a^{k_0 + k_1 2 + k_2 2^2 + \cdots + k_t 2^t} \\ a^k &= a^{k_0} \cdot (a^2)^{k_1} \cdot \left(a^{2^2}\right)^{k_2} \ldots \cdot \left(a^{2^t}\right)^{k_t} \\ a^k &\equiv a^{k_0} \cdot (a^2)^{k_1} \cdot \left(a^{2^2}\right)^{k_2} \ldots \cdot \left(a^{2^t}\right)^{k_t}\ (mod\ m) \end{aligned}$$

Ejemplo:

Calcular $3^{218}\ (mod\ 1000)$

Primero llevemos $k = 218$ a base binaria

$$218 = 0 \cdot 2^0 + 1 \cdot 2^1 + 0 \cdot 2^2 + 1 \cdot 2^3 + 1 \cdot 2^4 + 0 \cdot 2^5 + 1 \cdot 2^6 + 1 \cdot 2^7$$

$$218 = 2^1 + 2^3 + 2^4 + 2^6 + 2^7$$

Luego obtenemos que:

$a^k = a^2 \cdot a^{2^3} \cdot a^{2^4} \cdot a^{2^6} \cdot a^{2^7}$; Sabemos que $a = 3$ $y\, k = 218$, entonces

$3^{218} = 3^2 \cdot 3^{2^3} \cdot 3^{2^4} \cdot 3^{2^6} \cdot 3^{2^7}$

Observemos la tabla

i	$3^{2^i}\ (mod\ 1000)$
0	3
1	9
2	81
3	561
4	721
5	841
6	281
7	961

Así

$$3^{218} = 3^2 \cdot 3^{2^3} \cdot 3^{2^4} \cdot 3^{2^6} \cdot 3^{2^7}$$

$$3^{218} \equiv 9 \cdot 561 \cdot 721 \cdot 281 \cdot 961\ (mod\ 1000)$$

$$3^{218} \equiv 489\ (mod\ 1000)$$

2.5 La función ϕ de Euler

Se define

$\phi : \mathbb{Z}^+ \to \mathbb{E}$ $(\mathbb{E} = \mathbb{R}$ ó $\mathbb{C})$

$\phi(n) = n°\ de\ enteros\ positivos\ menores\ o\ iguales\ a\ n\ y\ primos\ relativos\ con\ n$

Ejemplo:

$$\phi(12) = 4\ ;\ \phi(36) = 12$$

¿Cómo se calcular $\phi(n)$ para números grandes?

La idea principal es descomponer aquel número n. Para ello comencemos por las siguientes proposiciones:

a) *Si n es un número p primo, entonces $\phi(p) = p - 1$*

Demostración: Si p es primo, todo entero menor que p es primo relativo con p y p no es primo relativo con p; ∴ hay $p - 1$ enteros primos relativos con p.

b) Si p es primo y $\alpha \in \mathbb{Z}$, entonces $\phi(p) = p^{\alpha} - p^{\alpha-1} = p^{\alpha}\left(1 - \frac{1}{p}\right)$

Demostración: Ver página 30 en [6].

Ejemplo:

$$\phi(16) = \phi(2^4) = 2^4 - 2^3 = 8$$

c) *Si p es primo, entonces*

$$\phi(1) + \phi(p) + \phi(p^2) + \cdots + \phi(p^n) = p^n \text{ ó}$$

$$\sum_{i=0}^{n} \phi(p^i) = p^n$$

Demostración:

Tenemos que:

$$\phi(p) = p - 1$$
$$\phi(p^2) = p^2 - 1 = p\,(p-1)$$
$$\vdots$$
$$\phi(p^n) = p^n - p^{n-1} = p^{n-1}\,(p-1)$$

Al sumar obtenemos lo siguiente:

$$\phi(1) + \phi(p) + \phi(p^2) + \cdots + \phi(p^n)$$
$$= (p-1)(1 + p + p^2 + \cdots + p^{n-1}) \ *$$

Ahora al lado derecho de la igualdad aplicamos la suma de una progresión geométrica:

$$S_n = a_1 \cdot \frac{r^n - 1}{r - 1}$$

dónde:

r, es la razón de la progresión.

a_1, es el primer término de la progresión.

Conociendo la razón $(r = p)$ y el primer término $(a_1 = 1)$ de la progresión, tenemos:

$$S_n = 1 \cdot \frac{p^n - 1}{p - 1}$$

$$S_n = \frac{p^n - 1}{p - 1}$$

Entonces * queda de la siguiente forma:

$$\phi(1) + \phi(p) + \phi(p^2) + \cdots + \phi(p^n) = (p - 1)\frac{p^n - 1}{p - 1}$$

$$= p^n - 1$$

Así:

$$\sum_{i=0}^{n} \phi(p^i) = \phi(1) + p^n - 1 = p^n.$$

¿Cómo calcular $\phi(n)$, para cualquier n?

Ya conocemos $\phi(n)$ para $n = p$

Y $\phi(n)$ para $n = p^\alpha$

Ejemplo:

Calcular $\phi(72)$, o sea $\phi(2^3 \cdot 3^2)$

Ahora, los primos relativos con 72 son aquellos números que son primos relativos con 2 y 3 a la vez, es decir:

i. Sea a, cualquier número, que no es primo relativo con 2. Tampoco lo será primo relativo con 72.

   De esta forma no son primos relativos con 2, aquellos múltiplos de 2 y hay 36 $\left(\frac{72}{2} = 36\right)$ números que no son primos relativo.

ii. Lo mismo ocurre con cualquier número a, que no es primo relativo con 3. No lo será con 72.

   Entonces no son primos relativos con 3 ni tampoco los múltiplos de 3, hay 24 $\left(\frac{72}{3} = 24\right)$ números que no son primos relativos.

iii. Por último, los múltiplos $2 \cdot 3$ ya están incluidos con los casos anteriores. Hay 12 $\left(\frac{72}{2 \cdot 3} = 12\right)$ números que no son primos relativos.

