UNIVERSIDAD VILLA RICA

ESTUDIOS INCORPORADOS A LA UNIVERSIDAD NACIONAL AUTÓNOMA DE MÉXICO

FACULTAD DE CIENCIAS DE LA COMUNICACIÓN

"CRIPTOGRAFÍA COMO PROCESO DE COMUNICACIÓN ENIGMÁTICA"

TESIS

QUE PARA OBTENER EL TÍTULO DE:

LICENCIADA EN CIENCIAS DE LA COMUNICACIÓN

PRESENTA:

SERENELA MATTIELLO GUERRERO

Director de Tesis
LIC. ALEJANDRO ARMANDO ANAYA HERNÁNDEZ

Revisora de Tesis
LIC. MARÍA GUADALUPE CRUZ NÚÑEZ

BOCA DEL RÍO, VER. **2007**

Agradecimientos:

Gracias a todos mis maestros, a mi directora de carrera, a mis asesores de tesis y a todas aquellas personas que participaron en mi formación académica, por todos los conocimientos y enseñanzas que compartieron conmigo.

Dedicatoria:

Este trabajo se lo dedico a mi familia por el apoyo incondicional que me brindaron durante toda mi vida académica. A mi papá, por ser el mejor ejemplo a seguir, por darme la oportunidad de superarme cada día y por creer en mí. A mi mamá, por cuidar de mis desvelos y por su comprensión y amor a lo largo de este camino. A mi hermana, por darme ánimo y motivación para seguir adelante. A mi hermano, por compartir su conocimiento conmigo y tener la paciencia de enseñarme cosas nuevas. Y a todos mis seres queridos que con su cariño y apoyo me han hecho tener confianza en mis ideas y la fuerza necesaria para cumplir esta y todas las metas que me proponga. Mil gracias.

ÍNDICE

INTRODUCCIÓN……..…..1

CAPÍTULO 1. ANTECEDENTES DE LA CRIPTOGRAFÍA

1.1. Definición…….....….....8

1.2. Conceptos afines…….....12

1.3. Modelo y elementos de un criptosistema……15

1.3.1. Elementos de un criptosistema…….…..15

1.4. Clasificación de los criptosistemas……...16

1.4.1. Criptografía simétrica……..……...17

1.4.2. Criptografía asimétrica……..……....19

1.4.3. Criptografía híbrida.……...20

1.5. Desarrollo histórico de la criptografía.……21

1.5.1. Criptografía antigua……..……...…….....21

1.5.2. Criptografía moderna…….……25

1.5.3. Criptografía contemporánea……28

CAPÍTULO 2. CRIPTOGRAFÍA COMO PROCESO DE COMUNICACIÓN

2.1. Modelo de comunicación……..…..…....31

2.1.1. Teoría de la información de Shannon y Weaver…..……....33

2.1.2 .Teoría de la comunicación de Wilbur Schramm…..…….....….37

2.1.3. Teoría de la comunicación de David K. Berlo……42

2.2. Fuente……..…..48

2.3. Codificador……..…..49

2.4. Emisor……..……...52

2.5. Mensaje……..…….53

2.6. Canal……...56

2.7. Contexto……..57

2.8. Ruido……...59

2.9. Receptor……..…61

2.10. Decodificador……63

2.11. Destinatario……..…64

2.12. Retroalimentación……..…65

CAPÍTULO 3. APLICACIONES DE LA CRIPTOGRAFÍA: UNA TÉCNICA PARA EL PRESENTE Y EL FUTURO

3.1. Principales funciones de la criptografía……..67

3.1.1. Autenticación……..…….68

3.1.2. Firma digital……..……...69

3.1.3. Identificación del usuario……..……...72

3.2. La utilidad de la criptografía en la vida diaria……74

3.2.1. Medicina y criptografía……..…75

3.2.2. Empresa y criptografía……..77

3.2.3. Correo electrónico y criptografía……..……78

CAPÍTULO 4. CONCLUSIONES……....81

FUENTES CONSULTADAS……...88

ANEXOS

Anexo 1. El código secreto de la Biblia……90

Anexo 2. El método César……..……96

Anexo 3. La máquina Enigma……..99

INTRODUCCIÓN

La criptografía ha sido de gran importancia para la sociedad, no sólo en los aspectos bélicos o de estrategia militar, sino también en asuntos de trascendencia religiosa, diplomática y financiera. En la actualidad, la criptografía no sólo se utiliza para comunicar información de forma segura ocultando su contenido a posibles intrusos. Una de las ramas de la criptografía que más ha revolucionado el panorama actual de las tecnologías de la información es el de la firma digital, tecnología que busca asociar al emisor de un mensaje con su contenido de forma que éste no pueda negar que ha sido la fuente del mismo posteriormente.

Por lo anterior, el tema es de suma importancia por su conocimiento y análisis, ya que el uso de la criptografía es ampliamente utilizada en el ámbito comercial, en la comunicación diplomática y en varias áreas de toma de decisiones que repercuten a nivel social, político y económico donde su aplicación es imprescindible, por lo que cada día se van revolucionando las técnicas criptográficas y la convierten en un área de la comunicación con un futuro prometedor.

El objetivo general de esta investigación fue elaborar un material comunicativo, que sirva como apoyo teórico para los interesados en el tema de la criptografía, en el que se explique qué es la criptografía, se cree un marco teórico

acerca de esta disciplina y sus inicios, y se le analice como proceso de comunicación, además de mencionar sus proyecciones a futuro.

Los objetivos específicos fueron: definir y explicar qué es la criptografía y el conjunto de técnicas y conceptos que se utilizan en esta disciplina. Describir el contexto y marco teórico de la criptografía y su desarrollo histórico. Analizar a la criptografía como proceso de comunicación, desde la perspectiva de Shannon y Weaver, Schramm, Berlo, Pino, Fúster y Escarpit, entre otros autores. Y reconocer las perspectivas para esta disciplina y las ramas en las que tiene y tendrá aplicación.

El estudio se realizó en un periodo de 11 meses que inició en el mes de febrero y finalizó en el mes de diciembre de 2006, llevándose a cabo en las ciudades de Veracruz y Boca del Río. Se consultaron como principales fuentes de datos las aportaciones relacionadas con las teorías de la comunicación, la criptografía, la historia y algunas obras cinematográficas. De esta forma, se elaboró un material comunicativo, basado en las contribuciones de reconocidos autores en el campo de las Ciencias de la Comunicación, como los que se mencionaron anteriormente, todos ellos creadores de modelos que en su momento explicaron los efectos de la comunicación colectiva, desde varios enfoques vinculados al fenómeno comunicativo, como son la ingeniería, la psicología y la sociología. Para esta investigación se consideraron como unidades de observación diversos documentos relacionados con los temas de la comunicación, la criptografía, la informática, la tecnología y la historia, acerca de la

utilización de las técnicas criptográficas y el impacto que ha tenido esta disciplina en algunos eventos de importancia histórica.

Este estudio trató de responder a la siguiente pregunta de investigación: **¿Qué importancia tiene la criptografía como proceso de comunicación?**; partiendo de la hipótesis de que la criptografía es un conjunto de técnicas para cifrar y descifrar información de manera que ésta sea estrictamente confidencial, dando como resultado una comunicación segura que en su conjunto conforman un proceso de comunicación. Para lograr lo anterior se recurrió a un tipo de estudio que por su finalidad dio como resultado una investigación de tipo pura o fundamental, ya que no se persiguieron fines prácticos, no se interfirió con alguna variable o situación durante su estudio, y sus resultados servirán para aumentar el cuerpo teórico de la ciencia que se estudia. Por su objetivo, esta investigación fue de tipo aclaratoria, ya que se analizó el objeto de estudio del cual ya se tenía conocimiento previo, desde una perspectiva comunicativa aclarando algunas características que lo integran como proceso. Por su procedimiento esta investigación fue de tipo cualitativo, ya que no se llevó a cabo la aplicación de algún método estadístico de confirmación o recolección de datos. Según los campos de la actividad humana esta investigación fue de tipo multidicipinaria, ya que se basó en las aportaciones de varias disciplinas científico – sociales, como lo son las ciencias de la comunicación, la criptología, la criptografía y la historia. Según los procesos de estudio y la extensión del campo del mismo esta investigación fue monográfica, ya que se realizó una recopilación de datos que presenta un análisis sistemático de la forma, funcionamiento, elementos e

interrelaciones que conforman el proceso comunicativo que se lleva a cabo mediante la criptografía, que fue en este caso el objeto de estudio. Según sus técnicas y los instrumentos de observación se realizó por medio de una observación indirecta, ya que se realizó principalmente por medio de una consulta bibliográfica y documental, que comprendió la recopilación de datos obtenidos a través de libros, revistas, periódicos y toda clase de documentos que fueron utilizados para recoger observaciones referentes al tema de investigación.

La importancia de esta investigación radica principalmente en que la criptografía es una disciplina que a lo largo de la historia ha representado un importante canal de comunicación cuya principal función ha sido garantizar que la transmisión de los mensajes se logre, llevando estos a sus destinos de una manera eficaz, pero sobre todas las cosas segura, evitando que estos mensajes y sus contenidos sean violados en el camino y dicha información caiga en manos de alguien más que el destinatario original. Además de que esta investigación reforzará el material teórico existente en relación a la criptografía y su análisis desde el punto de vista de la comunicación, ya que adaptará algunas teorías y modelos de comunicación al proceso comunicativo que se lleva a cabo con la criptografía. Los beneficios arrojados por esta investigación son de índole teórico, siendo los principales favorecidos los estudiantes de Ciencias de la Comunicación, de historia, interesados en el estudio de la criptografía y, en general, todo el público interesado en ésta como proceso de comunicación.

En cuanto a la estructura del trabajo, éste se encuentra dividido en 4 capítulos: el primero abarca los antecedentes de la criptografía, su definición y se presenta un análisis de conceptos afines a la criptografía que ayudarán al lector a comprender mejor el contenido del texto. También se presenta un modelo básico de criptosistema, se explican los elementos que lo integran y qué papel desempeñan en el proceso comunicativo criptográfico. Se hace una clasificación de los diferentes tipos de criptosistemas, partiendo de los métodos básicos como los utilizados en la criptografía simétrica, hasta llegar a los más avanzados como la criptografía asimétrica y la híbrida. Como último punto de este capítulo y con el propósito de crear un marco teórico, se hace una breve descripción de su desarrollo histórico, partiendo de la criptografía antigua, la moderna y con una breve descripción de la criptografía actual. El segundo capítulo habla de la criptografía como proceso comunicativo. En este se presenta una introducción sobre qué se debe entender cuando se habla de un proceso comunicativo, y posteriormente se explican la teoría de la información de Shanon y Weaver, la teoría de la comunicación de Wilbur Schramm y la teoría del proceso de comunicación de David K. Berlo, con sus respectivos modelos, los cuales han servido de pauta para el estudio del proceso de comunicación criptográfico. Además, en este capítulo se definen y explican los elementos básicos del proceso comunicativo como son: la fuente, el codificador, el emisor, el mensaje, el canal, el contexto, el ruido, el receptor, el decodificador, el destinatario y la retroalimentación. El tercer capítulo habla acerca de las aplicaciones que tiene la criptografía en el presente y sus proyecciones a futuro. En éste se explican las tres principales funciones de la criptografía en la actualidad y con visión a futuro

como lo son la autenticación, la firma digital y la identificación de usuario. Además de hacer una breve referencia de algunas ramas de la vida cotidiana en las que el uso de la criptografía se ha vuelto frecuente y cada vez más necesaria, como lo son las ciencias de la salud o medicina, el ámbito empresarial y el ambiente personal ejemplificado con el correo electrónico. En las conclusiones obtenidas durante el desarrollo de este trabajo de investigación, se realizó un recuento acerca de las indagaciones teóricas acerca del tema y un breve ejercicio reflexivo acerca de la importancia de la relación entre el estudio de los procesos de comunicación y la rama de la criptología.

En cuanto a las limitaciones del estudio las principales dificultades que se enfrentaron durante este trabajo de investigación, fue que en la mayoría de los casos, a la criptografía se le aborda como un sistema de información matemática, y las disciplinas que lo estudian a profundidad son las relacionadas con el campo de la informática, por lo que es muy poco lo que se le analiza como el inminente proceso comunicativo que es y las características de las partes que integran dicho proceso desde un enfoque puramente comunicativo. Otra dificultad que se presentó, durante este trabajo de investigación radicó en que existían muy pocas fuentes en idioma español que abarcaran al objeto de estudio desde el punto de vista de la comunicación. Así mismo, debido a que existe un gran desconocimiento de las técnicas criptográficas por parte de la comunidad académica del campo de la comunicación, fue necesario dar un contexto previo del tema para poder introducir al lector en lo que es el desarrollo del trabajo y este desconocimiento puede causar falta de credibilidad en cuanto a la relación que existe entre la

criptografía y las ciencias de la comunicación, lo que dificulta la tarea de explicarla como proceso de comunicación.

CAPÍTULO 1. ANTECEDENTES DE LA CRIPTOGRAFÍA

1.1. Definición

En general, se considera a la criptografía como una técnica o herramienta útil para la protección de la información. Surgió por la necesidad del hombre de asegurar que algunos de sus mensajes sólo fueran comprendidos por las personas a las que estaban destinados. Por ejemplo, desde tiempos inmemorables se necesitó esconder información de los enemigos en las batallas para ayudar a la transmisión de información vital para la realización de distintas estrategias militares. Además del campo militar, la criptografía también ha servido a lo largo de la historia para asegurar la confidencialidad de mensajes de índole religiosa e, inclusive, en la actualidad se utiliza para transmitir mensajes de importancia política y en transacciones económicas, así como para mensajes de otros aspectos de la vida social que requieren de almacenamiento y transmisión de información importante.

En un principio, la criptografía fue considerada un arte. Sin embargo, desde 1949, a raíz de la publicación de la *Teoría de las Comunicaciones Secretas* de Shannon, la criptografía ha sido reconocida como una ciencia aplicada. La criptografía se apoya en otras ciencias, como la estadística, la informática, la física o las matemáticas, para el desarrollo de nuevas teorías y herramientas como el análisis de frecuencias de signos y la criptografía cuántica.

