CAPÍTULO 1
CRIPTOGRAFÍA

1.1 CRIPTOGRAFÍA

Para dar un significado a lo que es la criptografía, debemos saber ¿Por qué y para qué fue creada?

Desde que el ser humano ha tenido la necesidad de comunicarse con una o más personas han buscado la forma de realizar dicha trasmisión de ideas, pensamientos, entre otros, dando origen a lo que hoy se le conoce como modelo de comunicación.

Pero para que exista un modelo de comunicación básico es necesario que el emisor (origen) proporcione un mensaje o texto, a trasmitir por un medio a un receptor (destinatario).como se muestra en la figura 1.1.

Figura 1.1. Modelo de comunicación básico

La comunicación ha sido necesaria desde sus orígenes por diversas razones, como son los fines bélicos. En donde no sólo se requería transmitir información, sino que además era necesario que esta información no fuese conocida por personas ajenas a ella.

Por lo que surgió la tarea de buscar métodos o técnicas para ocultar la información dando origen a lo que hoy se le conoce como criptografía. Proveniente del griego *Kryptós, criptos "ocultar"y graphe, grafos "escribir", lo que da origen a* escritura oculta.

Los primeros registros del uso de la criptografía datan del siglo V a.C. A partir de la escritura de la obra Mathematical Theory of Communication, escrito por C.E Shannon era considerado como **un arte** de escribir algún mensaje mediante el uso de claves secretas o un modo misterioso. A principios de la segunda guerra mundial se implementa la utilización de algoritmos matemáticos, de máquinas, programas, entre otros para el ocultamiento del mensaje, algunos de ellos usados aún en nuestros días considerando a la criptografía como **ciencia**.

Es decir la ciencia que se encarga de diseñar funciones o dispositivos capaces de generar el ocultamiento de información.

Por anteriores acontecimientos es por ello que se divide en:
Asesorar

- Criptografía Clásica.
- Criptografía moderna.

Como se puede visualizar en la figura 1.2

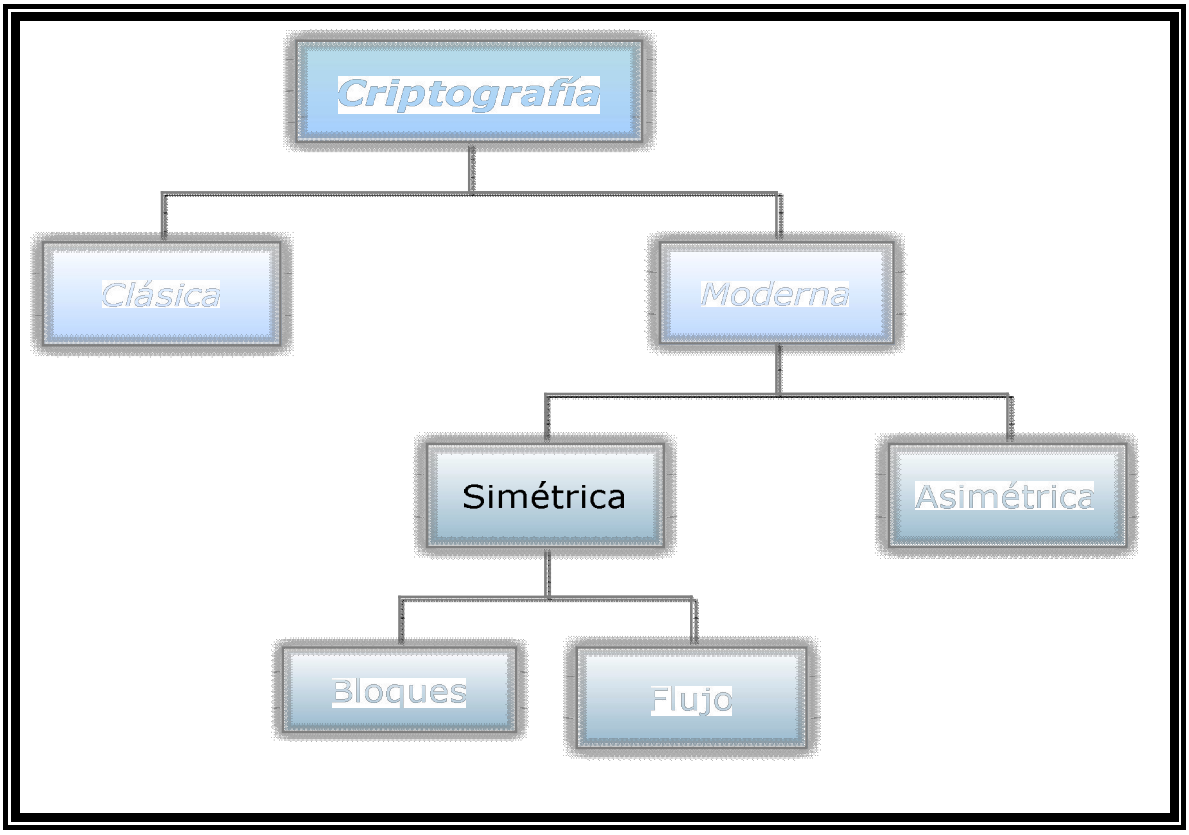

Figura 1.2. Clasificación de criptografía

1.2 CRIPTOGRAFÍA CLÁSICA

En la criptografía clásica se ocupaban diversos métodos para ocultar mensajes, que sólo podían leer o llegar a personas de mucho prestigio como reyes, jefes y monarcas. En muchos de los casos fue utilizada para la comunicación en las guerras. Es por ello que se le considero como el arte de ocultar el mensaje.