Finalmente no son primos relativos

$$36 + 24 - 12 = 48$$

Y los primos relativos de 72 son:

$$72 - (36 + 24 - 12) = 24$$

Veamos el caso general para una descomposición con dos números primos.

Sea $n = p_1^{\alpha 1} \cdot p_2^{\alpha 2}$

Los primos relativos con n deben ser primos relativos con $p_1 y\, p_2$ a la vez.

Los casos siguientes no son primos relativos:

i. Múltiplos de p_1 que son $\frac{n}{p_1}$
ii. Múltiplos de p_2 que son $\frac{n}{p_2}$
iii. Múltiplos de n que son $\frac{n}{p_1 \cdot p_2}$

Por lo tanto los primos relativos con n son:

$$n - \left(\frac{n}{p_1} + \frac{n}{p_2} - \frac{n}{p_1 \cdot p_2}\right)$$

Asimismo,

$$\begin{aligned}\phi(n) &= n - \left(\frac{n}{p_1} + \frac{n}{p_2} - \frac{n}{p_1 \cdot p_2}\right) \\ &= n\left(1 - \frac{1}{p_1} - \frac{1}{p_2} + \frac{1}{p_1 \cdot p_2}\right) \\ &= n\left(1 - \frac{1}{p_1}\right)\left(1 - \frac{1}{p_2}\right)\end{aligned}$$

Ya conocemos que $n = p_1^{\alpha 1} \cdot p_2^{\alpha 2}$, reemplazando:

$$= p_1^{\alpha 1} \cdot p_2^{\alpha 2} \left(1 - \frac{1}{p_1}\right)\left(1 - \frac{1}{p_2}\right)$$

$$= p_1^{\alpha 1} \left(1 - \frac{1}{p_1}\right) \cdot p_2^{\alpha 2} \left(1 - \frac{1}{p_2}\right)$$

$$= \prod_{i=1}^{2} p_i^{\alpha i} \left(1 - \frac{1}{p_i}\right)$$

Teorema

Si

$$n = \prod_{i=1}^{2} p_i^{\alpha i}$$

Representa la forma normal del entero positivo n, entonces:

$$\phi(n) = n \prod_{i=1}^{k} \left(1 - \frac{1}{p_i}\right) \text{ ó}$$

$$\phi(n) = \prod_{i=1}^{k} \left(p_i^{\alpha i} - p_i^{\alpha i - 1}\right)$$

Ejemplo:

$$\begin{aligned}\phi\,(24) &= \phi\,(2^3 \cdot 3)\\ &= 24 \cdot \left(1 - \frac{1}{2}\right)\left(1 - \frac{1}{3}\right)\\ &= 8\end{aligned}$$

CAPITULO III

En este capítulo responderemos a las siguientes preguntas:

¿Qué es un CRIPTOSISTEMA? ¿Cómo se clasifican los CRIPTOSISTEMAS? ¿Cómo funciona el CRIPTOSISTEMA RSA?

3.1 Tipos de Cifrados

Antes de conocer los tipos de cifrados, debemos saber que es un CRIPTOSISTEMA.

Definición:

Un CRIPTOSISTEMA, es una tupla (M, C, K, E, D) tal que:

- M: conjunto de textos planos u originales.
- C: conjunto de posibles textos cifrados.
- K: conjunto de posibles claves.
- E: conjunto de transformaciones de cifrados.
- D: conjunto de transformaciones de descifrados.

Para todo clave $k \in K$, hay un función de cifrado $e_k \in E$ y una correspondiente función de descifrado $d_k \in D$, donde $e_k : M \longrightarrow C$, $d_k : C \longrightarrow M$ y $d_k(e_k(m)) = m$, cualquiera sea $m \in M$.

a) Cifrados Simétricos

Se refiere al conjunto de métodos que permiten tener una comunicación segura entre emisor y receptor, siempre y cuando con anticipación se hayan intercambiado la clave que es llamada clave simétrica.

Es denominado cifrado simétrico, porque utiliza la misma clave para cifrar y descifrar un mensaje. Se conoce también como cifrado de clave privada.

Se ha caracterizado por ser la más usada durante toda la historia, siendo implementada en diversos dispositivos como manuales, mecánicos, eléctricos y algoritmos computacionales. La idea principal es aplicar diferentes funciones al mensaje que se quiere cifrar de modo que solo se conozca una clave que se aplique de forma inversa para poder descifrar.

Transposición y sustitución

Los cifrados simétricos se pueden dividir de acuerdo al tipo de operación que se realiza al mensaje, esta operación puede ser transposición o sustitución que se obtienen de las características que posee el alfabeto.

La transposición, consiste en desordenar el texto original, es decir se realiza una alteración en el orden de las letras del mensaje original a través de una clave. En cambio la sustitución, reemplaza cada letra del texto original por otra utilizando una clave, generalmente se hace uso de la aritmética modular

Algunos ejemplos de cifrados simétricos son:

- Cifrado tipo Cesar:
  Si $M = C = K = \mathbb{Z}/n\mathbb{Z}$ con n entero, entonces:

$$e_k(m) \equiv m + k \ (mod\ n)$$
$$d_k(c) \equiv c - k \ (mod\ n)$$

- Cifrado tipo Afín:
  Si $M = C = \mathbb{Z}/n\mathbb{Z}$ y $K = \{(k_1, k_2) \in \mathbb{Z}/n\mathbb{Z} : mcd\ (k_1, n) = 1\}$. Si $K = (k_1, k_2) \in K$, entonces:

$$e_k(m) \equiv k_1 m + k_2 \ (mod\ n)$$
$$d_k(c) \equiv k_1^{-1}(c - k_2)(mod\ n)$$