La criptografía es el estudio del conjunto de técnicas para el cifrado de los mensajes. Ésta es, en realidad, una rama de la criptología, ciencia que abarca tanto a la criptografía como al criptoanálisis, el cual estudia los métodos que se utilizan para romper los textos cifrados y poder leer la información original de estos cuando no se tiene al alcance la clave de cifrado.

Algunas definiciones comunes de criptografía son:

> *"La criptografía es la técnica de escribir con claves secretas o de un modo enigmático." (Diccionario de la Real Academia Española*, 2006).
>
> *"Las raíces etimológicas de la palabra criptografía son 'kriptos', que significa oculto, y 'graphos', que se traduce como escribir, lo que da una clara idea de su definición clásica: arte de escribir mensajes en clave secreta o enigmáticamente"* (Fúster *et al*., 2001).
>
> *"La criptografía se ocupa del diseño del procedimiento para cifrar, es decir, para enmascarar una determinada información de carácter confidencial."* (Pino, 2003).
>
> *"La criptografía, el arte de enmascarar los mensajes con signos convencionales, que sólo cobran sentido a la luz de una clave secreta, nació con la escritura."* (Coto, en red, disponible en http://www.albertocoto.com/secciones/cripto.htm).

El objetivo principal de la criptografía es el de proporcionar comunicaciones seguras y secretas entre dos entidades (las cuales pueden ser personas, organizaciones, etc.) sobre canales o medios seguros o inseguros, certificando que los mensajes sólo puedan ser leídos por las personas a quienes van dirigidos, proporcionando un método sencillo de certificación del emisor y de la autenticidad e integridad de la información y confirmando que el mensaje no ha sido modificado durante su trayecto.

> *A y B son, respectivamente, el emisor y receptor de un determinado mensaje. A transforma el mensaje original (texto claro o texto fuente), mediante un determinado procedimiento de cifrado controlado por una clave, en un mensaje cifrado (criptograma) que se envía por un canal público. En recepción, B con conocimiento de la clave*

> *transforma ese criptograma en el texto fuente, recuperando así la información original.* (Pino, 2003:25).

La criptografía, como ya se ha dicho, persigue el fin de una comunicación secreta y segura. Sin embargo, para lograr esto no sólo basta con lograr esa transmisión. Se debe asegurar además que las entidades que están participando en este proceso de comunicación secreta sean realmente quienes dicen ser, ya que existe siempre el riesgo de que el mensaje al ser interceptado por un enemigo sea modificado, para beneficio del interceptor, llegando a su destino original con información incorrecta.

Se tomará como ejemplo un campo de batalla y en lo sucesivo se explicarán los elementos del proceso de comunicación: El general del ejército rojo manda un mensaje a otro general que se encuentra en el frente de batalla. Durante su trayecto, el mensaje es interceptado por un general del ejército azul, el enemigo, y es modificado, informando al general del ejército rojo que debe rendirse. Obviamente, esto significaría la victoria para el ejército azul. Cuando un enemigo logra interceptar y descifrar un mensaje encriptado, tiene el poder para manipular dicha información y sacar provecho de ella. Por ello, la finalidad de la criptografía es asegurar no sólo la confidencialidad del mensaje, sino la fidelidad de toda la información transmitida, incluyendo la fuente y el destino de esta.

> *La finalidad de la criptografía es múltiple: primeramente, mantener la confidencialidad del mensaje, es decir, que la información allí contenida permanezca secreta; a continuación, garantizar la autenticidad tanto del criptograma (integridad) como del par remitente/destinatario. En efecto, el criptograma recibido ha de ser realmente el enviado (evitando así manipulaciones o alteraciones en el proceso de transmisión), a la vez que el remitente y destinatario han de ser realmente quienes dicen ser, y no remitentes y/o destinatarios fraudulentos.* (Pino, 2003:25).

Como se mencionó, además de todas las dificultades en los procesos de cifrado y descifrado de los mensajes, la criptografía se enfrenta a un reto aún mayor: la necesidad de ocultar la información. Es este reto el que propició en un principio el surgimiento de las técnicas criptográficas. Efectivamente, si es necesario proteger la información transmitida se debe a que se supone la existencia de peligro de intercepción y de un enemigo que pretende obtenerla y beneficiarse de ésta. Debido a esto, la criptografía continúa evolucionando y mejorando sus técnicas de cifrado y descifrado, adaptándose a los requerimientos y preferencias de los usuarios. Esto ha dado lugar a diferentes métodos criptográficos (los cuales se analizarán más adelante) que varían en complejidad en una de las partes del proceso criptográfico o en ambas:

> *En el proceso de transmisión, el criptograma puede ser interceptado por un enemigo criptoanalista que lleva a cabo una labor de descriptazo; es decir intenta, a partir del criptograma y sin conocimiento de la clave, recuperar el mensaje original. Un buen sistema criptográfico será por tanto aquel que ofrezca un descifrado sencillo pero un descriptazo imposible o, en su defecto, muy difícil.* (Pino, 2003:27).

En caso de una intercepción, para conocer el mensaje se requiere el uso de la rama hermana de la criptografía, conocida como criptoanálisis. Ésta estudia las técnicas utilizadas para descifrar un mensaje cuando se carece de la clave para hacerlo, de tal forma que no sólo pone a prueba la habilidad del interceptor, sino la seguridad y efectividad del sistema criptográfico que se empleó para cifrar el mensaje original:

> *La criptografía corresponde sólo a una parte de la comunicación secreta. Si 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*. (Fúster *et al*., 2001:2).

El criptoanálisis y la criptografía forman una ciencia más completa, conocida como criptología, que abarca tanto los procesos de cifrado y descifrado de mensajes como las técnicas utilizadas para traspasar la seguridad de los mecanismos de cifrado. La criptología ha sido valiosa herramienta utilizada para tejer capítulos de la historia que sin ella serían desconocidos; como señala Fúster (2001:2): *"En toda comunicación secreta se presenta una lucha entre criptógrafos y criptoanalistas. El éxito de unos representa siempre el fracaso de los otros".* En esta batalla de la comunicación secreta, la criptografía debe poder garantizar casi por completo la seguridad de sus mensajes. Sólo entonces se podrá decir que ésta ha cumplido satisfactoriamente con su función y que ha sido una herramienta útil.

1.2. Conceptos afines

A continuación se presentan algunos conceptos comúnmente utilizados en el lenguaje criptográfico:

- **Algoritmo:** Un conjunto de reglas bien definidas para la solución de un problema en un número finito de pasos.
- **Cifra o algoritmo de cifrado:** Es la técnica utilizada para el cifrado del texto en claro o mensaje original y sirve para ocultarlo y hacerlo ilegible para todas las personas que no posean la clave para descifrarlo. De esta manera, se asegura que el texto llega sin ser violado por otra persona que no sea el destinatario del mensaje. Existen dos técnicas básicas de cifrado en la criptografía clásica: la técnica de la sustitución, que se basa en el cambio de significado de

los componentes básicos del mensaje, como las letras, números, etc., y la técnica de la transposición, que se basa en la reordenación de los elementos básicos que componen el mensaje, letras, números, etc.

- **Cifrado:** El proceso de cifrado es, básicamente, la función de la criptografía que consiste en convertir el texto en claro en uno que resulte ilegible a simple vista. También pueden utilizarse como sinónimos de cifrado los términos de **codificado** y **encriptado.**
- **Clave:** Información secreta que adapta el algoritmo de cifrado para cada uso distinto. Es aquélla que contiene las indicaciones para cifrar y descifrar el mensaje original. Es la llave para abrir el mensaje cifrado y poder leer el mensaje original.
- **Código secreto:** Es un método de criptografía clásica, el cual consiste en sustituir unidades textuales, más o menos largas o complejas para ocultar el mensaje.
- **Criptoanálisis:** Disciplina que estudia las técnicas utilizadas para romper o descifrar los textos cifrados en ausencia de la clave, su objetivo final es conocer el texto en claro o mensaje original que está oculto.
- **Criptoanalista:** Es el especialista encargado de aplicar todas las técnicas necesarias para descifrar un mensaje cifrado sin tener la clave. En ocasiones dicho mensaje se encuentra oculto por medio de la estenografía.

- **Criptograma o texto cifrado:** Es el texto o mensaje que queda como resultado de transformación del texto en claro a través del proceso de cifrado, manteniendo oculto el mensaje original.
- **Criptología:** Ciencia que abarca los procesos y técnicas de la criptografía y el criptoanálisis**.**
- **Criptosistema:** Es el conjunto de protocolos, algoritmos de cifrado, claves y actuaciones de los usuarios de los mismos para constituir un conjunto de normas con las que finalmente el usuario trabaja e interactúa.
- **Descifrado:** Es el proceso inverso al cifrado y sirve para recuperar el texto en claro o mensaje original teniendo el criptograma y la clave. También pueden utilizarse como sinónimos de descifrado los términos de **decodificado** o **desencriptado.**
- **Estenografía:** Es un método alterno a la criptografía que generalmente se utiliza simultáneamente con esta. Consiste en ocultar el propio mensaje ya cifrado dentro del canal de información. Por ejemplo, un mensaje que contiene un texto cifrado puede, a su vez, estar oculto en una superficie con una imagen, una pintura, etc., para que de esta forma pase inadvertido ante los ojos enemigos.
- **Protocolo criptográfico:** Especifica los detalles de utilización de los algoritmos y las claves para conseguir el efecto deseado.

- **Texto en claro:** Se conoce como texto en claro al mensaje que contiene la información original y que debe ser protegido por medio de la criptografía.

1.3. Modelo y elementos de un criptosistema

La criptografía moderna es el sistema o implementación de un algoritmo de cifrado mediante un criptosistema. Sus elementos son:

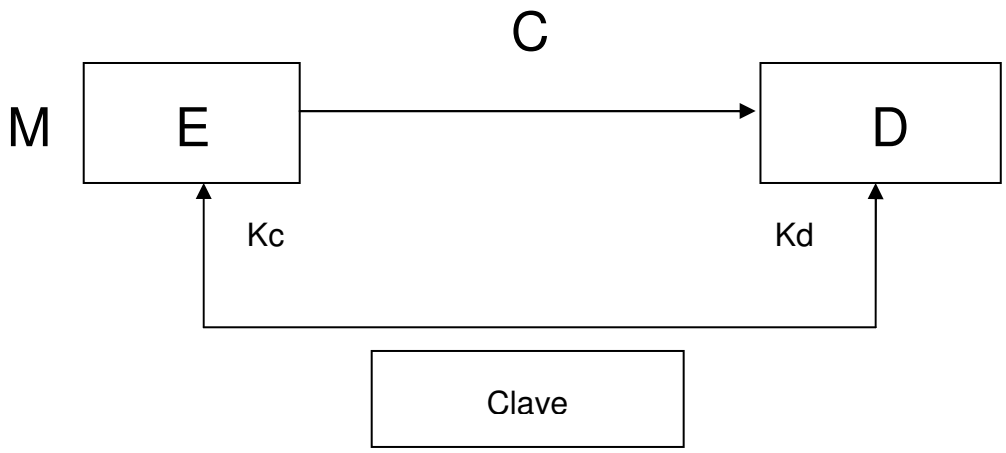
- Mensaje en claro. **M**
- Clave de cifrado. **Kc**
- Proceso de cifrado. **E**
- Texto cifrado. **C**
- Proceso de descifrado. **D**
- Clave de descifrado. **Kd**

1.3.1. Elementos de un criptosistema

En el diagrama 1 se presenta el modelo básico de un criptosistema, en donde: M, que representa al mensaje original o texto en claro, pasa por el proceso E, el proceso de cifrado, lo que lo convierte en C, que es el texto cifrado. Para esto, se utiliza la clave de cifrado, representada en el esquema por las letras Kc. El mensaje C es enviado entonces por el emisor y viaja a través de un canal seguro hacia el receptor que realizará el proceso de descifrado, representado por la letra

D, utilizando la clave de descifrado, representada por las letras Kd, culminando así el proceso de comunicación secreta.

Diagrama 1.



Fuente: http://www.wikilearning.com/imagescc/3584_w_54.jpg, 2006

Dentro del esquema se presentan cinco elementos básicos, aunque, como en todo proceso de comunicación, pueden intervenir también otros factores, como el ruido y la contaminación en los canales utilizados para transmitir la información. Estos factores son importantes y pueden alterar el proceso, por lo que serán abordados a profundidad en el siguiente capítulo.

1.4. Clasificación de los criptosistemas

La transformación que se lleva a cabo sobre el texto claro o mensaje original, así como las características de las claves utilizadas, marcan las diferencias entre los

sistemas de cifrado y las técnicas criptográficas. Existe una clasificación de criptosistemas, dependiendo de estas claves y técnicas. Una de las más comunes se basa en las claves utilizadas; ésta los divide en métodos simétricos, aquéllos en los que las claves de cifrado coinciden con la de descifrado y, por lo tanto, esa clave debe de permanecer secreta y supone un mutuo acuerdo previo entre emisor y receptor; y los métodos asimétricos, aquéllos en los que la clave de descifrado es diferente a la de cifrado. Debido a la necesidad de crear sistemas criptográficos mucho más seguros, actualmente se utiliza con frecuencia una tercera clase de criptografía, conocida como criptografía híbrida, en la que se combinan las dos anteriores.

1.4.1. Criptografía simétrica

Los métodos simétricos son propios de la criptografía clásica, conocida como criptografía de clave secreta. Éste es un método que utiliza la misma clave para cifrar y para descifrar los mensajes. De esta forma, las dos partes involucradas en el proceso de comunicación secreta, tanto el emisor como el receptor, se ponen de acuerdo con anterioridad sobre qué clave van a utilizar y se aseguran de que ambos tengan acceso a la misma clave. De esta manera, el emisor cifra el mensaje con esta clave y el receptor lo descifra con la misma. En este tipo de sistema la seguridad se basa en la clave y la confidencialidad de ésta y no tanto en el tipo de algoritmo o procedimiento que se utilice para encriptar. Aun cuando una persona ajena al emisor y al receptor trata de interceptar el mensaje, de nada le serviría saber el algoritmo que se utilizó en el cifrado si no tiene la clave. Por lo

tanto, es de suma importancia que la clave se encuentre dentro de un gran rango de posibilidades, para que sea muy difícil obtenerla.