Existen diversos métodos utilizados con respecto al año o época dependiendo de los recursos disponibles (tecnológicos, humanos, etc.), para poder entender la criptografía clásica, se mencionaran algunos ejemplos sobresalientes utilizados a lo largo de la historia.

1.2.1 EVOLUCIÓN DE LOS MÉTODOS

En el siglo V a.C. durante la guerra entre Atenas y Esparta, los espartanos utilizaron la Scítala. Este método consistía en una vara o bastón, el cual era envuelto en un trozo de tela donde era escrito un texto alterado en el orden de las palabras, el cual servía para ocultar el significado del mensaje.

Para poder leerlo se necesitaba un bastón del mismo grosor y largo como se observa en la figura 1.3.

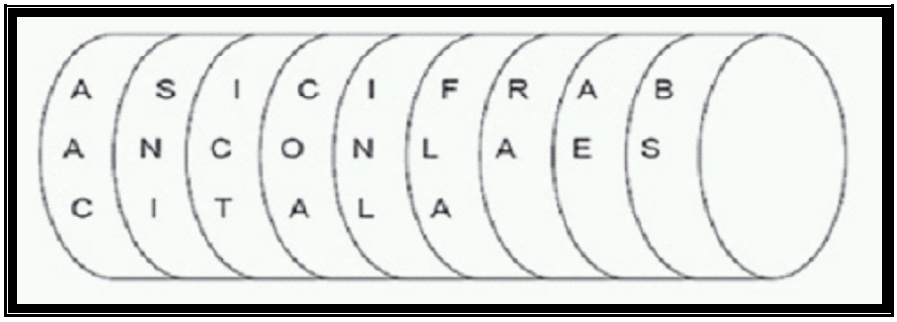

Figura 1.3. Scítala

En el sigo II a.C. Polybio, historiador griego miembro de la clase gobernante, invento un cuadro de 5x5 que permitía intercambiar símbolos, mediante el remplazo de coordenadas de dos ejes ocasionando el aumento del texto. Posteriormente se realizaron modificaciones en los símbolos, mediante la sustitución de dos letras o números, dicha sustitución se realizaba una por una, es decir dependiendo de las coordenadas de la ubicación del símbolo. Como se muestra en la figura 1.4

	A	B	C	D	E
A	A	B	C	D	E
B	F	G	H	IJ	K
C	L	M	N/Ñ	O	P
D	Q	R	S	T	Y
E	A	B	C	D	E

	1	2	3	4	5
1	A	B	C	D	E
2	F	G	H	IJ	K
3	L	M	N/Ñ	O	P
4	Q	R	S	T	Y
5	A	B	C	D	E

Figura 1.4. Cuadro de Polibybios

En el año 1466 Alberti escribe la obra “De Compendis Cifirs” dando origen al polialfabético, es decir el uso de varios alfabetos, mediante dos discos divididos en casillas designadas a cada carácter utilizado. Dicho método consiste en el movimiento de los discos, el cual consiste en una serie de saltos entre casillas, dependiendo del número asignado a cada salto era sustituido el carácter, Como se muestra en la figura 1.5.

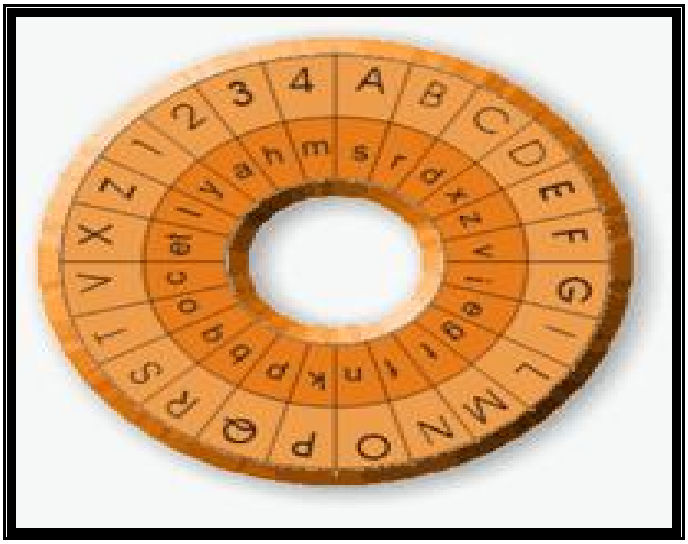

Figura 1.5. Disco de Alberti

A partir del Disco de Alberti surgen otros métodos que emplean el uso del mismo mecanismo base, uno de ellos es la rueda de Jefferson (1743). Esta máquina se conformaba por una serie de discos con letras impresas, que giraban libremente alrededor de un mismo eje, como se observa en la figura 1.6.

Figura 1.6 Rueda de Jefferson

En la primera y segunda guerra mundial (siglo XX) la criptografía juega un papel importante al hacer necesaria la utilización y desarrollo de técnicas como las máquinas de cifrado, empleadas en los sistemas de comunicación para la trasmisión de mensajes secretos.