Ejemplo: Cifrado tipo Afín

Cifremos la palabra **código** con la clave $k = \{4, 5\}$
En primer lugar se realiza una equivalencia entre las letras y los números, a través de la siguiente tabla:

a	b	c	d	e	f	g	h	i	j	k	l	m	n
1	2	3	4	5	6	7	8	9	10	11	12	13	14

ñ	o	p	q	r	s	t	u	v	w	x	y	z
15	16	17	18	19	20	21	22	23	24	25	26	27

Así **código** se transforma en $c = 3;\ o = 16;\ d = 4;\ i = 9;\ g = 7;\ o = 16$

Utilizando la clave $k = \{4, 5\}$ ciframos el mensaje **código**

$$e_k(3) \equiv 4 \cdot 3 + 5\ (mod\ 27) \equiv 17\ (mod\ 27)$$
$$e_k(16) \equiv 4 \cdot 16 + 5\ (mod\ 27) \equiv 15\ (mod\ 27)$$
$$e_k(4) \equiv 4 \cdot 4 + 5\ (mod\ 27) \equiv 21\ (mod\ 27)$$
$$e_k(9) \equiv 4 \cdot 9 + 5\ (mod\ 27) \equiv 14\ (mod\ 27)$$
$$e_k(7) \equiv 4 \cdot 7 + 5\ (mod\ 27) \equiv 6\ (mod\ 27)$$
$$e_k(16) \equiv 4 \cdot 16 + 5\ (mod\ 27) \equiv 15\ (mod\ 27)$$

De esta forma la palabra **código** se transforma en el siguiente mensaje cifrado **PÑTNFÑ.**

Tomemos el mensaje cifrado **PÑTNFÑ** y utilicemos la equivalencia entre los números y letras obtenemos:

$$p = 17;\ \text{ñ} = 15;\ t = 21;\ n = 14;\ f = 6;\ \text{ñ} = 15$$

Luego descifremos:

$$d_k(17) \equiv 4^{-1}(17 - 5)(mod\ 27) \equiv 3\ (mod\ 27)$$
$$d_k(15) \equiv 4^{-1}(15 - 5)(mod\ 27) \equiv 16\ (mod\ 27)$$
$$d_k(21) \equiv 4^{-1}(21 - 5)(mod\ 27) \equiv 4\ (mod\ 27)$$
$$d_k(14) \equiv 4^{-1}(14 - 5)(mod\ 27) \equiv 9\ (mod\ 27)$$
$$d_k(6) \equiv 4^{-1}(6 - 5)(mod\ 27) \equiv 7\ (mod\ 27)$$
$$d_k(15) \equiv 4^{-1}(15 - 5)(mod\ 27) \equiv 16\ (mod\ 27)$$

Tenemos la siguiente congruencia de los números

$$c = 3;\ o = 16;\ d = 4;\ i = 9;\ g = 7;\ o = 16$$

Por tanto el mensaje original es **CODIGO.**

Observación:

Notemos que con el cifrado tipo cesar o afín, la persona que cifra el mensaje automáticamente puede descifrarlo con el simple hecho de aplicar la inversa de la función que utilizo para cifrar.

b) Cifrados Asimétricos

Este cifrado se caracteriza por utilizar dos claves diferentes para el emisor y receptor, entonces para cifrar mensajes se necesita una clave pública y para descifrar mensajes una clave privada. Nace con la finalidad de buscar métodos más prácticos para intercambiar claves simétricas.

Aproximadamente en 1975, dos ingenieros de la Universidad de Stanford, Whitfield Diffie y Martin Hellman, publican un artículo llamado *"New Directions in Cryptography*" (Nuevas direcciones en Criptografía) que introdujo el concepto de criptografía de clave pública. Los algoritmos de cifrado con clave privada o mejor dicho los cifrados simétricos hasta el momento eran los únicos conocidos, pero ya no poseían las necesidades de seguridad para cifrado un mensaje.

Ahora presentamos el cambio de clave de Diffie – Hellman porque marco el inicio del cifrado asimétrico:

Intercambio de clave de Diffie – Hellman:

a) Se seleccionan dos usuarios, $A\ y\ B$, un grupo finito cíclico[9], grupo G, de orden n y generador $\alpha\ \in\ G$.
b) A genera un número a, se calcula $\alpha^a\ \in G$ y se transmite a B.
c) B genera un número b, se calcula $\alpha^b\ \in G$ y se transmite a A.
d) A recibe α^b y se calcula $(\alpha^b)^a\ \in G$
e) B recibe α^a y se calcula $(\alpha^a)^b\ \in G$

Los dos usuarios $A\ y\ B$ tienen un elemento en común y por propiedades de potencias se tiene:

$$(\alpha^b)^a\ =(\alpha^a)^b\ =\ \alpha^{ab}$$

Ejemplo:

Elijamos dos usuarios Alejandra (A) y Bernardita (B) que han sido escogidos públicamente en un grupo $G=\ \mathbb{Z}_{53}^*$ y el generador $\alpha=2$. Luego A genera un número $a=23$, calcula:

$$\alpha^a=2^{23}(mod\ 53)\ \equiv\ 33$$

Este valor lo transmitimos a B, por su parte elige un numero $b=10$ y calcula:

[9] Los grupos que pueden ser generados por un único elemento se llaman Grupos Cíclicos.

$$\alpha^b = 2^{10}(mod\ 53)\ \equiv\ 17$$

Luego envía el valor obtenido a A, ahora conoce $a = 23$ y $\alpha^b = (2)^{10}(mod\ 53)\ \equiv\ 17$

Calcula:

$$(\alpha^b)^a =\ (2^{10})^{23}\ \ (mod\ 53) \equiv 43$$

De igual forma B, conoce $b = 10$ y $\alpha^a = (2)^{23}(mod\ 53)\ \equiv\ 33$, obtiene:

$$(\alpha^a)^b =\ (2^{23})^{10}\ \ (mod\ 53) \equiv 43$$

Queda mostrado que los usuarios $A\ y\ B$ comparten el mismo número secreto 43.

Observación:

No podemos olvidar que el método de Diffie – Hellman no es considerado un CRIPTOSISTEMA, ya que sólo permite el intercambio de información y no lleva a cabo el cifrar y descifrar un mensaje.