En la actualidad, algunos programas de cómputo son capaces de descubrir claves muy rápidamente. Es por esto que el tamaño de la clave debe ser grande y el abanico de claves posibles debe ser muy amplio para dificultar la tarea del enemigo, o interceptor del mensaje cifrado, y evitar que ésta sea violada antes de llegar a su destino. Otro problema que presentan los sistemas de criptografía simétricos es que su utilización ideal sólo se da cuando la comunicación ocurre entre dos personas o, en su defecto, grupos muy pequeños de personas. Esto se debe a que el número de claves que se requerirían para hacer segura la comunicación entre grupos grandes, sería demasiado alto. Sin embargo, la principal limitante de los sistemas de criptografía simétrica es precisamente el canal de comunicación por el cual se transmiten las claves, ya que es mucho más fácil para un intruso interceptar la clave que probar las posibles combinaciones de claves que existen hasta dar con la que se ha utilizado.

Lo anterior remite nuevamente a la inseguridad de los canales de transmisión de dicha información. Se puede asegurar que una vez que la clave utilizada es del conocimiento del emisor y del receptor, y ha llegado a sus manos sin ser violado el sistema criptográfico simétrico puede presentar una transmisión segura de la información o del mensaje original. Sin embargo, es muy difícil asegurar que la clave durante su trayecto no caiga en manos enemigas y sea interceptada. Esto desembocó en el desarrollo de nuevos sistemas criptográficos

que evitaran este problema dando nacimiento a la criptografía asimétrica y la criptografía híbrida. Estás representan opciones más seguras de comunicación secreta.

1.4.2. Criptografía asimétrica

En este método de criptografía se utilizan dos claves diferentes para la transmisión de los mensajes: una clave pública y una clave privada. Para entender mejor su funcionamiento es necesario especificar a qué se alude cuando se habla de claves públicas y privadas, cuáles son sus características, diferencias y en qué caso se utilizan. La clave pública es, como su nombre lo indica, de carácter público; se puede entregar a cualquier persona. Cada receptor que utiliza los sistemas de criptografía asimétrica tiene su clave pública, que es la que cualquier emisor que desee comunicarse con este receptor debe utilizar para cifrar el mensaje. Sin embargo, sólo el receptor, que es dueño de la clave pública que el emisor utilizó, conoce la clave privada para descifrar dichos mensajes cifrados con su clave pública.

Por ejemplo, el Sr. X quiere comunicarse con el Sr. Y. Por lo tanto, lo único que el Sr. X tiene que hacer para lograrlo es conseguir una copia de la clave pública del Sr. Y y cifrar el mensaje con esta clave pública. Tras recibir el mensaje, el Sr. Y utiliza su clave privada, la cual sólo es conocida por él, para descifrar dicho mensaje. De este modo, todos los usuarios manejan las claves públicas de los demás, pero únicamente los propios usuarios conocen las claves privadas que

corresponden a sus claves públicas. Es decir, la clave pública funge como un buzón donde todo aquél que conozca su ubicación puede meter cartas, pero solamente el dueño del buzón tiene la llave para sacarlas. Esta llave es la clave privada. Un ejemplo común en la actualidad se da en los correos electrónicos, en los que la dirección de correo funge como la clave pública, y la contraseña para ingresar a ese correo es la clave privada.

Al igual que en los buenos sistemas de criptografía simétrica, la seguridad del sistema de cifrado de clave pública o asimétrico se basa también en la clave y no en el algoritmo o proceso de cifrado. Por lo tanto, el tamaño de la clave es una medida de seguridad del sistema y ésta debe ser bastante grande para evitar una violación del mensaje. A pesar de las ventajas de seguridad que presentan los sistemas de criptografía asimétrica sobre los de criptografía simétrica, existen también desventajas; por ejemplo, los mensajes requieren de un tiempo mucho mayor de proceso en un sistema de criptografía asimétrico que en uno simétrico. Además, las claves deben ser de mayor tamaño que las simétricas. Por último, el resultado del mensaje cifrado ocupa mucho mayor espacio que el mensaje original.

1.4.3. Criptografía híbrida

Es un método criptográfico que utiliza tanto las técnicas de la criptografía simétrica, como aquéllas de la criptografía asimétrica y las combina para lograr una unión entre la seguridad, la rapidez y la eficacia de ambas. Esto significa que

se utiliza el cifrado con clave pública para compartir una clave para el cifrado simétrico que será con el que se cifre el mensaje original. De este modo, se evita el problema de inseguridad de transmisión de claves de los sistemas simétricos, ahorrando a su vez tiempo y esfuerzo en el cifrado y descifrado de mensajes de los sistemas asimétricos que, en este caso, no se utilizarán para cifrar el mensaje.

1.5. Desarrollo histórico de la criptografía

La criptografía como medio para proteger la información personal es un arte tan antiguo como la propia escritura. Ha permanecido de ese modo durante siglos con la gran ayuda que le han brindado, sobre todo, las estrategias desarrolladas en los círculos militares, de forma que, si el mensajero era interceptado, la información real o mensaje original que éste tenía no cayera en manos del enemigo, aun cuando la tuviera físicamente en su poder. También ha sido de gran ayuda en asuntos de índole diplomático, ya que, en un principio, eran los únicos que presentaban una auténtica necesidad de las técnicas criptográficas.

1.5.1. Criptografía antigua

Desde tiempos inmemorables, los mensajes cifrados han jugado un papel destacado en la historia, en diversos campos de la actividad humana, como son la milicia, la diplomacia, el espionaje y, en tiempos más recientes, el comercio y las transacciones financieras. Esto la convierte en una técnica tan antigua como la civilización.

Es así como diversas civilizaciones se han valido de técnicas criptográficas para asegurar la confidencialidad de la información más importante. Los egipcios, por ejemplo, utilizaban métodos criptográficos. Sus sacerdotes utilizaban jeroglíficos, que ahora hemos estudiado y descifrado, pero que en su época eran incomprensibles para los demás. Como otro ejemplo están los babilónicos, quienes utilizaban escritura cuneiforme. Ésta es la forma más temprana conocida de expresión escrita de la que se han encontrado vestigios arqueológicos y que recibe este nombre debido a que estaba conformada por marcas en forma de cuña o semicírculos.

A todo esto se le podría definir como los inicios de las técnicas criptográficas y confirman que, desde que el hombre comenzó a tener un tipo de organización social, empezó también a tener la necesidad de transmitir información importante de forma secreta, sobre todo entre personas con una jerarquía alta en dicha sociedad.

Sin embargo, el primer antecedente claro de un sistema criptográfico se presentó durante la guerra entre Atenas y Esparta, en el siglo V a.c. Este sistema se basaba en construir dos rodillos exactamente iguales que tenían en su poder tanto el emisor como el receptor del mensaje. Estos rodillos, conocidos como “escítalas”, eran utilizados para cifrar y descifrar el mensaje. También se incluían símbolos innecesarios dentro de los mensajes, que se redactaban de forma vertical sobre una cinta de pergamino enrollada. Esta actividad puede ser

considerada como uno de los primeros procesos de cifrado. Estos símbolos aparecía desordenados o traspuestos al desenrollar la cinta, de tal forma que sólo se pudiera leer el texto al enrollar la cinta de nuevo en una escítala del mismo grosor, logrando el proceso de descifrado y aclarando el contenido del mensaje original.

Otra de las técnicas criptográficas antiguas de las que se tienen conocimiento data de la época de los romanos. Se le conoce como "método César"; ya que, supuestamente, Julio César lo utilizó en sus campañas. Este método consistía en una sustitución de determinados símbolos o letras por otros según una regla fija. Por ejemplo, se sustituía la primera letra del alfabeto, A, por la cuarta letra, D; la segunda, B, por la quinta E; y así sucesivamente con todas las demás. De esta forma, a cada letra del mensaje cifrado le corresponde una letra tres puestos adelante en el abecedario. En este rudimentario método de cifrado, el procedimiento dejaba al descubierto la frecuencia utilizada en el cifrado y, por tanto, era un método poco seguro y fácil de descifrar.

Otro ejemplo histórico es el que se utiliza en la Biblia, donde se puede encontrar texto cifrado en hebreo; o en el Kamasutra, donde entre las 64 artes que se recomiendan se incluye la utilización de la escritura secreta. *"Sin embargo, es del siglo XIV la obra más antigua que existe sobre criptografía. Setitua Liber Zifrorum y su autor, Cicco Simoneta, estudia en ella diversos sistemas basados en simples sustituciones de letras".* (Fúster *et al.,* 2001:2). Posteriormente, alrededor de 1465, el italiano León Battista Alberti, quien era un destacado pintor, músico,

escritor y arquitecto de la época, destaca en el campo del criptoanálisis y es considerado el padre de la criptología, ya que inventó un nuevo sistema, basado en la sustitución múltiple, que supuso grandes avances para la criptografía. Este sistema consistía en sustituir las letras, como en el "método César", pero empleando varios abecedarios, avanzando de uno a otro cada tres o cuatro palabras.

Durante el siglo XVI, la criptografía y su uso se generalizaron, sobre todo, en los ambientes diplomáticos. En el año de 1586, sobresale uno de los criptógrafos más importantes del siglo: el francés Blaise de Vingenere, con la publicación de su obra titulada *Traicté des Chiffres* (*La escritura secreta*) donde reúne diversos métodos utilizados durante esa época y crea un método de cifrado que actualmente lleva su nombre. Utilizaba una clave más larga que los métodos anteriores, por lo que provee mayor seguridad y mayor dificultad para el proceso de descifrado en ausencia de la clave. Sin embargo, no es considerado aún un sistema criptográfico con una seguridad probada matemáticamente.

Durante los siglos XVII, XVIII y XIX aumentó el interés por la criptografía, principalmente, de parte de la nobleza. Un ejemplo sería el uso de cifras con un alfabeto de más de 500 símbolos por parte de los ejércitos de Felipe II. Este sistema fue creado por los matemáticos del rey y de acuerdo a ellos era inquebrantable. Por su parte, la reina Isabel I de Inglaterra ejecutó a su prima, la reina María Estuardo, reina de los escoceses, al descubrir que ésta estaba

planeando un golpe de estado en su contra. Esto se logró gracias a un criptoanálisis exitoso por parte de los matemáticos de Isabel I.

1.5.2. Criptografía moderna

El periodo que más cambios tuvo para la criptografía, al igual que para otras tecnologías, tuvo lugar durante las dos guerras mundiales. En el caso de la criptografía, éstos se dieron por la necesidad de transmisión de importantes mensajes que contenían información relevante y estratégica de corte militar y diplomática. Esta transmisión de información se dio principalmente por medio de nuevas tecnologías, como la radiotecnia y la telegrafía. También surge el uso de una nueva herramienta en la criptografía, la cual representa un avance considerable para el desarrollo de las técnicas criptográficas, ya que permite conseguir mejores y más complejas cifras, haciendo de la criptografía un método mucho más seguro. Todo esto fue posible mediante la invención y utilización de las "máquinas de cálculo".

Durante la Primera Guerra Mundial, el descubrimiento de una información secreta que fue desencriptada por los aliados británicos del telegrama conocido como *Zimmermann*, fue crucial para el desarrollo de los eventos. En este telegrama se descubrió al ministro alemán tratando de convencer a Japón y a México para que invadieran Estados Unidos, información que fue el detonante que impulsó a que Estados Unidos tomara la decisión de entrar a la guerra, lo cual cambió el curso de la historia.

Sin embargo, durante la Segunda Guerra Mundial fue cuando la criptografía dio un salto considerable en la tecnología que utilizaba; esto con la invención de la más conocida de las máquinas de cálculo, realizada por el alemán Arthur Scherbius, la máquina *Enigma*. Esta máquina criptográfica fue considerada por el ejército nazi como inviolable. Este dispositivo consistía en una máquina de rotores que automatizaba considerablemente los cálculos necesarios para lograr un cifrado y descifrado de los mensajes. Para romper el secreto de su funcionamiento y vencer el ingenio alemán fue necesario contar con la ayuda de los mejores matemáticos de la época y la ayuda de las más avanzadas computadoras.

Debido a esto, los mayores avances tanto de la criptografía como del criptoanálisis no empezaron sino hasta entonces. Pero, esta herramienta, que un principio significó una de las armas más poderosas de los nazis y que les dotó de significativa ventaja en relación con sus oponentes, fue precisamente la causa de su derrota.

En 1942, aproximadamente, Alan Turing, unos de los precursores de la inteligencia artificial y la informática, logró romper el encriptado realizado por la máquina y desenmascaró las claves de *Enigma*, desarrollando una máquina llamada *Colossus,* la cual fue precursora de las computadoras actuales.

El desenlace de la Segunda Guerra Mundial se vio influenciado por el uso de la criptografía y el criptoanálisis. Éstos fueron el detonante para que los

acontecimientos tomaran el curso que hoy se conocen, ya que en la contienda existió un factor decisivo y apenas conocido: los aliados podían descifrar en su totalidad los mensajes secretos de los alemanes, tomando ventaja con esta información. Durante la Segunda Guerra Mundial y, como consecuencia de las ventajas que en un principio representó la máquina *Enigma* para los nazis, se construyeron varias máquinas basadas en métodos muy similares. La versión japonesa era una máquina casi igual a *Enigma*, conocida como *"Purple"* debido a que ese era el nombre que se le daba a sus códigos, los cuales también fueron descubiertos por un grupo de analistas. La versión estadounidense de la máquina *Enigma* se llamó *Sigaba* y era conocida entre los alemanes como *La Gran Máquina.* Este aparato fue el único que conservó sus secretos durante la Segunda Guerra Mundial y funcionaba principalmente en estaciones fijas.

Después de la Segunda Guerra Mundial, la criptografía tuvo varios avances en el ámbito teórico. Tales fueron las aportaciones de Claude Shannon, con sus investigaciones acerca de la teoría de la información, que propiciaron un desarrollo teórico del tema. Además de estos avances teóricos, la criptografía se vio revolucionada en la década de los años setentas con la invención del primer diseño lógico de un cifrador, realizado por la *NBS (Oficina Nacional de Estándares,* por sus siglas en inglés, actualmente conocida como Instituto *Nacional de Estándares y Tecnología),* que produjo aquél que fuera el principal sistema criptográfico de finales de siglo: el conocido como *Estándar de Encriptado de Datos,* o *DES*, que dio paso a lo que sería hasta ahora la última revolución

criptográfica teórica y práctica: la criptografía asimétrica, que sigue presentando avances apoyándose en la informática.