En la primera guerra mundial se emplean los avances tecnológicos como estrategias de comunicación y armamento. Ejemplo: el espionaje de Margaret Geetruida Zelle, conocida como Mata Hari, quien empezó como espía de los alemanes para obtener información mediante la técnica de ingeniería social y posteriormente trabajando como agente doble proporcionando información a los franceses.

En 1919 se registra la primera patente de máquina de cifrado mecánica y electromecánica llamada *Enigma* creada por el holandés Alexander Koch y el alemán Arthur *Scherbius, de la cual se* obtienen diferentes versiones. Su objetivo principal era facilitar la comunicación a través de la transmisión de

documentos entre comerciantes y hombres de negocios de una manera privada.

Dicha máquina se componía de una serie de rotores que contenían el alfabeto, su funcionamiento se basaba en sustituir cada letra, al ir girando cada rotor se podía generar un gran número de alfabetos diferentes dando un total de 614,656 combinaciones. Haciendo de enigma una pieza importante para esa época, debido a que era casi imposible la obtención del mensaje sin la utilización de la misma.

Los métodos anteriormente descritos mostraban diversas vulnerabilidades. Un ejemplo de ello se presenta en la sustitución de alfabetos, al aplicar un análisis de secuencia dentro de la sustitución de caracteres, lo cual permite descifrar el mensaje oculto.

Debido lo anterior, se sustituyen los métodos manuales dando pie al uso de máquinas y la utilización de procedimientos matemáticos poniendo fin a la criptografía clásica, iniciando así una nueva era en la criptografía. Como se observa en la figura 1.7.

Figura 1.7. Enigma

1.3 CRIPTOGRAFÍA MODERNA

En 1948 Bell System Technical Journal publica el artículo llamado ***Una teoría matemática de la comunicación*** escrita por Clude Shannon y las aportaciones de Warren Weaver, se demuestra que toda fuente de información se puede medir y que los canales de comunicación tienen una unidad de medida similar, apoyado en la teoría de muestreo de Nysquit (la cual indica que se produce una pérdida de información llamada distorsión, error o ruido de cuantificación y que existe un límite para su transmisión), es decir que toda información se trasmite sobre un canal si la magnitud de la fuente no excede con la capacidad de trasmisión del canal que la conduce, sentando las bases para corrección de errores, suspensión de ruido y redundancia.

En 1949 se publicó la Teoría de las comunicaciones secretas escrito por Shannon, en donde la criptografía se apoya de otras ciencias como la estadística, la teoría de la información, la física, las matemáticas, etc.

Con los dos anteriores escritos surge la teoría de la información, que emplea el siguiente modelo de comunicación de una forma desarrollada, mostrado en la siguiente imagen 1.8.

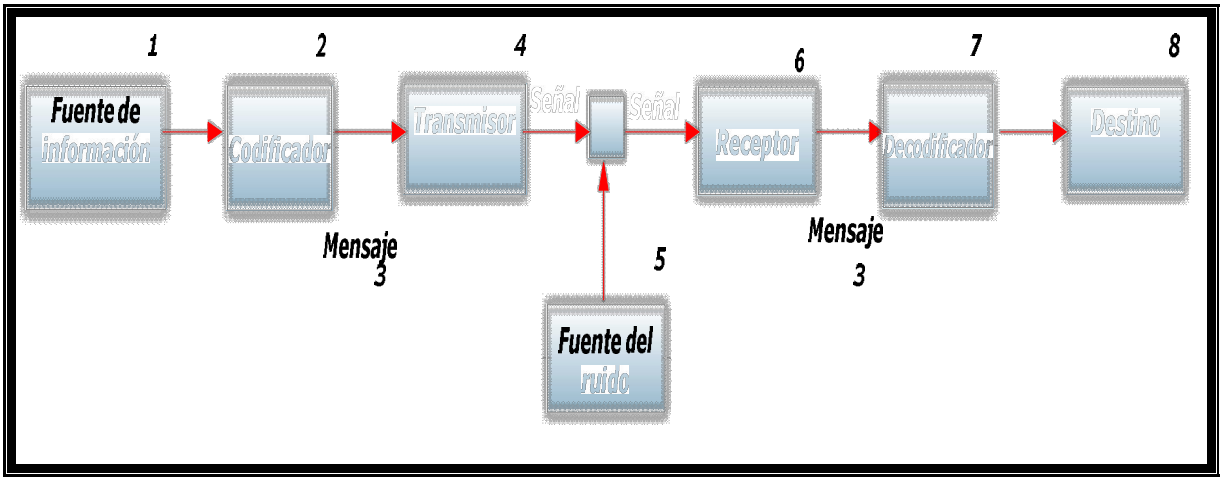

Figura 1.8. Modelo de comunicación de Shannon.

La figura anterior muestra cómo se lleva a cabo el proceso de la comunicación en donde la fuente de información genera el mensaje a trasmitir, posteriormente se aplica una codificación, es decir se trasforma el mensaje, para poder ser mandado como señal sobre un canal, en el transcurso el mensaje o señal se puede ver afectada por el ruido, el cual provocara pérdida o alteración para poder llegar al receptor. Una vez que se reciba la señal por el receptor y sea decodificado, es decir a su forma original, se manda el destino que es el punto final del proceso de comunicación.

Lo importante en este modelo es que la señal se descodifique en el transmisor de forma adecuada para que el mensaje codificado por el emisor sea el mismo que es recibido por el destino.