Ahora ya conocidos dos tipos de cifrados (simétrico y asimétrico), se logra apreciar la siguiente tabla resumen:

Tipo de Cifrado	**Simétrico**	**Asimétrico**
Seguridad	Clave	Clave privada
Algoritmo de cifrar	Igual al de descifrar	Se cifra con clave privada
Numero de claves	1	2
Tipos de Claves.	Secreta	Pública y Privada
Relación emisor receptor	Uno a uno	Uno a muchos mas
Falla de la seguridad.	Quien revele la clave.	Quien posee la clave privada.

3.2 CRIPTOSISTEMA RSA

Antes de entrar de lleno en el CRIPTOSISMETA RSA, debemos conocer la siguiente proposición que hace alusión a una generalización del Teorema de Fermat:

Proposición:

Sean p *y* q *primos distintos y* $g = mcd\ (p-1,\ q-1)$*. Entonces*

$$a^{\frac{(p-1)(q-1)}{g}} \equiv 1\ (mod\ pq)$$

Para todo a *satisfaciendo* $mcd\ (a, pq) = 1$.

Demostración:

En primer lugar veamos que:

$$(i)\ \ a^{\frac{(p-1)(q-1)}{g}} \equiv 1\ (mod\ p)$$

Por el Teorema de Fermat sabemos que $a^{\,(p-1)} \equiv 1\ (mod\ p)$ y además $\frac{q-1}{g}$ es un entero.

Así:

$$(a^{p-1})^{\frac{(q-1)}{g}} \equiv 1^{\frac{(q-1)}{g}}\ (mod\ p)$$
$$\equiv 1\ (mod\ p)$$

De la misma manera:

$$(ii)\ a^{\frac{(p-1)(q-1)}{g}} \equiv 1\ (mod\ q)$$

Luego de $(i)\ y\ \ (ii)$ tenemos por la definición del Mínimo Común Múltiplo:

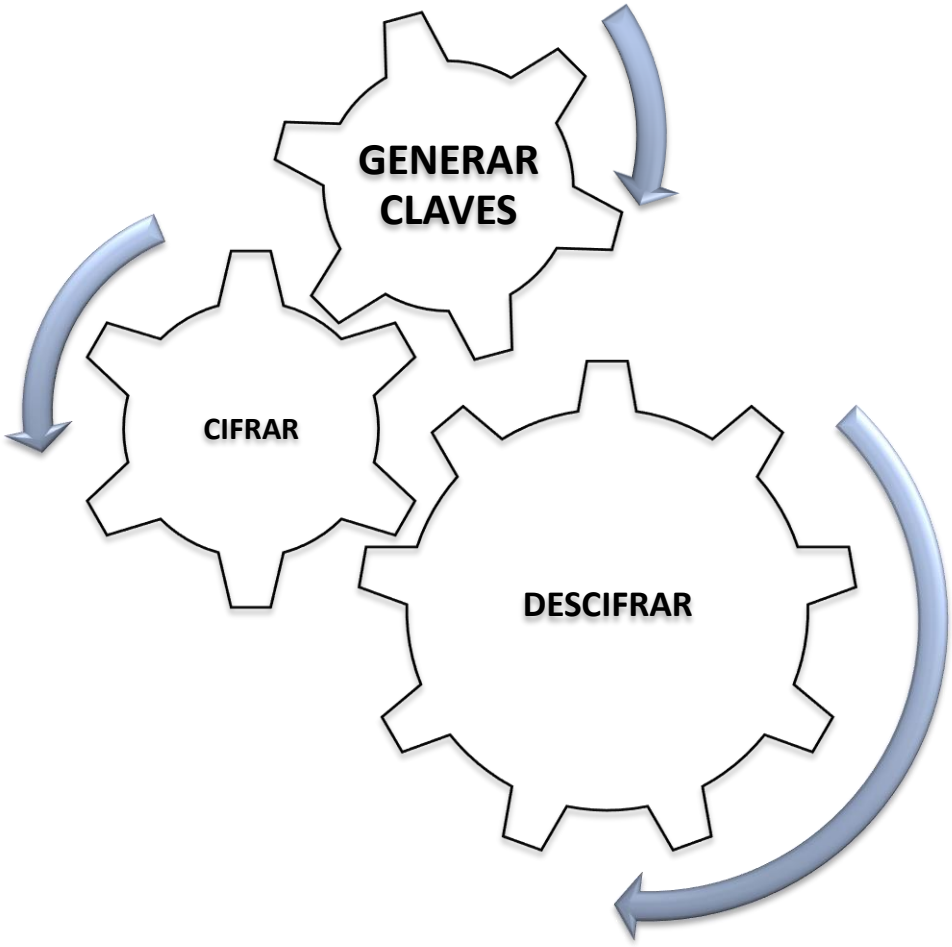
$$a^{\frac{(p-1)(q-1)}{g}} \equiv 1\ (mod\ mcm(p,q))$$

Como $mcm(p,q) = pq$, obtenemos lo deseado.

En 1976 W. Diffie y M. Hellman presentaron una descripción teórica de un método de cifrado en el cual una parte seria pública, y en 1977 R. Rivest, A. Shamir y L. Adleman encontraron un esquema práctico para implementarlo. Se conoce como el CRIPTOSISTEMA DE CLAVE PUBLICA RSA. Las etapas involucradas son las siguientes:

- Generar claves para el mensaje.
- Cifrado el mensaje.
- Descifrado el mensaje.

Cabe mencionar que cada una de las etapas antes nombradas están enlazas entre sí, es decir cada una depende de la anterior.