Durante la segunda mitad del siglo XX han surgido nuevas aplicaciones para la criptografía. Debido al desarrollo acelerado de la cultura informática e Internet, los avances en las comunicaciones electrónicas y la gran demanda general y masiva de estas, existen grandes cantidades de información confidencial que es necesario proteger durante su trayecto. De esta forma, el uso de la criptografía ha dejado de ser una exigencia de las minorías y se ha convertido en una necesidad real de la gente común que requiere proteger su información y su intimidad. Además de proteger toda esta información que viaja a través de redes de comunicación electrónicas, los avances en esta área han traído como consecuencia que los sistemas criptográficos, que antes resultaban seguros frente a procedimientos manuales, no lo sean ante la eficacia y rapidez de las computadoras. Es por esto que los sistemas criptográficos clásicos han tenido que ser sustituidos por nuevos sistemas criptográficos de seguridad matemática demostrable.

1.5.3. Criptografía contemporánea

La criptografía actual se ha beneficiado tanto del avance en las comunicaciones como del desarrollo exponencial del poder de cómputo. Esto ha llevado a la creación de cifras y algoritmos de encriptado más avanzados y, por ende, más difíciles de descifrar. Sin embargo, dichos avances traen consigo nuevos riesgos

de ataque, ya que la tecnología queda al alcance no sólo de los participantes en el intercambio de información, sino también de aquellos posibles interceptores de la comunicación. Es por esto que en los últimos años se han buscado nuevas formas de hacer más seguro el tránsito de la información confidencial.

Uno de los principales avances que, se prevé, tendrá un gran impacto en la comunicación criptográfica en el futuro es el surgimiento de la criptografía cuántica. Esta nueva forma de criptografía basa su seguridad en la física del envío del mensaje, contrario a la criptografía tradicional que utiliza varias técnicas matemáticas de difícil cómputo como la factorización de integrales para evitar que los interceptores conozcan el contenido del mensaje confidencial. En la criptografía cuántica, el mensaje es enviado alterando las características físicas de un conjunto de cuantos (generalmente fotones), que son unidades elementales e indivisibles de energía. Estos cuantos son enviados luego por un medio físico, como un cable de fibra de vidrio, mediante pulsos de energía.

La criptografía cuántica basa su seguridad en el *Principio de Indeterminación de Heisenberg*. De acuerdo con este principio cuántico, no se puede determinar, simultáneamente y con precisión arbitraria, ciertos pares de variables físicas, como son, por ejemplo, la posición y la cantidad de movimiento de un objeto dado. Es decir, en mecánica cuántica la medición no es un acto pasivo, como en la mecánica tradicional. El acto de medir una característica de una partícula de energía afecta a otra característica interrelacionada. Por ende,

cualquier intento de intercepción del mensaje por parte de un intruso dejaría evidencia física en el mensaje, advirtiendo a los participantes del ataque.

El enfoque más utilizado en criptografía cuántica es el de polarización de fotones de Bennett y Bassard, de 1984. En éste, se toman dos características de polarización de los fotones, por ejemplo, polarización lineal que puede ser vertical u horizontal, y polarización circular, que puede ser levógira o dextrógira (con giro a la izquierda o a la derecha, respectivamente).

El emisor afecta una característica de los fotones para codificar el mensaje. Por ejemplo, la polarización vertical pudiera equivaler a “0”, mientras que la polarización horizontal lo haría a “1”. Además, para evitar la intercepción exitosa del mensaje, los fotones son pasados por un filtro que los polariza de manera dextrógira o levógira de manera aleatoria. Este orden aleatorio de giro es transferido al receptor. Una vez recibidos, los fotones son pasados por un filtro que verifica que la polarización circular sea la misma que la utilizada por el emisor y la polarización lineal es medida. En el caso de un intento de intercepción, los fotones interceptados son alterados y se alerta tanto al emisor como al receptor del suceso. Esto permite detener el tránsito de información antes de que el intruso conozca el mensaje.

CAPÍTULO 2. CRIPTOGRAFÍA COMO PROCESO DE COMUNICACIÓN

2.1. Modelo de comunicación

Existen diversos modelos referentes al proceso de comunicación. Estos modelos abarcan la acción comunicativa desde diferentes perspectivas y varían en la cantidad de pasos que mencionan como parte importante de esta. Sin embargo, es importante mencionar que, si bien las partes siempre están presentes en el ciclo de comunicación, la línea que las divide es tan fina que, a veces, se vuelve imposible distinguirlas y se contienen unas dentro de las otras.

Para explicar qué es el proceso de la comunicación, se debe conocer primero qué es un proceso y qué es comunicación. Proceso es el conjunto de las fases sucesivas de un fenómeno natural o de una operación artificial, es decir, una operación o tratamiento continuo. Por lo tanto, el concepto de proceso engloba lo dinámico, el constante cambio y movimiento, ya que no es estático y no descansa. “Los componentes de un proceso ‘interaccionan’, es decir cada uno de ellos influye sobre los demás”. (Berlo, 1969:19).

Por otro lado, según Ricci (1983:25), el acto de la comunicación “es la unidad más pequeña susceptible de formar parte de un intercambio comunicativo y que una persona puede emitir con una única y precisa intensión”. Éste puede estar constituido por “la producción de una sola palabra, de un gesto, aunque más

a menudo suele ir acompañado de una sola combinación de elementos verbales y no verbales".

La comunicación es en términos más sencillos la acción y efecto de comunicar o comunicarse. Es la transmisión de señales mediante un código común del emisor al receptor, aunque también puede referirse a las vías existentes para transportar o trasladarse de un lugar a otro. El proceso de comunicación está conformado por varios elementos que interactúan entre sí, dando lugar al intercambio de información entre una o más personas o entidades. Sin embargo, al ser un tema de suma importancia para su estudio y análisis a lo largo de la historia, diversos teóricos han abordado el proceso comunicativo desde diferentes perspectivas, ya que, al construir una realidad, el especialista organiza sus percepciones libremente.

A raíz de esto, han surgido diferentes modelos de comunicación que reiteran los puntos comunes entre éstos y aportan nuevos elementos y componentes al proceso. Sin embargo, existen tres elementos que se encuentran siempre presentes en cualquier modelo de comunicación. Estos son el emisor, el mensaje y el receptor. Se parte de la premisa de que para que exista comunicación se requiere alguien que comunique, algo que comunicar y alguien que reciba esa información. A partir de estos tres elementos, se derivan otros varios que influyen en el proceso de la comunicación, tales como el canal, el ruido, el contexto situacional en el que se da la comunicación y la retroalimentación, entre otros.

Para el estudio de la comunicación secreta que se lleva a cabo por medio de la criptografía, existen tres importantes modelos que han servido como aportación para estudiar los procesos comunicativos que cumplen con las características de la misma. Estos modelos fueron presentados por Shannon, Schramm y Berlo. Dichos modelos se expondrán durante este capítulo y servirán de pauta para el análisis de la criptografía como proceso de comunicación.

2.1.1. Teoría de la información de Shannon y Weaver

Claude Elwood Shannon, nació el 30 de abril de 1916 en Michigan, Estados Unidos, y se le considera como el padre de la teoría de la información. Desde joven, Shannon mostró una inclinación hacia la mecánica y sus aplicaciones. En 1932 ingresó a la Universidad Estatal de Michigan. En 1936 obtuvo los títulos de ingeniero eléctrico y matemático. En 1936 fue asistente de investigación en el departamento de Ingeniería Eléctrica en el Instituto Tecnológico de Massachusetts (MIT). Su situación le permitió continuar estudiando mientras trabajaba por horas para el departamento, obteniendo como resultado la calculadora más avanzada de esa era. En ese momento surgió su interés hacia los circuitos de relevadores complejos, sumado a su gusto por la lógica y el álgebra booleana.

Estos nuevos intereses pudo desarrollarlos durante el verano de 1937, que pasó en los laboratorios Bell en la ciudad de Nueva York. Su tesis doctoral en el MIT, despertó un interés considerable por parte de otros investigadores tras su publicación en 1938 en las revistas especializadas. En 1940 le fue concedido el

premio *Ingenieros Americanos del Instituto Americano Alfred Nobel* de Estados Unidos, presea otorgada cada año a una persona de no más de treinta años. Un cuarto de siglo más tarde H. H. Goldstine, en su libro *Las computadoras desde Pascal hasta Von Neumann*, citó su tesis como una de las más importantes de la historia que ayudó a cambiar el diseño de circuitos digitales. En el mismo año estudió una maestría en ingeniería eléctrica y se doctoró en filosofía matemática.

Shannon pasó quince años en los laboratorios Bell, una asociación muy fructífera con muchos matemáticos y científicos de primera línea como Harry Nyquist, Brattain, Bardeen y Shockley, inventores del transistor; George Stibitz, quien construyó computadoras basadas en relevadores y muchos otros más. Durante este período trabajó en muchas áreas, siendo lo más destacable su trabajo referente a la teoría de la información, que fue publicado en 1948 bajo el nombre de *Una Teoría Matemática de la Comunicación*.

En este trabajo se demostró que todas las fuentes de información (telégrafo eléctrico, teléfono, radio, la gente que habla, las cámaras de televisión, etc.) se pueden medir y que los canales de comunicación tienen una unidad de medida similar. Mostró también que la información se puede transmitir sobre un canal si, y solamente si, la magnitud de la fuente no excede la capacidad de transmisión del canal que la conduce, y sentó las bases para la corrección de errores, supresión de ruidos y redundancia.

En el área de las computadoras y de la inteligencia artificial, publicó en 1950 un trabajo que describía la programación de una computadora para jugar ajedrez, convirtiéndose en la base de posteriores desarrollos. Falleció el 24 de febrero del año 2001, a la edad de 84 años, después de una larga lucha en contra del Alzheimer.

Por su parte, Warren Weaver nació en Reedsburg, Winsconsin, en Estados Unidos, en 1894. Fue un reconocido matemático estadounidense y otro de los pioneros de la teoría de la información. El modelo propuesto por esta teoría es el resultado de las aportaciones realizadas por Claude E. Shannon, en su *Teoría Matemática de la Comunicación,* publicada por el *Bell System Technical Journal* en octubre de 1948, y por las aportaciones y observaciones realizadas a este trabajo por Warren Weaver, en un ensayo que fue publicado junto al texto anterior en julio de 1949. Weaver murió en New Milford, Connecticut, en el año de 1978.

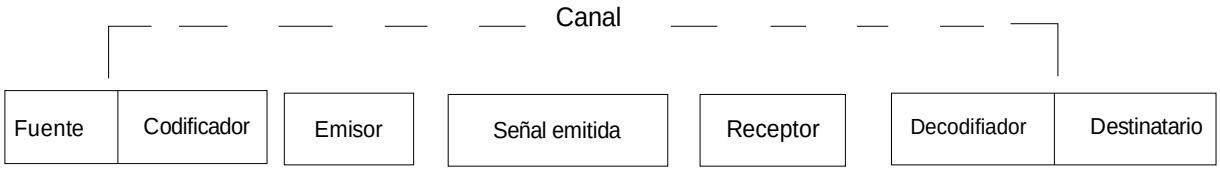
La teoría de la información propiamente dicha es un clásico esquema al que se refieren prácticamente todos los teóricos de la información y varios teóricos de la comunicación. En su forma más desarrollada, comprende ocho elementos. Estos son la fuente, el codificador, el emisor, el mensaje, el canal, el receptor, el decodificador y el destinatario, presentados en un esquema lineal de la comunicación (diagrama 2). De acuerdo con este esquema, el paso de la información se da de la fuente al destinatario. Entre ellos existe una disminución de la entropía o incertidumbre informativa, ya que cuando el mensaje es recibido

ya se encuentra decodificado, mientras que entre el emisor y el receptor existe un aumento de entropía.

> *El codificador inscribe en el sector energético las modulaciones salidas de la fuente, el decodificador las identifica y la transmite al destinatario. Entre el emisor y el receptor, el medio, que es todo o parte, del conductor, transporta la energía modulada. El canal es el conjunto del dispositivo situado entre la salida de la fuente y la entrada del destinatario.* (Escarpit, 1976:34).

Este modelo de la información, no sólo es aplicable a la telecomunicación, a pesar de haber nacido con ese propósito por su creador Shannon. En este aspecto, precisamente Weaver realiza las aportaciones necesarias a la teoría para resaltar la importancia de dicho modelo en la comunicación humana. En una comunicación interpersonal, la parte del cerebro situada en el córtex actúa como fuente; otra parte, situada en la zona temporal del hemisferio izquierdo, en el caso de los diestros, sirve como codificador. Desde el centro de codificación o el hemisferio izquierdo se producen y envían impulsos que modulan la energía acústica producida por el sistema muscular, el aparato fonador y el sistema respiratorio. Esto es el proceso de emitir el pensamiento en forma de mensaje por medio de las palabras. La energía previamente modulada se transporta por un medio, que en este caso es el aire, para ser captada por un receptor, el sistema auditivo, conformado por el pabellón auditivo, el tímpano, los huesos del oído medio y el oído interno. Este último envía las vibraciones emitidas por la voz hasta el nervio auditivo, que funge como decodificador. De esta forma, las modulaciones ya decodificadas forman el mensaje que es recibido por el destinatario que está situado en el córtex de la persona que escucha.

Diagrama 2. Modelo de Comunicación de Shannon y Weaver



Fuente: Gallardo, cit. por Escarpit (1990:130).

2.1.2. Teoría de la comunicación de Wilbur Schramm

Wilbur L. Schramm, nació en Marietta, Ohio, Estados Unidos, en 1907. Estudió en la Universidad de Harvard y se doctoró en literatura americana en la Universidad de Iowa en 1932. En este mismo centro comenzó como docente en 1934 y dirigió la Escuela de Periodismo desde 1943 hasta 1947. Fue Director del Instituto de Investigación en Comunicación de la Universidad de Illinois de 1947 a 1995 y decano de los estudios de Comunicación de 1950 a 1955. En este último año se traslada a la Universidad de Stanford donde dirige el Instituto para la Investigación sobre Comunicación hasta 1973, año en el que es nombrado profesor emérito. Posteriormente, dirigió el Instituto de Comunicación de la Universidad de Hawaii en Honolulu.