Con el apoyo de los dos artículos anteriores la criptografía deja de ser considerada como un arte y empieza a ser considerada como una ciencia, por lo que la criptología, se divide en criptografía que son los métodos y algoritmos que se han estado estudiando en los cuales se profundizara más adelante, y el criptoanálisis que estudia los métodos para obtener los mecanismos de cifrado para la obtención del mensaje.

Como se puede observar la criptografía toma un papel importante en la actualidad para el intercambio de información, mediante el medio de comunicación. Un ejemplo de lo anterior es la internet medio más utilizado en la actualidad, que debe proporcionar seguridad para que el medio de comunicación no tenga los siguientes problemas:

- Intercepción de los datos por un ente externo que busca obtener la información antes de que llegue a su destino y después dejar que siga su curso sin alterarla provocando el problema de **confidencialidad**.
- Falsificación: se produce cuando un ente externo obtiene el mensaje, se adueña de él y de la identidad del emisor, generando un nuevo mensaje

que manda al receptor provocando un problema de **integridad y confidencialidad**.

La criptografía moderna se dividida en dos grandes vertientes: criptografía simétrica y asimétrica.

Cabe mencionar que para fines de esta investigación se profundizara en la criptografía asimétrica.

1.4. CRIPTOGRAFÍA SIMÉTRICA O DE CLAVE SECRETA

Los algoritmos simétricos son aquellos que utilizan ***una sola clave*** de cifrado y de descifrado, por lo que se tiene que proteger su difusión, ya que es sólo para el emisor/receptor autorizado.

Ejemplo

El usuario verónica antes de mandar la información utiliza un algoritmo con una llave para poder trasformar la información y así poder mandarla por la Internet, esta es recibida por el usuario minerva que utiliza la misma clave con la que se encripto para poder obtener la información, como se muestra en la siguiente imagen 1.9.

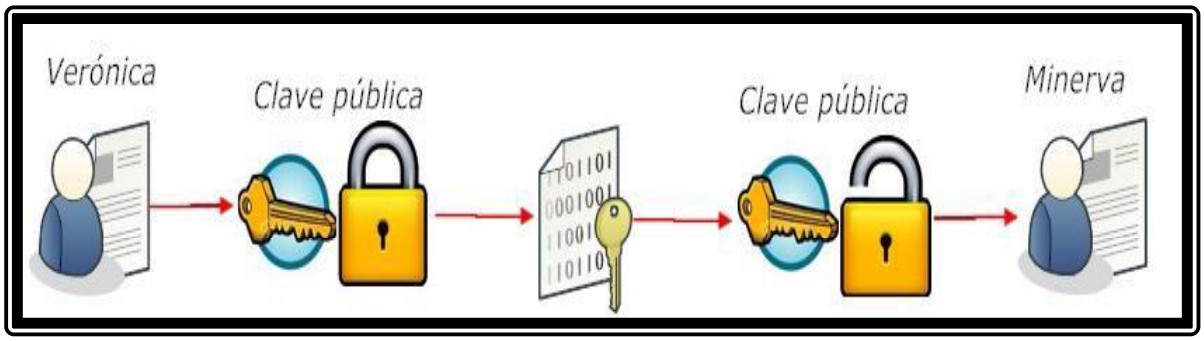

Figura 1.9 Criptografía simétrica

Es por ello que se le conoce como secreto compartido, existen dos tipos de algoritmos para poder encriptar y desencriptar por bloques y flujo.

1.4.1 ALGORITMO SIMÉTRICO EN BLOQUE

Es cuando el algoritmo divide el mensaje a cifrar en bloques de tamaño constante y cifra uno a uno los bloque con su clave del mismo tamaño, dependiendo del algoritmo utilizado, de tal forma que se va cifrando bloque por bloque como se puede observar ene la figura 1.10.

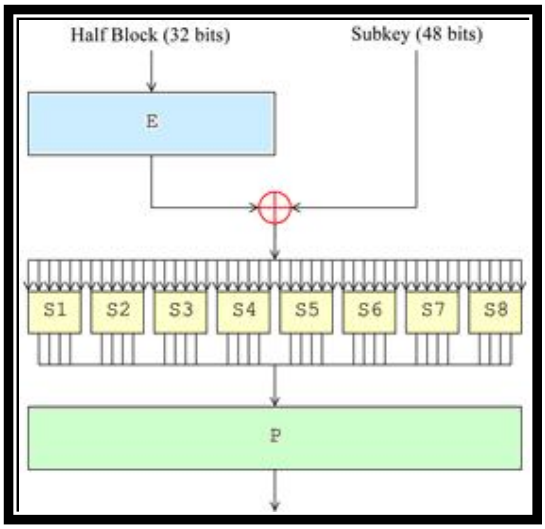

Figura 1.10. Esquema de Función de Feiste

Este algoritmo depende de los siguientes elementos:

- Transformación lineal: dependen de una o dos funciones que pueden o no depender de la clave.
- Transformación intermedia: son las iteraciones o las N veces de repeticiones para la trasformación aplicando la función y el uso de la clave.
- Transformación final: garantiza que las operaciones de cifrado y descifrado sean asimétrica es decir la operación inversa de la inicial.
- Algoritmo de expansión de clave: es la conversión de la clave del usuario en subclaves.