Antes de generar las claves para cifrar un mensaje se debe convertir en una secuencia de números, para ello a cada letra se le asigna un numero de dos dígitos. Utilizando la siguiente tabla:

A	B	C	D	E	F	G	H	I	J	K	L	M	N
11	12	13	14	15	16	17	18	19	20	21	22	23	24

Ñ	O	P	Q	R	S	T	U	V	W	X	Y	Z
25	26	27	28	29	30	31	32	33	34	35	37	37

Y el espacio entre cada palabra se le asigna el número 99. Por ejemplo si consideramos la frase **"CIFRADO ASIMETRICO"**, queda de la siguiente forma:

C	I	F	R	A	D	O		A	S	I	M	E	T	R	I	C	O
13	**19**	**16**	**29**	**11**	**14**	**26**	**99**	**11**	**30**	**19**	**23**	**15**	**31**	**29**	**19**	**13**	**26**

Entonces obtenemos lo siguiente:

1319162911142699113019231531291913 26,

hay que tener en cuenta si el mensaje es bastante a largo tendremos una secuencia de números muy grande.

A continuación describimos las tres etapas anteriores mencionadas:

Generación de claves:

- ✓ Se eligen dos números primos grandes que denominaremos $p\ y\ q$. Ahora se calcula el producto de estos números primos $n = p \cdot q$.
- ✓ Por la propiedad de la función de Euler tenemos

$$\varphi(n) = \varphi\ (p \cdot q) = (p-1)(q-1)$$

- ✓ Luego elegimos un $e \in \mathbb{N}$ tal que $1 < e < \varphi(n)$. Debe cumplir con la condición de ser primo relativo con $\varphi(n)$.
- ✓ Obtenemos $d \in \mathbb{N}$ y $1 < d < \varphi(n)$, que es $de \equiv 1\ mod\ (\varphi(n))$. Es decir es el inverso multiplicativo.
- ✓ Finalmente el emisor hace públicos $n\ y\ e$ pero mantiene en secreto $p, q\ y\ \varphi(n)$. Así, cualquiera que desee enviar un mensaje cifrado usara solo valores públicos $n\ y\ e$.

Cifrado:

- ✓ Se convierte el mensaje en una secuencia de dígitos como en el ejemplo del “cifrado asimétrico”.
- ✓ Utilizando el $mod\, n$ separa la secuencia de dígitos en grupos de números menores a n, de esta forma el mensaje se convierte en una lista de números $a_1, a_2, a_3, \dots a_r$. La única condición es que ningún bloque comience con cero, para evitar ambigüedad al momento de descifrar.
- ✓ Calculamos cada potencia en modulo n, usando el exponente e:

$$b_1 \equiv a_1^e \ (mod\ n)$$

$$b_2 \equiv a_2^e (mod\ n)$$

$$\vdots \qquad\qquad \vdots$$

$$b_r \equiv a_r^e (mod\ n)$$

- ✓ Finalmente obtenemos el mensaje cifrado.

Descifrado:

- ✓ Para descifrar el mensaje, recordemos a $\varphi(n)$ para resolver la ecuación diofántina[10]

$$ed - \varphi(n)v = 1$$

La solución de la ecuación, está dada por el siguiente

Teorema:

Si la ecuación diofántica $ax + by = c$ *tiene solución si y solo si*

$$d/c \ \ donde\ d = mcd\ (a, b)$$

- ✓ Para dar solución a la ecuación debemos acudir al algoritmo de Euclides con el fin de obtener los valores correspondientes a $d\ y\ v$. Y realizamos sustitución regresiva para escribir el mcd en combinación lineal de ambos números.
- ✓ Calculamos:

$$x_1 \equiv b_1^d\ (mod\ n\ )$$

$$x_2 \equiv b_2^d\ (mod\ n\ )$$

$$\vdots \qquad\qquad \vdots$$

$$x_r \equiv b_r^d (mod\ n)$$

- ✓ Conseguimos el mensaje original.

Ejemplo:

Consideremos el siguiente mensaje **PÚBLICA**:

En primer lugar elegimos dos números primos $p\ y\ q$. La única condición es que estos números primos deben tener la misma cantidad de dígitos.

Sea $p = 13$; $q = 19$

Obtenemos el módulo

$$n = p \cdot q$$
$$n = 13 \cdot 19$$
$$n = 247$$

A través de la propiedad de la función φ de Euler, tenemos

$$\varphi(n) = (p-1)(q-1)$$
$$\varphi(n) = (13-1)(19-1)$$
$$\varphi(n) = (12)(18)$$
$$\varphi(n) = 216$$

Ahora seleccionamos un exponente e que debe ser primo y a la vez cumplir con: $mcd\left(e, \varphi(n)\right) = 1$

Si $e = 7$, entonces $mcd\ (7, 216) = 1$

$$\therefore son\ primos\ relativos.$$

Ya teniendo los valores de $p, q, n, \varphi(n)\ y\ e$. Luego realizamos correspondencia entre las letras y números de la siguiente tabla:

A	**B**	**C**	**D**	**E**	**F**	**G**	**H**	**I**	**J**	**K**	**L**	**M**	**N**
11	**12**	**13**	**14**	**15**	**16**	**17**	**18**	**19**	**20**	**21**	**22**	**23**	**24**

Ñ	**O**	**P**	**Q**	**R**	**S**	**T**	**U**	**V**	**W**	**X**	**Y**	**Z**
25	**26**	**27**	**28**	**29**	**30**	**31**	**32**	**33**	**34**	**35**	**37**	**37**

De esta forma el mensaje **PUBLICA**, se transforma en una secuencia de números

P	U	B	L	I	C	A
27	**32**	**12**	**22**	**19**	**13**	**11**

Más explícitamente, tenemos:

$$\boldsymbol{PUBLICA = 27321222191311}$$

Separamos la secuencia de números en bloques menores a

$n\ (a_i < n,\ i \in \mathbb{R})$, esto quiere decir que los bloques no deben superar el valor de $n = 247$

Entonces:

$$a_1 = 27$$
$$a_2 = 32$$
$$a_3 = 122$$
$$a_4 = 219$$
$$a_5 = 13$$
$$a_6 = 11$$

Llegamos a la fase de cifrado el mensaje, para ello recordemos

$$b \equiv\ a^e\ (mod\ n)$$

Así,

$b_1 = a_1^e = (27)^7 \equiv 27\ (mod\ 247)$

$b_2 = a_2^e = (32)^7 \equiv 124\ (mod\ 247)$

$b_3 = a_3^e = (122)^7 \equiv 8\ (mod\ 247)$

$b_4 = a_4^e = (219)^7 \equiv 15\ (mod\ 247)$

$b_5 = a_5^e = (13)^7 \equiv 143\ (mod\ 247)$

$b_6 = a_6^e = (11)^7 \equiv 106\ (mod\ 247)$

Los bloques se convierten en los números $27, 124, 8, 15, 143, 106$ respectivamente.