Junto con Everett Rogers y Daniel Lerner, Schramm es uno de los teóricos norteamericanos que estudiaron el problema de la comunicación al servicio del desarrollo, ejerciendo una influencia significativa en los foros de la UNESCO y en el discurso de las doctrinas de la comunicación para el desarrollo surgidas en

América Latina. Asimismo, con Frederick S. Siebert (1901-1982) y Theodore Peterson (1918), publicó en 1956 un libro de amplio eco académico *Four Theories of the Press*, en el que se relacionan sistemas políticos con sistemas de medios y se plantean cuatro modelos de prensa: el autoritario, el liberal, el comunista-soviético y el de responsabilidad social.

Schramm menciona que la comunicación en su forma más simple consiste en un comunicador o emisor, un mensaje y un perceptor o receptor. Dice, a su vez, que el emisor y el receptor pueden llegar a ser la misma persona si hablamos, por ejemplo, de la comunicación intrapersonal. Sin embargo, menciona también que en cualquier tipo de comunicación llega un momento en que el mensaje emitido no es más que una simple señal con algún tipo de significado para el emisor y con alguna interpretación que le dará el receptor y se encuentre separado de ellos. Por ejemplo, en una comunicación escrita el mensaje en un momento es tan sólo tinta sobre un papel, en una comunicación oral el mensaje es una serie de condensaciones y rarefacciones en el aire.

> *Estos signos tiene un significado señalado por nosotros convencionalmente o por la experiencia. Por ejemplo, una palabra impresa en un lenguaje que no conocemos puede tener poco o ningún significado secreto que solamente dos personas pueden conocerlo. Por otro lado una luz roja de tráfico probablemente tiene el mismo significado para todos los conductores de automóvil, y un grito de terror posiblemente quiere decir lo mismo en todas partes. Este es uno de los principios básico de la teoría general de la comunicación; que los signos solamente tiene el significado que la experiencia de la persona permite atribuir*. (Schramm, 1965:6).

Es decir, los mensajes sólo pueden ser elaborados a partir de signos y códigos que sean conocidos por quien los elabora, y quien recibe estos signos que conforman el mensaje sólo puede darles un significado de acuerdo con lo que

conoce de ellos. A este conjunto de significados se le llama “marco de referencia” y es inevitablemente utilizado al momento de interpretar los significados de todos los mensajes que nos rodean. De éste depende la comunicación que tiene un individuo. El que dos personas o entidades con marcos de referencia muy distintos se comuniquen da lugar a las malas interpretaciones, por lo que es importante compartir este marco de referencia entre emisor y receptor para que el mensaje sea formulado e interpretado correctamente.

Schramm también menciona algunas características que presentan los mensajes. Señala, por ejemplo, que los mensajes tienen dos formas diferentes de significado: la denotativa, que es referente al significado común y es aproximadamente el mismo para todas las personas que utilizan un mismo código (por ejemplo, el idioma), y el significado connotativo, que se refiere a las emociones, es decir, qué tan bueno o agresivo puede resultarle al receptor dicho mensaje. Además, señala que los mensajes tienen un significado superficial, el cual es simplemente lo que se expresa, y un significado latente que se basa en el contexto de relación existente entre el emisor y el receptor.

> *Por ejemplo: Cuando decimos `buenos días´, generalmente no significamos nada sobre el color azul del cielo matutino o sobre el brillo del sol de la mañana; más bien, estamos expresando algo sobre nuestra relación social con el perceptor. Decimos algo como: `somos todavía amigos´, o `me alegra verte´, o algo parecido. Muchos mensajes toman su significado principal del contexto de la relación entre el emisor y el perceptor, y por esta razón es a veces peligroso interpretar lo que se expresa según definición `de las palabras´, sin considerar su significado latente.* (Schramm, 1965:7).

En el proceso de comunicación de un mensaje intervienen, además del contenido de dicho mensaje, factores que conforman una serie de mensajes

paralelos. Por ejemplo, en el caso de una conversación, el mensaje no estaría conformado tan sólo por lo que se dice, sino por la entonación con la que se dice, la rapidez, el énfasis, el volumen y la gesticulación que se da al momento de decir el mensaje. Todo esto dota de significado al mensaje.

El primer obstáculo que un mensaje debe vencer es el proceso de selección por parte del receptor, para ser aceptado o rechazado por este una vez que ha sido recibido. Este proceso de aceptación o de rechazo depende de la medida en que dicho mensaje coincide con los valores y creencias del receptor y de qué tan efectivamente se ubique entre ellas. Este proceso de aceptación o de rechazo de un mensaje se da tanto a nivel conciente como subconsciente.

Además de lo anterior, para que el mensaje sea aceptado o, en su defecto, rechazado por el receptor existe otro factor determinante al que Schramm menciona como “grupo de referencia”. Al igual que el individuo aprecia sus creencias y valores y se apega a estos, asimismo, aprecia su pertenencia a grupos, tales como la familia, sus compañeros de trabajo, grupo de amistades, etc. Los mensajes de cierta relevancia que este individuo pueda recibir a lo largo de su vida, estarán ligados a alguno de sus “grupos de referencia”. Debido al aprecio que siente por dicho grupo o al valor que le atribuye, hará una comparación entre los valores y creencias que tiene el grupo al que está ligado el mensaje recibido. Si coincide con ellas, el mensaje será aceptado.

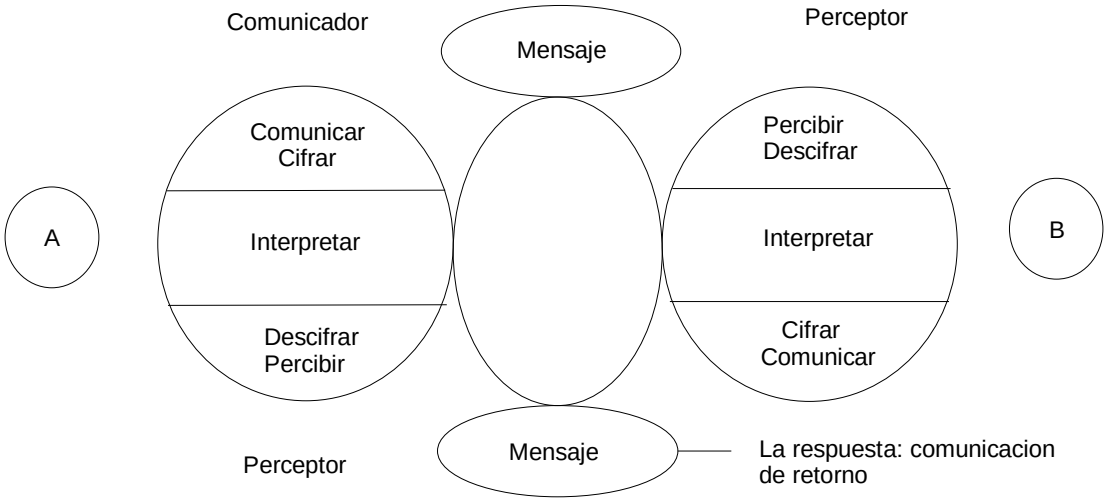
En caso contrario, es muy probable que para lograr dicha aceptación, el mensaje deba sufrir cambios sustanciales para apegarse más hacia los intereses

del “grupo de referencia” del individuo. Cuando el mensaje trata de penetrar en una zona o temática donde las creencias del individuo como las de su grupo de referencia son muy arraigadas y contrarias a la significación de dicho mensaje, Schramm menciona la posibilidad de obtener mejores resultados en el proceso de aceptación mediante lo que llama “canalización” de las actitudes. Ésta consiste, precisamente, en tratar de darle un nuevo enfoque a las actitudes ya existentes de manera sutil para que el individuo no lo resienta tanto:

> *Si se quiere conseguir algo de cierta importancia con un mensaje, el comunicador debe buscar que el perceptor lo seleccione y preste atención a ese mensaje, debe tratar de que lo acepte, e intentar que pase a través de la censura y las normas opuestas de los valores de grupo.* (Schramm, 1965:10).

Un último paso en el proceso comunicativo ocurre con la información que regresa desde el receptor hasta el emisor para dar a conocer a este último si su mensaje ha tenido éxito o no; a esto se le denomina “comunicación de retorno”. Se dice entonces que el modelo propuesto por Wilbur Schramm (diagrama 3) está compuesto por siete elementos, de los cuales el comunicador, el mensaje y el perceptor son los tres básicos involucrados en el proceso de la comunicación. Éstos son alterados o influenciados por factores como el marco de referencia, los grupos de referencia, la canalización y la comunicación de retorno.

Diagrama 3. Modelo de comunicación de Wilbur Schramm



Fuente: Gallardo, cit. por Escarpit (1990:135)

2.1.3. Teoría del proceso de comunicación de David K. Berlo

David K. Berlo nació en 1929. Fue discípulo de Wilbur Schramm en la Escuela de Periodismo de la Universidad de Illinois, donde se doctoró en 1956, con la tesis *Allocation of Procedural Responsibilities as a Determinant of Group Productivity and Satisfaction,* dirigida por Charles E. Osgood. En 1960 publicó su libro más conocido, en el que hace la exposición de sus modelos teóricos sobre la naturaleza psicológica de la comunicación: *Process of Communication: An Introduction to Theory and Practice*. Fue director del Departamento de Comunicación de la Universidad del Estado de Michigan, donde dirigió, entre otras muchas tesis doctorales, la del teórico boliviano Luis Ramiro Beltrán. Fue,

además, rector de la Universidad de Illinois de 1971 a 1973. Ese año se retiró del cargo por graves cuestionamientos en la gestión.

El modelo de comunicación propuesto por David K. Berlo (diagrama 4) está compuesto por seis elementos que integran la cadena comunicativa. Estos son: la fuente de la comunicación, el encodificador, el mensaje, el canal, el decodificador y el receptor de la comunicación. Es a estos elementos del proceso comunicativo a los que se refiere al hablar de la comunicación en sus distintos niveles de complejidad. Todo tipo de comunicación humana tiene una fuente, que es la persona o el grupo de personas que persiguen un objetivo por medio de dicha comunicación. Este objetivo o propósito de la fuente de la comunicación se expresa en forma de mensaje. *"En la comunicación humana un mensaje puede ser considerado como conducta física: traducción de ideas, propósitos e intenciones en un código, en un conjunto sistemático de símbolos." (*Berlo,1969:24).

Para lograr que el propósito de la fuente de la comunicación sea transformado en mensaje, éste debe pasar por un proceso de traducción a un código, lenguaje, etc., que sea compartido tanto por la fuente como por el receptor de la comunicación. A su vez, para que este último pueda darle una interpretación correcta al mensaje se requiere de otro de los elementos del proceso comunicativo, conocido como *encodificador*, que es el encargado de tomar las ideas de la fuente y disponerlas en un código, expresando así el objetivo y propósito de la fuente en forma de mensaje.

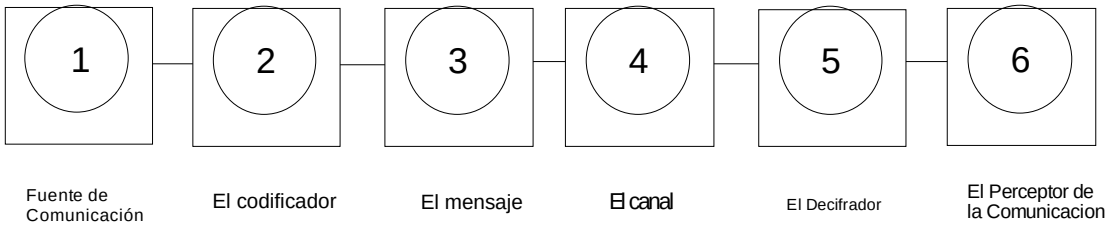
Los dos primeros elementos del proceso comunicativo, como lo señala Berlo, pueden, sin embargo, ser uno sólo dependiendo de la complejidad de la situación de comunicación. Por ejemplo, dentro del proceso de comunicación que se da entre dos personas, la fuente y el encodificador es uno sólo, ya que la función de encodificar es realizada por la capacidad motora de la fuente, como podría ser la voz, los gestos, las señas, etc., mientras que en una situación de comunicación más compleja, estos dos elementos se separan y existen tanto la fuente de la comunicación como el encodificador como entidades individuales. *"Por ejemplo, podemos considerar a un gerente de ventas como la 'fuente' y a los vendedores como sus encodificadores; es decir, que estos últimos son gente que en forma de mensaje traduce para el consumidor la intención o los propósitos del gerente".* (Berlo, 1969:25).

Otro de los elementos propuestos en el modelo de Berlo es el *canal*. El autor hace referencia a este como el medio o conducto, portador de mensajes. La elección del canal es un factor importante para la efectividad de la comunicación, ya que dependiendo de las cualidades que tenga el canal varía la calidad de la transmisión. Así como la fuente necesita un encodificador para traducir los objetivos perseguidos en forma de mensajes, el receptor requiere de un decoficador para retraducir el mensaje recibido y previamente encodificado y, de esta forma, hacerlo utilizable para el receptor. Al ser decodificado el mensaje, éste es recibido por el receptor.

Esto hace posible la comunicación, ya que para que exista comunicación propiamente dicha el mensaje debe llegar en su recorrido hasta el receptor, quien

debe responder al estímulo que le ha sido enviado por la fuente. Sin embargo, fuente y receptor no siempre son entidades distintas, ya que puede también ser la misma persona, si hablamos de comunicación intrapersonal. En la comunicación entre una o dos personas, los sentidos juegan el papel de descifradores de códigos para los mensajes.

Diagrama 4. Modelo de comunicación de David K. Berlo



Fuente: Gallardo, cit. por Escarpit (1990:133).

A lo largo de este capítulo se utilizará el siguiente ejemplo para explicar las partes del proceso comunicativo como una unidad (tomando como base los modelos anteriormente expuestos) en el contexto de la comunicación criptográfica.