A continuación nombrare algunos algoritmos que fueron creados bajo un esquema simétrico en bloques

El algoritmo **Data Encryption Standard (DES)** creado en los 70’ por IBM, utiliza el esquema feister (los bloques de datos se dividen en dos partes iguales y en cada iteración trabaja de manera alternada cada una de las partes), es decir en bloques de 64 bits, su clave inicial es de 64 bits y después se genera por cada iteración una de 56 bits, en total trabaja con 16 iteraciones, implementando una permutación inicial y una final.

El Algoritmo Internacional de Cifrado de Datos **(IDEA)** fue creado por Xuejia Lai y James L. Massey y publicado en 1991, es un sistema de cifrado de bloque creado como remplazo del algoritmo DES ya que mediante fuerza bruta pudieron descifrarlo, originalmente se llamaba IPES. Se implementa mediante la utilización de claves de 128 bits las cuales se dividen en 8 bloques de 16 bits cada una, las primeras 6 claves son utilizadas en la primera ronda del cifrado y las otras dos en la segunda iteración y operación de bloques de 64 bits (Datos) y 8 ciclos.

En 1993 fue creado el **algorimo Blowfish** por Bruce Schneier, que cifra datos en bloques de 64 bits divididos en un mismo tamaño, su clave puede ser variable y puede ser hasta de 448 bits (en cada ciclo ocupa diferente subclave), es decir genera 18 iteraciones para poder obtener el mensaje encriptado.

El algoritmo **RC5** se dio a conocer en 1995 por Rivers Clipher que son las iniciales que tiene como nombre, el 5 representa la secuencia de algoritmos de cifrado simétrico, a este tipo de algoritmo se le puede especificar el tamaño de la palabra 16, 32 o 64 bits, es decir, si es diferente el tamaño de la palabra se puede producir diferentes bloques para cifrar en bloques de 32, 64 o 128 bits. El número de iteraciones a realizar van desde 1 hasta 255 dependiendo del tamaño del bloque (palabra y clave).

El National Institute of Standards and Tecnology (NIST) en 1999 da a conocer el algoritmo **3DES o TDES**, donde se modifica el problema de la utilización de clave por una más corta y consiste en aplicar 3 veces el algoritmo DES dos de cifrado y uno de descifrado utilizando 2 o 3 claves diferentes para generar las subclave.

1.4.2 ALGORITMO SIMÉTRICO EN FLUJO

Se requiere de un generador de llaves o fuente, la clave tiene que ser tan grande como el mensaje a cifrar, el inconveniente con este algoritmo es que será difícil recordar para el usuario. Donde mencionas la figura 1.11.

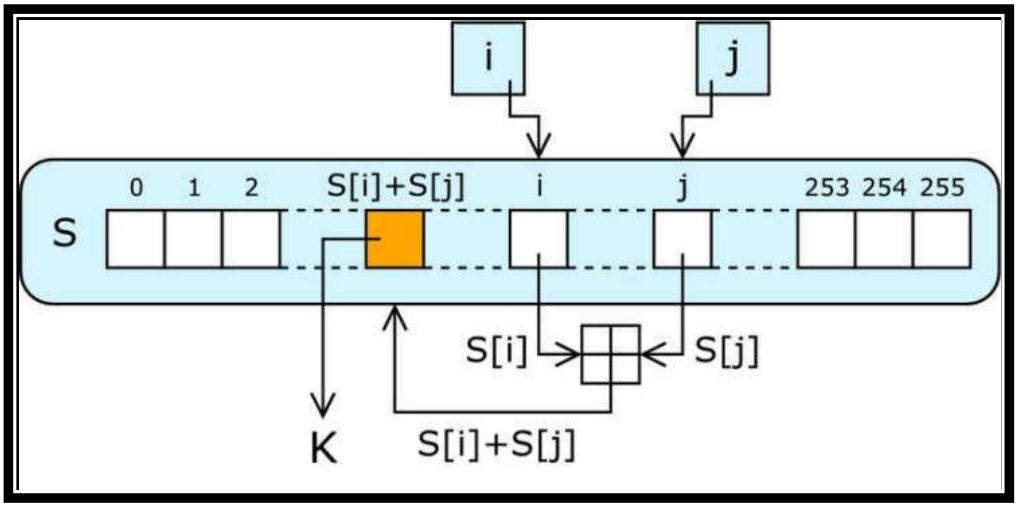

Figura 1.11. Esquema de generador de llave

Dentro de la criptografía simétrica en bloque podemos encontrar el siguiente algoritmo:

En 2001 tras un concurso por la National Institute of Standards and Tecnology (NIST) se da a conocer el nuevo Algorimo Advanced Encryption Standard (AES) que soporta un mensaje mínimo de 128 bits, las claves pueden ser de diferentes longitudes, así como las iteraciones pueden ser de 10 a 14.

1.5 CRIPTOGRAFÍA ASIMÉTRICA O DE CLAVE PÚBLICA

En 1976 la publicación de New Directions in Cryptography desarrollado por Whitfiel Diffie y Martin Hellman (Diffice-Herma), demuestra la distribución de la claves de cifrado para poder ser utilizado en los diferentes sistemas resolviendo el problema de distribución de claves.