Observación

Recordemos que para cifrado un mensaje sólo utilizamos los datos públicos $m\ y\ e$.

Para descifrar, debemos conocer $\varphi(n)$ para resolver la siguiente ecuación diofántica:

$$ed - \varphi(n)v = 1$$
$$7d - 216v = 1$$

A través del algoritmo de Euclides y de la sustitución regresiva, obtenemos los valores de $d\ y\ v$ respectivamente.

$$(7, 216) = 1$$
$$216 = 7 \cdot 30 + 6$$
$$7 = 6 \cdot 1 + 1$$
$$6 = 6 \cdot 1 + 0$$

Luego

$$1 = 7 + (-1) \cdot 6$$
$$1 = 7 + (-1)[\,216 + (-7) \cdot 30]$$
$$1 = 7 + (-1) \cdot 216 + 7 \cdot 30$$
$$1 = 7 \cdot 31 + (-1) \cdot 216$$

Los valores de $d = 31\ y\ \ v = -1$.

Algoritmo para descifrar:

$$x \equiv\ b^d (mod\ n)$$

Calculamos:

$$x_1 =\ \ b_1^d =\ (27)^{31} \equiv\ 27\ (mod\ 247\ )$$

$$x_2 =\ \ b_2^d =\ (124)^{31} \equiv\ 32\ (mod\ 247\ )$$

$$x_3 =\ \ b_3^d =\ (8)^{31} \equiv\ 122\ (mod\ 247\ )$$

$$x_4 =\ \ b_4^d =\ (15)^{31} \equiv\ 219\ (mod\ 247\ )$$

$$x_5 =\ \ b_5^d =\ (143)^{31} \equiv\ 13\ (mod\ 247\ )$$

$$x_6 =\ \ b_6^d =\ (106)^{31} \equiv\ 11\ (mod\ 247\ )$$

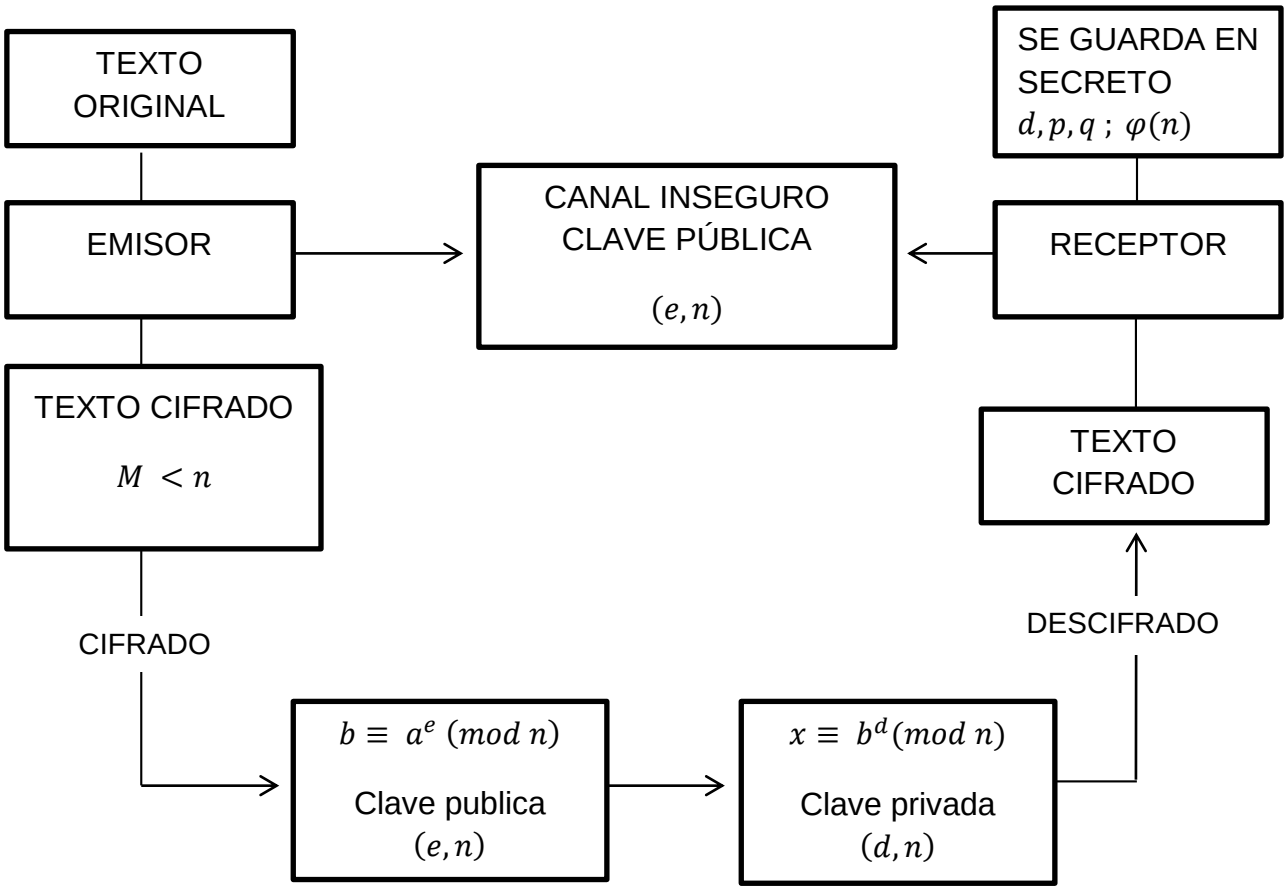
De esta forma el mensaje descifrado es la siguiente secuencia de bloques:

$$27, 32, 122, 219, 13; 11$$

Finalmente utilizando la tabla de congruencia entre las letras y los números, logramos el mensaje original.