Se supone la existencia de una batalla entre el ejército rojo y el ejército azul. Un general del ejército rojo desea enviar un mensaje a un coronel encargado de la artillería en el frente de batalla. El general desea dar la siguiente orden al coronel: "mover artillería al norte", por lo que pide a su criptógrafo que cifre el mensaje para evitar que en su tránsito pueda ser descubierto por los miembros del ejército azul; el resultado es el siguiente: "MPXHV-ASVLQRLZRK-AM-NPTXJ". Inmediatamente después de cifrar el mensaje, éste es enviado por clave Morse hasta el frente de batalla para ser entregado al coronel. En su tránsito, el mensaje

es interceptado por soldados del ejército azul, quienes tratan de descifrarlo sin resultados. Al llegar al frente de batalla el mensaje es descifrado por el criptógrafo y le es entregado el mensaje original al coronel del ejército rojo y éste le envía al general un mensaje en respuesta, informándole de las acciones que tomará.

En el siguiente cuadro se presentan las diferencias existentes entre los tres modelos de comunicación anteriormente vistos. En él se pueden apreciar las diferencias entre las teorías de la información (Shannon y Weaver), la teoría de la comunicación (Schram) y la teoría del proceso de comunicación (Berlo).

Características de las teorías de la comunicación y diferencias de contenido.

Modelo de Comunicación	Autor	Diferencias de contenido entre los modelos de comunicación.
Teoría de la información.	Claude E. Shannon y Warrenn Weaver.	- Este modelo está compuesto por 8 elementos, los cuales son fuente, codificador, canal, emisor, señal emitida, receptor, decodificador y destinatario. - Se explica en un esquema lineal de comunicación. - Este modelo aborda el tema de la entropía o incertidumbre informativa dentro del proceso comunicativo. - Nace con el propósito de estudiar la telecomunicación con su versión original hecha por su creador Shannon. - Posteriormente Weaver realiza aportaciones para resaltar la importancia de este modelo en el proceso de la comunicación humana.
Teoría de la comunicación.	Wilbur Schramm.	- Este modelo está compuesto por 7 elementos, de los cuales 3 son los considerados como elementos básicos que son: comunicador o emisor, mensaje perceptor o receptor, dichos elementos son influenciados por factores como el marco de referencia, los grupos de referencia, la canalización y la comunicación de retorno. - Este modelo contempla la posibilidad de que el emisor y el receptor de un mensaje sean la misma persona en el caso de la comunicación intrapersonal. - Acerca del mensaje menciona que este un momento del proceso comunicativo se convierte tan sólo en una señal que contiene signos que sólo pueden tener el significado, el denotativo y el connotativo, además del significado superficial y el latente. - Este modelo contempla dentro de sus elementos a la retroalimentación a la cual hace referencia como comunicación de retorno.
Teoría del proceso de comunicación.	David K. Berlo.	- Este modelo está compuesto por 6 elementos, los cuales son: fuente de comunicación, codificador, mensaje, canal, descifrador, perceptor de la comunicación. - Este modelo contempla la posibilidad de que la fuente y el perceptor de la comunicación sean la misma persona en el caso de la comunicación humana intrapersonal, y señala que en el caso de la comunicación más compleja estos dos elementos se separan. - Este modelo menciona la importancia del canal, resaltando que de su elección dependen factores tan importantes en el proceso comunicativo, como las cualidades y calidad de la transmisión.

2.2. Fuente

La fuente es quien abre o inicia el proceso de la comunicación. Es quien tiene la información que se quiere hacer llegar al destinatario. En muchos casos se agrupa a la fuente y al emisor en un sólo paso dentro del proceso comunicativo, pero en un análisis más profundo del mismo, la fuente y el emisor pueden no ser la misma entidad, entendiendo por esto que la fuente es la entidad primera de donde emana la información a transmitir. Es entonces en la fuente donde surge el contenido del mensaje que se desea comunicar, y es el entorno de la fuente el que dota de significado al mismo.

Dentro del proceso criptográfico, la fuente es la que envía información delicada que solamente puede ser recibida por el destinatario. Por lo que existe, por parte de la fuente, el deseo de que la información que transmite permanezca secreta. Esto se debe a que la fuente prevé algún tipo de peligro en la transmisión directa de la información o existe algún tipo de barrera que evita que la transmisión directa de información sea viable, ya sea peligro de intervención en el mensaje, algún tipo de presión social, etc.

En el ejemplo utilizado a lo largo del capítulo, la fuente sería el general del ejército rojo. De él surge la información que se desea transmitir y es él quien envía dicha información.

2.3. Codificador

El codificador es la entidad, ya sea persona, organización o aparato que convierte el mensaje en algo entendible para el receptor. Es el elemento del proceso comunicativo que realiza la acción de codificar el mensaje mediante un código previamente establecido, es decir, convierte las ideas en mensajes entendibles para su destinatario. La herramienta principal del codificador es el código que es una combinación de signos que tiene un determinado valor dentro de un sistema establecido, que permite formular y comprender un mensaje.

En la criptografía, el codificador busca que el único ente que pueda decodificar el mensaje sea el decodificador del destinatario original. Para esto, altera la forma del mensaje y lo convierte en un conjunto de símbolos diferentes a su forma original, con el objetivo de mantenerlo oculto durante su tránsito hacia el destinatario. Para cumplir su cometido, el codificador se vale de las técnicas criptográficas y, si desea que su destinatario pueda decodificar el mensaje, es necesario que tanto el codificador como el decodificador conozcan y compartan el código utilizado.

Se debe resaltar que la transformación que sufre el mensaje durante la codificación es únicamente de forma, más no de fondo. El sistema de codificación no debe alterar el contenido del mensaje original, ni permitir que durante su decodificación se altere o se pierda información del mismo. Se debe, entonces, evitar o prevenir ambigüedades en el mensaje al momento de elegir la cifra o código a emplearse.

Dentro de las técnicas criptográficas existe una diferencia entre un cifrado estándar y la utilización de un código. El cifrado o codificado estándar, puede ser un simple procedimiento de transposición de elementos, ya sean letras, números, signos, etc., o puede llevarse a cabo por la utilización de algún otro algoritmo de cifrado. A su vez, en la encriptación de un mensaje mediante la utilización de un código, el sistema se basa en que a cada palabra le corresponde siempre la misma palabra de código, es decir, este último es un diccionario fijo.

De esta forma, el código es una técnica que presenta la ventaja de la compresión de la información, siempre que las palabras de códigos usadas sean más cortas que las palabras del texto o mensaje original. Las desventajas de este sistema radican en que sólo pueden transmitirse aquellas palabras que tengan traducción asignada en el diccionario del código, el receptor debe tener el diccionario para poder decodificar; es decir, el código en su totalidad constituye la clave. Además, resulta costosa una modificación en el código. Por último, la principal debilidad en la utilización de un código como instrumento de cifrado es que el criptoanálisis se puede basar en un análisis de frecuencias, lo cual le resta seguridad al método.

Aparte de la existencia de algoritmos y códigos en los métodos criptográficos, existe otro elemento utilizado para codificar mensajes: la clave. La información secreta que adapta al algoritmo de cifrado para cada uso distinto. Las claves desempeñan un papel fundamental, sobre todo en los cifrados simétricos, en los que se utiliza la misma clave para codificar y descodificar un mensaje, ya que del secreto de dicha clave depende toda la seguridad del sistema

criptográfico. Es por esto que su longitud y renovación, así como su generación y distribución, son aspectos de suma importancia para evaluar la seguridad que el método ofrece. La longitud de la clave debe ser siempre suficiente para imposibilitar los ataques por búsqueda exhaustiva y se debe tomar en cuenta qué tiempo de vida requiere el secreto de dicha información. También, se debe determinar la vida de las claves dentro de la criptografía, especialmente en su variante simétrica, para asegurar su utilidad. Por todas estas cuestiones, existe un sistema de claves para la creación, renovación y transmisión de éstas, de manera que resulten más seguras. La gestión de las claves se basa en estructuras jerárquicas, en las que las claves de un nivel se utilizan para cifrar las claves del nivel inmediato inferior.

Algunos de los tipos de claves son:

- **Clave maestra:** La de mayor jerarquía. Se utiliza para cifrar claves primarias y secundarias, pero no para cifrar mensajes; se debe almacenar sin cifrar en un lugar seguro.
- **Clave primaria o secundaria:** Se cifra con la clave maestra y se utiliza para generar o cifrar otras claves.
- **Clave de sesión:** Es aquélla que se envía a través del canal al comenzar una comunicación. Se cifra con una clave primaria o secundaria y sólo se utiliza una vez para aumentar la seguridad del sistema criptográfico.
- **Clave de cifrado de archivos:** Es parecida a la de sesión, pero se utiliza para archivos en vez de mensajes.

En el ejemplo utilizado a lo largo del capítulo, son codificadores: el general, quien codifica el mensaje en un lenguaje común para los integrantes del ejército; el criptógrafo del general, quien se encarga de cambiar la forma del mensaje original, o texto en claro, utilizando para esto la cifra, código o clave en la que se ha convenido; y el telegrafista, quien codifica el mensaje en clave Morse. Existen, por lo tanto, en el ejemplo, tres códigos diferentes.

2.4. Emisor

El emisor es aquella persona o entidad que, ya sea de manera voluntaria o involuntaria, envía una señal o mensaje a otro actor de la comunicación, llamado receptor, esperando que lo que transmite pueda ser apreciado y comprendido. Para esto, el emisor realiza un trabajo de codificación, el cual consiste en la elección y selección de signos que le convienen para poder llevar dicho mensaje de la manera más comprensible al receptor, quien comparte el mismo código. Por ejemplo, en una conversación común entre dos personas, el emisor es la persona que inicia la conversación. Para que el mensaje enviado por el emisor sea captado y comprendido por el receptor, el emisor debe codificarlo con un código al que ambos tengan acceso. En este ejemplo, el código sería el idioma, el cual, al ser el mismo del receptor, dota de las herramientas necesarias a éste para decodificar el mensaje.

Dentro de la comunicación criptográfica el emisor es quien porta el mensaje. Y, en este tipo de comunicación, el emisor puede ser también el codificador, pero no necesariamente. Es importante recalcar que, en el caso de la

comunicación criptográfica, el emisor puede o no conocer la clave, el código y el mensaje original. Si los conoce es participante activo del proceso de comunicación, porque conoce todas las partes, y en cierto punto ocupa el papel de destinatario (se forma un ciclo comunicativo subordinado al ciclo original o general). En caso de no conocer la clave, el código y el mensaje original, sino tan sólo el mensaje cifrado, el emisor es un participante pasivo del proceso comunicativo y, hasta cierto punto, mero instrumento de la comunicación. En este caso puede llegarse a considerar como parte del canal.

En el proceso de comunicación criptográfico se puede apreciar bien la división que existe entre la fuente y el emisor, ya que en el sistema normal de comunicación, si el emisor no conoce el mensaje no es propiamente un emisor, mientras que el sistema criptográfico, el emisor es más bien un mensajero de la comunicación. Sin embargo, la línea divisoria entre emisor y canal es demasiado fina si se toma en cuenta la existencia de una fuente, separada del anterior.

En el ejemplo utilizado a lo largo del capítulo, el emisor sería el aparato telegráfico de la fuente, su operador o ambos. Su labor se limita a enviar el mensaje.

2.5. Mensaje

El proceso comunicativo solamente se da cuando existe algo que comunicar. A este algo se le conoce como mensaje. El mensaje es el contenido de la información. Es el conjunto de ideas, sentimientos u acontecimientos expresados

por la fuente para que sean captados por el destinatario de la manera en que la fuente lo desea.

El mensaje está formado por símbolos verbales que, ya sean orales o escritos y en compañía de los símbolos no verbales, representan la información que la fuente desea transmitir al destinatario. Muchas veces el mensaje emitido y el mensaje recibido no coinciden del todo, ya que durante el proceso de codificación y decodificación el significado de dicha información puede variar, dependiendo de los antecedentes y puntos de vista de la fuente y del destinatario en el momento de la comunicación y del contexto en el que se dé.

Según Berlo (1969), los mensajes son eventos de conducta que están relacionados con los estados internos de las personas, y todas las manifestaciones de comunicación que conocemos como: sonidos, escrituras, dibujos, movimientos del cuerpo, etc., son producidos por el hombre, quien realiza dicha comunicación en un esfuerzo para codificar sus ideas en una clave común y poder realizar el proceso de la comunicación con sus destinatarios.

Dentro del proceso criptográfico el mensaje tiene algunas características específicas que lo diferencian del mensaje en el proceso de comunicación normal o cotidiano. Para empezar, el mensaje, en el proceso criptográfico, es algo que se pretende que permanezca oculto durante su tránsito de la fuente al destinatario. Asimismo, en el proceso criptográfico, el mensaje sufre algún tipo de alteración física para ocultar su contenido o información original. Es importante aclarar que la

alteración física que sufre dicho mensaje es tan solo de forma y no de fondo, ya que no pretende cambiar la idea que se desea transmitir sino ocultarla. En algunas ocasiones, la forma cifrada del mensaje tiende a ser más larga que la forma original de este.

En el tránsito del mensaje, desde el emisor hasta el receptor, es cuando el mensaje sufre su mayor riesgo de seguridad dentro de la comunicación criptográfica. Dentro de la comunicación normal el mensaje tiende a ser directo. En cambio, en la comunicación criptográfica, como estrategia de ésta, el mensaje puede estar envuelto en sub-mensajes sin verdadera relevancia para la fuente o el destinatario, a manera de que si llegase a ser intervenido resultara más confuso para su interceptor, o si se llegase a robar tan sólo un fragmento de dicho mensaje se reduce la posibilidad de que la parte importante del mensaje sea interceptada. A esta técnica criptográfica se le conoce como estenografía.

Un ejemplo de esta técnica es el envío de un mensaje que ya tiene una transformación criptográfica, es decir, que ya ha sido oculto, mediante el cifrado, en un pergamino sobre el cual se hace una pintura para ocultar la información cifrada y confundir al interceptor. La principal característica del mensaje dentro del proceso criptográfico es que éste, en sí, contiene información delicada que por razones de seguridad no debe ser intervenida.

En el ejemplo utilizado durante este capítulo, el mensaje original o texto en claro sería: “Mover artillería al norte” y el mensaje cifrado sería: “MPXHV-

ASVLQRLZRK-AM-NPTXJ”. Es notable la dualidad del mensaje en la comunicación criptográfica; existe, por una parte, el mensaje que se desea transmitir, el texto en claro, y por otra el mensaje que realmente se transmite, es decir, el texto cifrado.