Es un algoritmo en donde dos entidades se ponen de acuerdo en un número, a través de un medio de transmisión público, de tal forma que no pueda ser conocido por alguna otra persona, es decir que se permite el intercambio de claves a través de canales inseguros, mediante el uso de un par de claves relacionadas matemáticamente entre sí para cifrar y descifrar, se basa en funciones de un solo sentido, estas claves se generan como privada y pública, no necesitando un canal seguro para el intercambio, el cual permitirá su visibilidad de la clave por un tiempo sin poner en riesgo la información por lo cual se obtendrá como se observa en la figura 1.12.

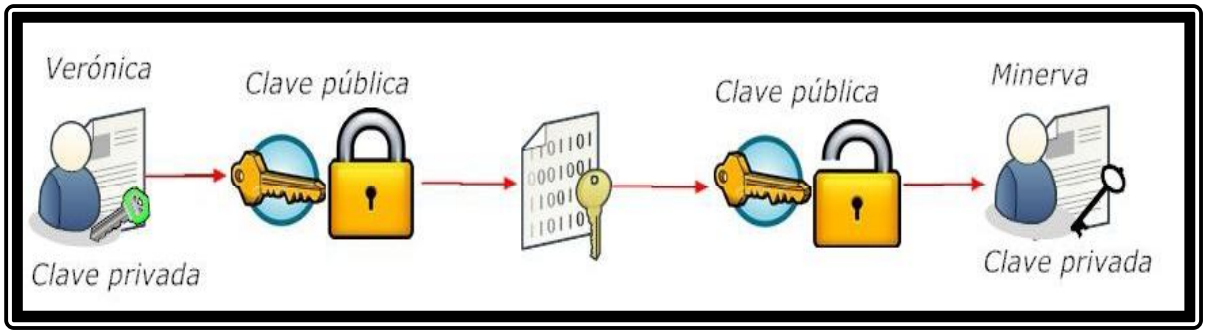

Figura 1.12 Criptografía asimétrica

Las siguientes formulas describen el procedimiento que se realiza en cualquiera de los algoritmos (f) y la utilización de un mensaje plano o claro (Mcla) así como de una clave (K) para poder obtener el criptograma y viceversa como se puede observar en la figura 1.13.

Cripto $=f(\text{Mcla}, K_{ca})$

$\text{Mcla}=g(\text{Cripto}, K_{da})$

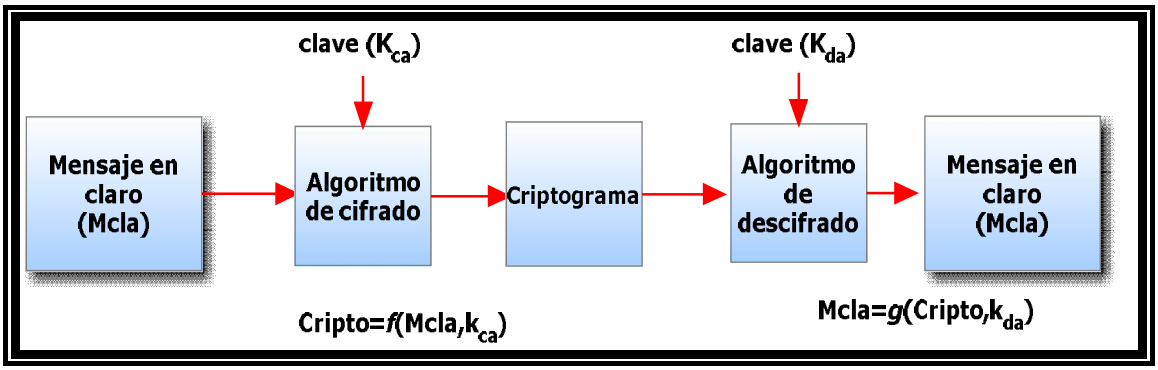

Figura 1.13 Procedimiento para generar un criptograma

Dentro de los algoritmos de criptografía asimétrica se tiene que:
En 1985 Taher Elgamal da a conocer su algoritmo **El gamal,** es un algoritmo basado en Diffie –Hellman, en un principio fue ideado para producir firmas digitales, aunque después se extendió su uso para utilizarlo en el cifrado de mensajes, es utilizado en GNU (Privacy Guard) versiones recientes de PGP, entre otros.

Para generar un par de llaves, se escoge un número primo p y dos números aleatorios α y *a* menores que *p*. Se calcula entonces la expresión:

$$y = \alpha^a \pmod p$$

Los valores p, α y β son públicos, y *a* es privado.

En 1997 se desarrollo el algoritmo **RSA** creado por Ron **R**ivest, Adi **S**hamiry Leonard **A**dleman considerado un esquema robusto, por la factorización de números muy grandes, porque para la obtención de clave pública es mediante la multiplicación de dos números primos ***p*** y ***q***, para poder calcular ***n*** que es la multiplicación de ***p*** y ***q,*** y este será de carácter público es por ello que la dificultad radica en la factorización de números grandes. Para después poder

obtener las claves para emplear este algoritmo como ejemplo se tiene la siguiente figura1.14.