$$\mathbf{27321222191311} = \boldsymbol{PUBLICA}$$

En los siguientes esquemas veremos un resumen del funcionamiento de RSA[11]



[11] Ruth Margarita Landa Hernández. (Septiembre, 2014). Herramientas matemáticas para implementar sistemas de encriptación. octubre 05, 2016, de cdigital Sitio web: http://cdigital.uv.mx/bitstream/123456789/38749/1/LandaHdz.pdf

3.3 Test de Primalidad

El test de primalidad consiste en determinar, si un número es primo o un primo probable. La necesidad de este test surge, porque el CRITPOSISTEMA RSA necesita dos primos $p\ y\ q$ grandes para poder ser utilizado. Por este motivo se requiere de los test de primalidad o de pseudoprimalidad, la diferencia radica en que el primero indica si un número es primo o compuesto. En cambio el segundo permite conocer la probabilidad de que un número sea primo.

Para ello consideremos un número n, entonces puede que sea primo o en caso contrario, es un número compuesto.

Proposición: (Pequeño Teorema de Fermat)

Sea p un número primo. Entonces:

$$a^{p-1} \equiv 1\ (mod\ p);\ \forall\ a \in\ \mathbb{Z}$$

Observación

En caso que no se cumple lo anterior, es decir:

$$a^{p-1} \not\equiv a\ (mod\ p);\ \forall\ a \in\ \mathbb{Z}$$

Sabemos que el número será compuesto.

Ejemplo:

i. Sea $a = 2,\ p = 271$

$$2^{270} \equiv 1\ (mod\ 271)$$

ii. Sea $a = 2,\ p = 100$

$$2^{99} \equiv 88\ (mod\ 100)$$

De los ejemplos podemos corroborar que el ejemplo i. se cumple el pequeño Teorema de Fermat, en cambio del ii. no se cumple.

Pero existen números que si cumplen la congruencia anterior, sin ser números primos. Estos números son denominados Números de Carmichael.

Definición

Un número de Carmichael es un entero compuesto tal que:

$a^{n-1} \equiv 1\ (mod\ n);\ \forall\ a\ \in\ \mathbb{Z}$ que satisface $mcd\ (a,n) = 1$

Ejemplo:

$$a^{1728} \equiv\ 1\ (mod\ 1729)$$

$$\forall\ a\ \in\ \mathbb{Z}\ , tal\ que\ \ mcd\ (a, 1729) = 1$$

El anterior número de Carmichael, tiene la siguiente descomposición.

$$1729 = 7\ \cdot 13\ \cdot 19$$

A continuación confirmemos si el número 1105, es Número de Carmichael para ello nos basamos en el Pequeño Teorema de Fermat:

Se desea probar que:

$$a^{1104} \equiv 1 \ (mod\ 1105), \forall\ a\ \in\ \mathbb{Z}$$

Tenemos

i. $a^{1104} = a^{4\cdot 276} \equiv 1 \ (mod\ 5), \forall\ a\ \in\ \mathbb{Z}\ tal\ que\ mcd\ (a, 5) = 1$

ii. $a^{1104} = a^{12\cdot 92} \equiv 1 \ (mod\ 13), \forall\ a\ \in\ \mathbb{Z}\ tal\ que\ mcd\ (a, 13) = 1$

iii. $a^{1104} = a^{16\cdot 69} \equiv 1 \ (mod\ 17), \forall\ a\ \in\ \mathbb{Z}\ tal\ que\ mcd\ (a, 17) = 1$

Luego de i. ii. y iii. obtenemos

$$a^{1104} \equiv 1 \ (mod\ 5\ \cdot 13\ \cdot 17)$$

$\therefore\ a^{1104} \equiv a \ (mod\ 1105), \forall\ a\ \in\ \mathbb{Z}$ quedando demostrado.

De esta forma mostramos que el Número de Carmichael 1105 es compuesto, puesto que su descomposición en números primos es la siguiente $1105 = 5\ \cdot 13\ \cdot 17$

3.3.1 Test de Miller – Rabin

El test de Miller – Rabin se basa en la siguiente proposición:

Proposición

Sea p un número primo y escribimos $p-1=2^t \cdot m$ con m número impar, sea a cualquier número no divisible por p. Entonces se cumple una de las siguientes condiciones:

1. a^q es congruente a 1 $(mod\ p)$
2. $a^q, a^{2q}, a^{4q}, a^{8q}, \dots, a^{2^{t-1}q}, a^{2^t q}$ es congruente a -1 $(mod\ p)$

Demostración:

Ver página 126 en 5].

¿Cómo funciona el Test Miller – Rabin?

Sea $p-1=2^t \cdot m\ ;\ donde\ m \in \mathbb{N}\ impar\ y\ t \in \mathbb{N}$. No podemos olvidar que el valor p es la entrada en el algoritmo del Test.