2.6. Canal

Para que el mensaje pueda ser transmitido necesita de un medio donde transitar; a este medio se le conoce como canal. El canal es el medio físico a través del cual se transmiten los mensajes y establece una conexión entre emisor y receptor, dando lugar al proceso de comunicación. Este canal es el soporte material por el cual circula el mensaje emitido. Por ejemplo, en el caso de la voz, el aire es el que funge como canal para ésta, al transmitir las vibraciones elásticas entre emisor y receptor.

La palabra “canal”, utilizada en las teorías de la comunicación, engloba tres significados, o se utiliza para referirse a tres aspectos del proceso comunicativo. Éstas son: las formas para codificar o decodificar los mensajes, los vehículos de mensajes y los medios de transporte, que en su conjunto conforman los canales de la comunicación. En el caso de la comunicación oral, por ejemplo, los canales para codificar o decodificar los mensajes serían el mecanismo verbal y el mecanismo auditivo, el vehículo de los mensajes serían las ondas sonoras emitidas por la voz, y el medio de transporte para estas ondas sonoras sería el aire.

El canal juega un papel determinante dentro del proceso de comunicación criptográfico, ya que para que se dé la necesidad de la criptografía, el canal debe tener riesgo de ser intervenido. Si no es así, el uso de la criptografía resulta incongruente. El deseo de evitar ese riesgo es el motor que impulsa el desarrollo de las técnicas criptográficas, tratando de superar su principal reto: el de proporcionar seguridad en la transmisión de mensajes a través de canales inseguros o susceptibles a intervención. Ahora bien, dentro de la comunicación criptográfica, el canal puede tener varias formas. Desde una persona hasta un aparato transmisor de señales, la forma que toma el canal es la principal diferencia entre la criptografía clásica y la criptografía moderna. En el ejemplo utilizado durante este capítulo, el canal sería el telégrafo.

2.7. Contexto

El contexto de un mensaje son las circunstancias que rodean un hecho de comunicación. Este elemento es un factor que influye en el proceso de comunicación, ya que contribuye al significado del mensaje. Por ejemplo, un semáforo en medio de una iglesia no emite ningún mensaje porque le falta contexto. Por esto, se debe tomar en cuenta el contexto situacional de un mensaje como un elemento necesario para su adecuada decodificación.

Dentro del proceso criptográfico, el contexto es el que da la pauta a la necesidad de ocupar un sistema criptográfico para transmitir una información. En un contexto “normal” la transmisión de los mensajes puede llevarse a cabo sin la

necesidad de la criptografía, ya que el contexto es favorable y está desprovisto de riesgos para una comunicación segura. Sin embargo, en el proceso de comunicación criptográfica, el contexto tiende a ser de tensión, ya que la naturaleza de los mensajes que se transmiten mediante estas técnicas puede otorgar herramientas a personas ajenas al mensaje para perjudicar o tomar ventaja sobre quienes emiten o reciben dicha información.

Por lo anterior, se puede afirmar que el contexto dentro del proceso criptográfico tiende a ser de importancia informativa, presenta algún grado de peligro de intercepción y hay inseguridad durante la transmisión de los mensajes. En general, el contexto que envuelve un proceso criptográfico se presenta en momentos bélicos, en transmisiones de información de orden jerárquico importante, en transacciones financieras, etc. Aunque la criptografía ha abarcado tantas ramas de utilidad que, en la actualidad, la única constante indispensable dentro del contexto de un proceso comunicativo criptográfico es la necesidad de intimidad y seguridad de la información. Esto puede ocurrir tanto en un mensaje entre políticos o un simple envío de correo electrónico entre dos amantes.

En el ejemplo presentado a lo largo de este capítulo, el contexto sería la batalla. Dentro del mismo, la necesidad de transmitir información de manera segura entre los integrantes de un ejército hace necesaria la utilización de algún sistema criptográfico.

2.8. Ruido

Se le conoce como ruido a cualquier perturbación experimentada por la señal en el proceso de comunicación. Esta perturbación es cualquier factor que dificulte el traspaso de información de manera intacta y que pueda proporcionar una pérdida de información. Durante la transmisión, el ruido puede darse en cualquiera de los elementos del proceso comunicativo.

El ruido puede presentarse en varias formas. En general cualquier cosa que interrumpa parcial o totalmente la transmisión de una información puede considerarse como ruido dentro del proceso comunicativo. Por ejemplo, las distorsiones del sonido en una conversación, ya sea en persona, o por radio, televisión o teléfono son ruido, pero también son ruido factores como la distorsión de las imágenes, la sordera de un oyente, la afonía de un hablante, y hasta la mala ortografía, ya que pueden restarle claridad a la transmisión de un mensaje.

Para evitar que exista alguna pérdida de información relevante durante la comunicación, en muchos casos, se utiliza la redundancia como recurso comunicativo, de tal manera que las partes de la información transmitida que poseen un mayor grado de importancia dentro del mensaje son repetidas de diversas formas. De esta manera, se envía más información al receptor; si se pierde parte de la información o existe ruido en alguna parte del mensaje existe mayor probabilidad de que la información relevante haya llegado a su destino.

Dentro del proceso criptográfico puede considerársele al ruido como la intercepción, interrupción o alteración del mensaje secreto durante su tránsito. En

general, el ruido es provocado en el proceso criptográfico por el interceptor, que desea conocer el contenido de un mensaje del cual no es el destinatario original. Este ruido puede llegar a ser la simple intercepción de los mensajes, hasta la interrupción de su tránsito, el descubrimiento del mensaje original o la alteración de este como una estrategia para confundir al destinatario original.

Otra forma de ruido es la provocada por el llamado criptoanálisis, es decir, el conjunto de técnicas destinadas a descifrar el contenido de un mensaje cifrado en ausencia de la clave para hacerlo. Este tipo de técnicas son utilizadas principalmente por un interceptor para tratar de descubrir el mensaje original; aunque es también utilizada por los historiadores para descubrir diversos mensajes encriptados por culturas antiguas.

Esto lleva a una división de los tipos de ataques o amenazas (ruidos) que puede sufrir un mensaje secreto: la pasiva, por ejemplo, su robo, el acceso no autorizado o su intercepción; y la activa, que radica en alguna modificación al mensaje, la interrupción de la transmisión o la falsificación del mensaje. En el caso del acceso no autorizado o la intercepción del mensaje secreto peligra la confidencialidad de la información, mientras que en caso de modificación y falsificación lo que se pone en peligro es tanto la integridad como la autenticidad de los mensajes.

Para llevar a cabo un estudio profundo de los sistemas criptográficos, es necesario conocer al enemigo, su situación y el tipo de ataque que utiliza, existen diferentes tipos de ataques, según explica Fuster (2001:10):

1. Ataque sólo con texto cifrado. Esta situación se presenta cuando el criptoanalista sólo conoce el criptograma, lo que dificulta en gran medida la posibilidad de descifrar el texto original.
2. Ataque con texto original conocido. Se da cuando el criptoanalista tiene una correspondencia de texto original y de texto cifrado, por ejemplo si se tiene conocimiento del tema del que trata el texto cifrado, de esta manera se utiliza la correspondencia entre las palabras más habituales utilizadas en dicho tema y los textos cifrados más repetidos.
3. Ataque con texto original escogido. Esta se da cuando el criptoanalista puede obtener el cifrado de cualquier texto que éste escoja, además del criptograma que trata de descifrar.
4. Ataque con texto cifrado escogido. Este se da cuando el enemigo o criptoanalista intruso es capaz de obtener el texto original de determinados textos cifrados de su elección, lo que le sirve para establecer una pauta.

En el ejemplo utilizado a través de este capítulo, el ruido sería la intercepción del mensaje por parte de los soldados del ejército azul.

2.9. Receptor

El receptor es la persona que recibe el mensaje y complementa el trabajo del emisor en el proceso comunicativo. Para que el receptor sea capaz de decodificar el mensaje recibido es necesario que el mismo se encuentre en un código

conocido por él. De este modo se asegura de poder interpretar el significado real del mensaje. Este proceso de interpretación es mucho más fácil si además de conocer el código del mensaje se conoce también el contexto situacional en el que fue elaborado por el emisor.

Existen dos tipos básicos de receptor:

- Receptor pasivo: Es el que se limita a recibir el mensaje.

- Receptor activo o preceptor: Es aquél que no sólo recibe el mensaje sino que lo percibe y lo almacena. En este caso, el mensaje es recibido tal como el emisor quiso decir y esto provoca lo que comúnmente se le conoce como retroalimentación, que es un paso que no siempre se da en un proceso comunicativo y que le da continuidad al mismo.

Dentro del proceso criptográfico, el receptor puede también ser el decodificador, pero no necesariamente. Por lo regular, en el proceso de comunicación criptográfica, el receptor suele ser más bien una parte del canal por el cual viaje el mensaje secreto, y la labor de decodificar el mensaje para que éste llegue en su forma original al destinatario final suele ser tarea del decodificador y no del receptor. Dentro de los sistemas de comunicación criptográficos, el receptor es más bien un mensajero de la información en su forma cifrada, puede ser una persona como sería el caso de la criptografía antigua, o en los métodos de criptografía actual o más avanzada, una máquina receptora de señales.

En el ejemplo utilizado en este capítulo, el receptor sería el aparato telegráfico del destinatario, el operador telegráfico o ambos.

2.10. Decodificador

El decodificador es la entidad, ya sea persona, organización o aparato, que convierte los datos codificados por una fuente en información entendible para el destinatario. Es el elemento del proceso comunicativo que realiza la acción de decodificar el mensaje mediante un código previamente establecido, entre este y el codificador. El proceso de decodificación “se trata de un proceso dinámico activo y complejo que comporta una rica actividad consciente, atención y esfuerzo para recaudar todos los datos necesarios para la comprensión de lo expresado” (Ricci, 1983: 38). El proceso que realiza el decodificador de un mensaje es la reconstrucción del mismo, esto es, rescatar el significado que se pretendía desde la fuente. Esta decodificación se basa en el conocimiento que el decodificador tenga del código utilizado por el codificador en el mensaje.

Dentro del proceso de comunicación criptográfica, el decodificador es parte fundamental para que la información secreta llegue al destinatario original en una forma que sea entendible para éste. El decodificador es, por lo tanto, el encargado de revelar el secreto del mensaje encriptado. Es, además, la entidad, persona o aparato que se supone debe hacerlo, ya que en caso de intercepción del mensaje secreto, el criptoanalista interceptor juega hasta cierto punto el papel de decodificador del mensaje, a pesar de que éste no le haya sido conferido por la fuente.

En el ejemplo utilizado en este capítulo, el decodificador sería el criptógrafo del coronel.

2.11. Destinatario

El destinatario es, como su nombre lo indica, el destino final de la información enviada por la fuente; una vez que éste recibe la información enviada por la fuente e interpreta lo que ésta quiere darle a conocer, el acto de comunicar carece de sentido si no hay alguien que reciba el mensaje enviado: si se carece de destinatario no existe comunicación. El destinatario es quien cierra el proceso de comunicación y puede agregarle a éste el paso de la retroalimentación si lo considera necesario.

En muchos casos, se agrupa al destinatario y al receptor en un solo paso dentro del proceso comunicativo, pero dentro de la comunicación criptográfica es muy común que estos no sean la misma entidad, entendiendo por esto que el destinatario es la entidad última a donde debe llegar la información transmitida y la interpretación de dicho mensaje se ve en gran medida afectada por el contexto del destinatario. Dentro del proceso criptográfico, el destinatario es a quien la fuente le envía información de carácter delicado que solamente puede ser recibida por él. Por lo regular, contiene datos de suma importancia, por lo que existe, por parte de éste, el deseo de que la información que se le transmite permanezca secreta.

En el ejemplo utilizado a lo largo de este capítulo, el destinatario sería el coronel en el frente de batalla. Es a él a quien le fue enviada la información.

2.12. Retroalimentación

La retroalimentación tiene lugar en un proceso comunicativo cuando el receptor ha reconocido el mensaje y desea responder al emisor. Esta retroalimentación completa el círculo de la comunicación, ya que existe un continuo flujo de los mensajes. La retroalimentación (o la falta de ésta) puede servir par corroborar que el proceso comunicativo se haya dado de manera exitosa, ya que si no se da la retroalimentación en el proceso de comunicación puede ser por diversos factores. Entre éstos destacan que el mensaje no haya sido recibido, no haya sido comprendido o en su defecto que el receptor no quiera responder a dicho mensaje o no tenga que hacerlo. Para verificar que el proceso de comunicación se haya llevado a cabo, aun cuando exista la ausencia de la retroalimentación, el emisor debe indagar el por qué de la falta de retroalimentación para actuar en consecuencia.

Existen dos tipos de retroalimentación:

- Retroalimentación positiva: Sucede cuando se fomenta la comunicación.
- Retroalimentación negativa: Se da cuando se busca cambiar el tema o terminar la comunicación.

Por ejemplo, en una conversación, cuando el receptor continúa la plática existe una retroalimentación. Algunas características de la retroalimentación es que ésta debe ser de utilidad para enriquecer la información del emisor, debe ser descriptiva para que exista eficacia en el proceso de intercambio de mensajes,

debe ser específica indicando de esta manera la comprensión del mensaje previamente recibido y debe ser oportuna, de manera que sea emitida en el momento y en el contexto oportuno para evitar confusiones.

En el ejemplo utilizado a lo largo de este capítulo, la retroalimentación sería el mensaje en respuesta enviado por el coronel para el general.

CAPÍTULO 3. APLICACIONES DE LA CRIPTOGRAFÍA: UNA TÉCNICA PARA EL PRESENTE Y EL FUTURO

3.1. Principales funciones de la criptografía

En la actualidad, los propósitos de la criptografía exceden el establecimiento de comunicaciones secretas sobre canales inseguros o la conservación de la confidencialidad de la información, a pesar de ser este el motivo de su origen y por muchos años la única rama de aplicación utilizada por los usuarios de la técnica criptográfica.

Actualmente, la criptografía moderna tiene un gran campo de aplicación en la sociedad. Cada día existen nuevos avances tecnológicos que, además de proporcionarle varios beneficios a las sociedades, a la par de éstos menguan la posibilidad de la privacidad y facilitan los procesos de alteración en las transmisiones de información o procesos comunicativos. Esta problemática ha dado pie a que existan grandes avances en las técnicas criptográficas que, a su vez, resuelvan los problemas de dichos procesos comunicativos. Entre estos problemas se encuentran la autenticación de la información, que puede ser considerada como la segunda utilidad principal de la criptografía; así como también la identificación de los usuarios de dicha información y la utilización, características y beneficios de las firmas digitales.