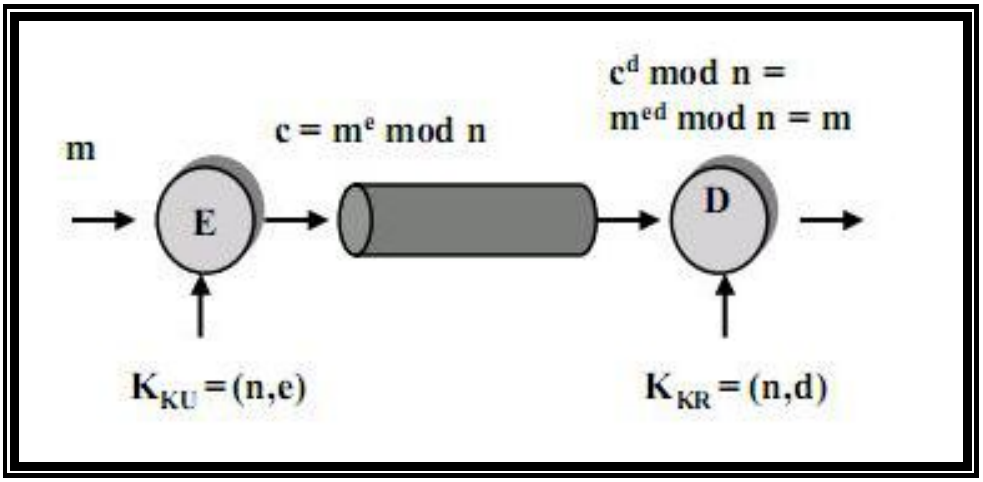

Figura 1.14. Esquema del algoritmo RSA

En 1997 **National Institute of Standards and Tecnology (NIST)** da a conocer el algoritmo de firmas digital **(Digital Signature Algorithm DSA)** y que fue para uso del estándar de firma digial o Digital Signature Standard **(DSS)** especificado en el FIPS 186, una firma digital (FD) permite identificar la autenticidad del mensaje, es decir que la información aceptada sea efectivamente enviada por quien dice ser el emisor, sin haber sufrido alguna modificación. Existen diferentes tipos de FD:

- Implícitas: que las contiene en el mismo mensaje.
- Explicitas: se añaden como una marca en el mensaje.
- Privadas ó verdadera: el remitente sólo puede verificar al usuario.
- Revocables: el remitente puede denegar su pertenencia.
- Irrevocables: el receptor prueba su origen.

Para obtener la firma es necesario tener un resumen de la información y es por ello que se utiliza las funciones hash, que son aquellas que toman como entrada una cadena de longitud variable para después con el uso de funciones

matemáticas comprimir el documento hasta generar una cadena o bloque de longitud fija llamada hash, así resolviendo el problema de integridad y autenticidad del mensaje

Existen diferentes funciones hash como son:

MD2 (128 bits)

MD4 (128 bits)

MD5(512 bits)

SHA-1 (160 bits)

SHA-256 (256 bits)

SHA-512 (512 bits)

Para realización del proyecto serán utilizados MD5 y SHA, cabe mencionar que la utilización de estas funciones en cuanto más grande sea su longitud en bites se tardara más tiempo en realizar la consulta y responder es por ello que es necesario revisar las características de servidores con los que se cuentan.

MD5 Message Digest Algorithm desarrollado en 1992 por Ron River mejorando la robustes de MD4, y se encuentra documentado en el RFC 1321, procesa mensajes de cualquier longitud, procesando uniformemente bloques de 512 bits, añadiendo bits si es necesario al final.