Este Test consta de los siguientes pasos:

1) Elegimos en forma aleatoria un número entero a, solo debe cumplir con $2 \leq a \leq n-2$

2) Luego, se calcula:

$$x_o \equiv a^m \ (mod\ n)$$

i. Si $x_o \equiv \pm 1\ (mod\ n)$, se termina el algoritmo con

"$n\ es\ probablemente\ primo$"

ii. Si $x_o \not\equiv \pm 1\ (mod\ n)\ y\ t = 1$, se termina el algoritmo con

"$n\ es\ probablemente\ compuesto$"

En otro caso, hacemos $j = 1$ y vamos al paso 3)

3) Ahora calculamos

$$x_j \equiv a^{2^j m}\ (mod\ n)$$

i. Si $x_j \equiv 1\ (mod\ n)$, el algoritmo termina con

"$n\ es\ definitivamente\ compuesto$"

ii. Si $x_j \equiv -1\ (mod\ n)$, termina el algoritmo con

"$n\ es\ probablemente\ primo$"

En caso que no ocurra ninguno de los casos anteriores (i. y ii.):

Tenemos

$$j = j + 1$$

Y avanzamos al paso 4)

4) Si obtenemos $j = t - 1$, nos dirigimos al paso 5) y en caso contrario volvemos al paso 3)

5) Calculemos:

$$x_{t-1} = a^{2^{t-1} m} \ (mod \ n)$$

i. Si $x_{t-1} \not\equiv -1 \ (mod \ n)$, el algoritmo termina con:

"$n \ es \ definitivamente \ compuesto$"

ii. Si $x_{t-1} \equiv -1 \ (mod \ n)$, termina el algoritmo con:

"$n \ es \ probablemente \ primo$".

Ejemplo

Consideremos $n = 1105$. Si $n - 1 = 2^4 \cdot 69$

Luego $t = 4 \ y \ m = 69$. Seleccionamos $a = 2$

Ahora aplicamos el algoritmo del Test:

$$x_o \equiv 2^{69} \equiv 967 \ (mod \ 1105)$$

Sea

- ✓ $j = 1$

$$x_1 \equiv 2^{2 \cdot 69} \equiv 259 \ (mod \ 1105)$$

✓ $j = 2$

$$x_2 \equiv 2^{4 \cdot 69} \equiv 781 \ (mod\ 1105)$$

✓ $j = 3$

$$x_3 \equiv 2^{8 \cdot 69} \equiv 1 \ (mod\ 1105)$$

Finalmente, tenemos por el paso 3) del test que

$$n\ es\ definitivamente\ compuesto.$$

Ya sabemos que el test de Miller – Rubin entrega la probabilidad que tiene un número n de ser primo, pero el reciente descubrimiento de un algoritmo determinista basado en una clase polinomial en la Universidad de Kanpur, tres académicos Agrawal, Kayal y Saxena; entrega la información de si el número n es primo o compuesto, denominado TEST DE PRIMALIDAD AKS.

CONCLUSIÓN.

Antes que todo debemos tener en cuenta que la CRIPTOLOGIA se ocupa de las técnicas, ya sean aplicas al arte como se observa en la Historia de la Criptografía o en la ciencia, CRIPTOSISTEMA RSA donde el objetivo es alterar mensajes mediante técnicas de cifrado para hacer ininteligibles a intrusos que desean descifrar el mensaje.

De esta forma el único objetivo de la criptografía es conseguir seguridad a los mensajes cifrados, por esto se diseñan CRIPTOSISTEMAS que permiten la confidencialidad del mensaje.

Considerando lo anterior, se muestra la diferencia entre los tipos de cifrados que existen (Simétrico y Asimétrica) en cada uno de ellos se presentan ejemplos explicativos con la finalidad de detectar la diferencia entre ellos. Así nos enfocamos en el CRIPTOSISTEMA RSA donde mostramos su estructura y funcionamiento a través de un ejemplo para facilitar la comprensión, no podemos olvidar que la complejidad de este CRIPTOSISTEMA se basa en la factorización de enteros (números primos bastante grandes).

Además se desglosaron y analizaron las herramientas matemáticas necesarias para conocer e implementar el RSA, el aspecto más importante que se debe mencionar es el inverso multiplicativo modular que es utilizado para obtener la clave privada en este CRIPTOSISTEMA.

Finalmente los test de primalidad son de vital importancia para los CRIPTOSISTEMAS por que entregan tanto la probabilidad de ser un número primo como determinar si es primo o compuesto, lo que se logra observar en el Test de Primalidad de Miller – Rubin y el Test de AKS.

BIBLIOGRAFIA

1. Amparo Fúster Sabater, Luis Hernández Encinas, Agustín Martin Muñoz, Fausto Montoya Vitini, Jaime Muñoz Masqué, Criptografía, protección de datos y aplicaciones, Ra – Ma, 2012.

2. Antoni Escrig Vidal. Alan Turing y el nacimiento de la Inteligencia Artificial, Antena de Telecomunicación, 2007. http://servicios.coitt.es/res/revistas/Antena167_08b_Articulo_Alan.pdf

3. D. R. Stinson, Cryptography: Theory and Practice,CRC Press, 1995.

4. Felipe Zaldivar, Introducción a la teoría de números. Fondo de Cultura Económica 2012.

5. Hoffstein, J. Pipher, J.H. Silverman, An introduction to mathematical cryptography. Springer, New York, 2008.

6. Ivo Basso Basso, Fernando Toledo Montiel, Apuntes de Aritmética, Universidad del Bio - Bio, 2015.

7. Katia Regina León Lomparte. Encriptacion RSA de archivos de texto, Académica comunidad digital del conocimiento, 2014.

8. Lucena López, Manuel José. Criptografía y Seguridad en Computadores. Dpto. de Informática Universidad de Jaén. Edición virtual.

9. Raúl Díaz, Luis Hernández Encinas, Jaime Muñoz Mosqué, El criptosistema RSA, Ra – Ma, 2005.

10. Ruth Margarita Landa Hernández. Herramientas matemáticas para implementar sistemas de encriptación, Cdigital 2014.

LINKOGRAFIA

1. http://www.hezkuntza.ejgv.euskadi.eus/r43-573/es/contenidos/informacion/dia6_sigma/es_sigma/adjuntos/sigma_24/9_Criptografia_clasica.pdf

2. http://macareo.pucp.edu.pe/mgonzal/publicaciones_archivos/RSA-con-Mathematica.pdf

3. http://theimitationgamemovie.com/#./About

4. http://cine3.com/2015/01/20/resena-the-imitation-game/