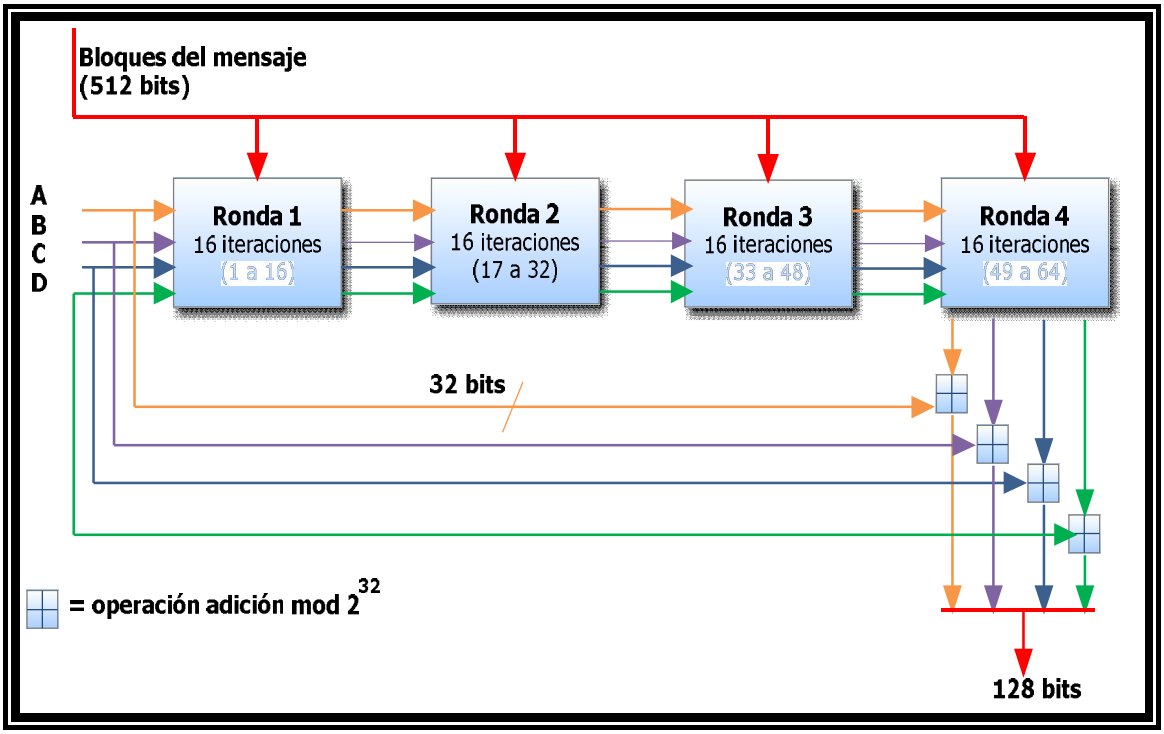

Figura 1.15. Función MD5

En la figura 1.15 se muestra como es el funcionamiento del algoritmo MD5, el cual está formado por 4 rondas cada una de 16 iteraciones en donde mediante sumas OR va generando el resumen, para después hacer una concatenación y obtener una longitud fija de 128 bits.

SHA Algoritmo Hash seguro desarrollado en 1993 y dado a conocer por FIPS 180, fue desarrollado para apoyar al estándar de firma digital DSS y se baso en el MD4, este algoritmo procesa mensajes de cualquier tamaño hasta 2^{64} bits operando en bloques de 512 bits a la vez, generando resúmenes de 160 bits.
SHA-l es la versión actualizada y especificada en el RFC 3174 consta de 5 pasos:

1. Proceso de relleno, es el agregar los bits que sean necesarios de manera que la longitud del mensaje sea long ≡ 448 mod 512 en dado caso que se requiera.

2. El mensaje original debe tener una longitud de 64 bits antes de aplicar el relleno.
3. Se inicia el registro de llamadas MD de 160 bits que permite almacenar y mantener los resultados. Este registro maneja secciones de 32 bits que son inicializadas con valores hexadecimales.
4. El mensaje se procesa a través de 16 bloques de 32 bits cada uno, por lo que se realiza 4 rondas de veinte pasos cada una dando un total de 80 iteraciones.
5. Se obtiene la concatenación que produce un bloque de 160 bits.

Como se puede observar ene la figura 1.16 el funcionamiento de SHA-l

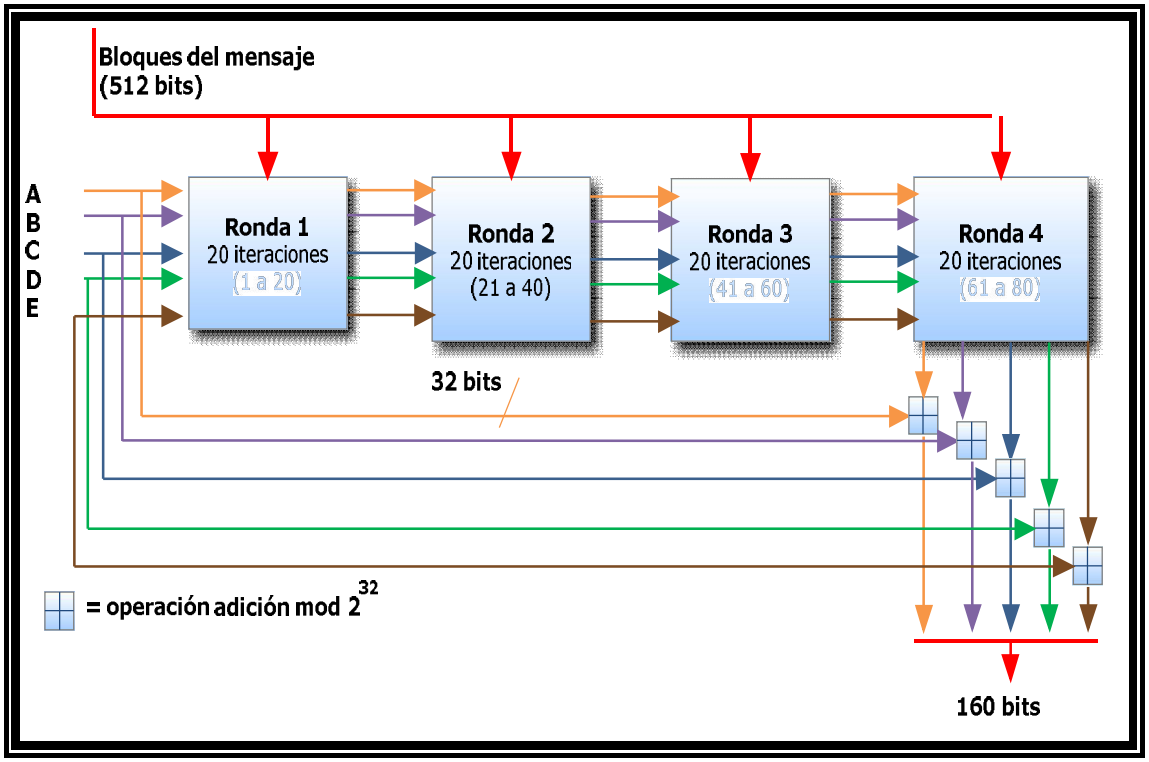

Figura 1.16. Función SHA-1

Como nota adicional se señala que el procedimiento para las otras variantes de las funciones SHA, siguen el mismo procedimiento.