3.1.1. Autenticación

El propósito de un sistema criptográfico de autenticación es el de asegurar que la información transmitida en un proceso comunicativo es legítima. Dentro de los procesos comunicativos criptográficos, el ruido provocado por los interceptores puede clasificarlos en criptoanálistas pasivos los cuales limitan su participación a la intercepción y conocimiento de la información transmitida por canales inseguros, y criptoanalistas activos que son los que intentan integrar información al mensaje original o modificarlo en su totalidad, haciendo creer al destinatario que son la fuente original de dicho mensaje. Por esto, el propósito de un sistema de autenticación se refiere a la detección de la presencia de un criptoanalista activo.

> *Siempre que un receptor B reciba un mensaje que parezca provenir del emisor A, el esquema debe permitirle averiguar no sólo si el mensaje viene de A, sino si fue modificado por el camino. Se supone que este tipo de intruso tiene acceso a la escucha de cuantos mensajes quiera y que su meta es conseguir que un mensaje falsificado no sea detectado por el receptor.* (Fuster *et al*., 2001:85-86).

Un sistema criptográfico proporciona secreto si determina quién es el receptor legítimo de un mensaje. Proporciona, además, autenticidad, toda vez que determine quién es el emisor real del mensaje y brinda integridad al proceso comunicativo, si determina con la mayor exactitud posible el contenido original y real del mensaje transmitido. Existen varias ocasiones en que el proceso comunicativo requiere como medida de seguridad durante la transmisión de alguna información, que el destinatario pueda confiar en el contenido del mensaje y en que éste no ha sido alterado y que la fuente sea quien dice ser, brindando autenticidad al mensaje y al origen del mismo; inclusive cuando existe algún tipo

de ruido en el canal, siempre y cuando los niveles de ruido no sean muy altos, y es en estas ocasiones cuando la autenticidad tiene su máxima utilidad.

3.1.2. Firma digital

Una de las principales necesidades comunicativas de la actualidad, como resultado del acelerado desarrollo de las telecomunicaciones, es el de la firma de documentos o mensajes transmitidos a través de los ordenadores y sus redes de información. De esta forma se planean en la vida cotidiana situaciones en que la firma digital sustituye a la firma manual y, por consiguiente, adquiere las mismas propiedades que esta. Una vez firmado un documento la firma identifica y compromete al firmante. La principal diferencia que existe entre una firma autógrafa y una firma digital radica en que la primera es el resultado de un proceso físico considerado intrínseco a la persona que firma.

En este aspecto radica su nivel de seguridad, ya que aunque no todas las firmas de una misma persona son exactamente iguales, existen grafólogos que pueden llegar a reconocer y determinar si una firma manual es auténtica o se trata de una falsificación. En cambio una firma digital es producida por una máquina y el firmante sólo aporta la entrada al proceso de creación. La firma digital está formada por un conjunto específico de *bits* que se utilizan para firmar un determinado documento. El objetivo del sistema de seguridad de la firma digital es que ningún otro usuario pueda producir el mismo conjunto de *bits*, lo que

significa que nadie debe ser capaz de conseguir la entrada secreta del firmante legítimo.

Otra diferencia importante es que la firma manual de una persona es la misma para todos los documentos del firmante. La seguridad de este sistema manual radica en la dificultad para recrear falsificaciones indetectables. En cambio, la firma digital debe ser diferente para cada documento avalado por el firmante, ya que al ser un conjunto de *bits*, si este conjunto fuera siempre el mismo, sería muy fácil para un impostor averiguarlo y falsificarlo. Es por esto que dentro del sistema de la firma digital cada firma es diferente y está formada por conjuntos distintos de *bits*, correspondientes a un mensaje o documento en particular y, de esta forma, garantiza que ese mensaje en concreto fue firmado y previene la sustitución de dicho mensaje.

Para cumplir con su función y ser una versión computarizada de la firma manual, la firma digital debe de cumplir con algunos requisitos como son: el no ser falsificable, ya que el intento de falsificación debe llevar asociada la resolución de un problema matemático intratable; debe ser fácil de autenticar, siendo posible para cualquier receptor su autenticación después de mucho tiempo; debe ser irrevocable, a manera de que el autor de dicha firma no pueda negarla y al ser realizada con un medio tecnológico debe de procurarse que esta sea fácil y barata de generar. Otra de las características principales de la firmas digitales es que para evitar fraudes y modificaciones del mensaje por parte del receptor al

conservar una firma no propia, éstas deben depender tanto del mensaje como del autor.

> *Si el emisor A envía un mensaje firmado digitalmente al receptor B, este último no sólo debe convencerse de que el mensaje fue firmado por el primero, sino que, además debe ser capaz de demostrar a un juez que A realmente firmó ese mensaje. La firma digital y el correo electrónico ofrecen conjuntamente sustanciosas ventajes, una de ellas es hacer posible el correo electrónico certificado y la firma de contratos.* (Fuster *et al*., 2001:92-93).

El proceso de la firma digital debe transformar al mensaje en un conjunto de información, de tal manera que la firma sólo pueda ser calculada por la fuente. Para esto, el proceso de transformación de la firma digital debe de utilizar algún tipo de información que posea únicamente el emisor. Esta información secreta será entonces la que fungirá como la clave en el proceso criptográfico de la firma digital, y será a su vez prueba de la identidad del firmante; además, de esta manera, establecerá el origen del mensaje o la fuente del mismo.

Existen dos tipos de esquemas de utilización en los sistemas de las firmas digitales: los esquemas no arbitrarios, en los que los mensajes firmados son enviados directamente del firmante al receptor, y este último verifica su validez, por lo cual, no existe la necesidad de remitir la firma a una tercera parte; así como los esquemas arbitrarios, en los que los mensajes firmados sólo pueden enviarse a través de una tercera parte de confianza, que se le conoce como árbitro. Este tipo de esquema en la firma digital se da cuando el receptor es incapaz de verificar la firma del emisor directamente, y el árbitro asegura la validez de dicha firma. En este esquema, ambas partes deben tener plena confianza en la tercera parte o árbitro para su labor de autenticación y la resolución de las posibles disputas, lo

que garantiza al emisor que su firma no será falsificada y al receptor que las firmas que recibe son realmente válidas.

3.1.3. Identificación del usuario

La identificación del usuario es un sistema de autenticación particular que se emplea para evitar la utilización de identidades falsas. Los métodos de identificación pueden arrojar dos posibles resultados, ya sea la aceptación o el rechazo de la identidad del usuario. Estos son procesos que se llevan a cabo en tiempo real, por lo que es necesaria la eficiencia tanto computacional como de las comunicaciones utilizadas durante el proceso de autenticación para agilizar los tiempos.

Otra característica con la que algunos de los sistemas de autenticación cuentan es la reciprocidad, es decir, que usuario y sistema puedan identificarse mutuamente. Aunque la mayoría de los métodos funcionan en la actualidad de una manera unilateral, en un futuro la reciprocidad en los sistemas criptográficos de identificación del usuario será altamente valorada para evitar posibles fraudes. Las técnicas de identificación deben poseer la capacidad de defender a sus usuarios de diferentes ataques a su identidad. El más común y simple de estos ataques es el de la suplantación, aunque existen algunos más sofisticados, como lo son la reproducción de identificaciones previas válidas, o la construcción de identificaciones previas, entre otros.

Por medio de las identificaciones periódicas se puede evitar también el riesgo de secuestro de sesiones, que se da cuando el usuario ya ha sido identificado, y el adversario aprovecha el momento en que el usuario baja la guardia y se apropia de la línea de las comunicaciones durante el proceso de transmisión de la información, interviniéndola y obteniendo los datos que se transmiten por el canal de información. Los modelos de identificación del usuario existentes responden, por lo regular, a dos fases básicas, una primera denominada fase de demostración, que es en la que el usuario entrega, muestra o usa alguna información en un proceso de comunicación con el sistema, y la segunda conocida como fase de verificación, que es en la que el sistema comprueba los datos recibidos.

Dependiendo de las características de la información que utiliza un usuario para su identificación, se puede hacer una clasificación de los esquemas en:

A) Los basados en “algo que se sabe”
B) Los basados en “algo que se tiene”
C) Los basados en “algo que se es”

En el primer caso, el esquema basado en “algo que se sabe”, es el más habitual, y emplea el *password* o contraseña. Este método se basa en que el usuario y el sistema comparten cierta información confidencial, por lo que el último puede comprobar la identidad del primero simplemente requiriéndole dicha información. La seguridad de este esquema depende completamente de la

habilidad para mantener en secreto las contraseñas, por lo que resulta el esquema de identificación más débil de todos.

En el caso de los esquemas basados en algo que se tiene, los usuarios utilizan terminales inteligentes o bien tarjetas inteligentes, con estos medios se puede resolver el problema de la identificación de usuario utilizando clave secreta, clave pública o demostraciones de conocimiento nulo. En el caso de la clave secreta compartida, el sistema lanza un reto y el usuario responde cifrándolo con la clave secreta dispuesta. En el caso de claves públicas, el funcionamiento se da de tal manera que cada usuario escoge una clave secreta aleatoria y la usa para generar la correspondiente clave pública, y revela la clave de cifrado al sistema y programa el algoritmo de descifrado en su terminal. En el caso de los esquemas basados en algo que se es, son los que se basan en características del individuo como huellas, retinas, etc. Estos son los esquemas más avanzados de identificación y, sin duda alguna, serán el futuro de las técnicas de identificación de usuarios en todo el mundo, ya que brindan una gran precisión.

3.2. La utilidad de la criptografía en la vida diaria

En la actualidad, la sociedad moderna tiene su principal soporte en las comunicaciones y las tecnologías de la información, las cuales aportan beneficios al ámbito social, así como al cultural, el económico y el político. Si se consideran dichos beneficios, se puede ver la inminente necesidad de que esta sociedad moderna cuente con el soporte de una estructura segura de tecnología y

comunicaciones que avale la confianza que los miembros de dicha sociedad depositan a diario en actos tales como las comunicaciones móviles que tiene su mayor expresión en los teléfonos celulares, las compras por Internet que cada día incrementan su popularidad y que son una gran fuente de actividad económica de los países desarrollados y cada vez más en los países en vías de desarrollo, los envíos de correo electrónico, etc.

Sin embargo, estas tecnologías y la capacidad que representan para el almacenamiento, distribución y proporción de datos relativos a las personas, invaden o amenazan en cierto grado la esfera privada, por lo que existen ya un gran número de leyes de protección de datos y derecho a la intimidad. Los ciudadanos perciben como la mayor amenaza a su intimidad al Estado, a pesar de los abusos que cometen contra ella el sector privado, y es precisamente esta contradictoria percepción del gobierno como amenaza y garante de los derechos de los ciudadanos, la que ha llevado a considerar la necesidad del uso de las técnicas criptográficas en una escala mucho mayor que la actual.

3.2.1. Medicina y criptografía

Actualmente un médico puede dar un diagnóstico vía correo electrónico, realizar intercambios de imágenes de casos especiales con otros médicos por medio de Internet, saber con exactitud cuándo fue la última vez que su paciente lo visitó, o conocer su padecimiento. Además de reconocer al paciente que le llama de emergencia en la madrugada y tener a su alcance el estudio clínico, lo único que

se requiere para realizar todo esto es una computadora, una impresora y un *software* especializado. Por lo anterior, se puede observar claramente la importancia que tiene el salvaguardar y asegurar la confidencialidad de la información de cada paciente. Es decir que toda esa información que viaja por Internet o Intranet utilizando *http,* debe ser totalmente segura y confidencial. Por ejemplo, en el caso de un paciente con VIH, si su historial médico fuera expuesto a personas que él no desea, las consecuencias podrían ser graves para esta persona, ya que podría ser víctima de discriminación o rechazo entre otras razones; en casos como este la confidencialidad es de suma importancia, por lo tanto, en la medicina se utilizan medidas de seguridad en el almacenamiento de información, para lo cual se recurre a la encripción de datos de tal manera que la información queda encapsulada y permite tanto a médicos como a pacientes tener la plena confianza de que esta no podrá ser descifrada en el trayecto a su destino, ya que los *softwares* que se utilizan proveen al usuario de conexiones remotas seguras por medio de claves, que son cambiadas aleatoriamente por su seguridad, y si una de estas claves llega a ser interceptada no existe el riesgo de que la información se divulgue.

El uso de la criptografía en el ámbito de la medicina presenta varias ventajas, gracias a la seguridad que esta provee, los médicos pueden manejar y almacenar su información de manera segura, intercambiar experiencias y conocimientos con otros médicos en cualquier parte del mundo y, de esta manera, disminuir enormemente los costos de llamadas telefónicas o viajes inesperados, entre otros aspectos.

3.2.2. Empresa y criptografía

Es común que hoy en día las empresas manejen grandes cantidades de información de diferentes jerarquías. Es por esto que sobre todo en las grandes empresas transnacionales y cada vez más en las empresas de menor tamaño, existan redes computacionales que ya sea de manera interna o externa, mantengan en comunicación a las organizaciones. Estas redes procesan y transmiten diariamente miles de datos archivados. Una de las principales herramientas para este procesamiento y almacenamiento de información son los sistemas operativos especializados como, por ejemplo, lo es el mundialmente utilizado *Windows* que desde su versión *Windows 2000* tiene integradas algunas opciones de seguridad. La intención es que cada usuario pueda entender y controlar cómo funcionan estas opciones, ya que operan en tres niveles:

1.- **Local**. La protección local se realiza a través de un sistema de encriptación de archivos que funcionan en unidades *NTFS* (Sistema de archivo de NT), este sistema está diseñado para evitar que usuarios no autorizados se salten el sistema de arranque y, por lo tanto, también las funciones de seguridad. La encriptación de los datos *NTFS* es un servicio que se basa en la arquitectura de *CriptoAPI* de *Windows* para implementar el sistema de claves públicas. Cada archivo (incluyendo sus temporales de trabajo) se encriptan a través de una clave generada aleatoriamente, asimilando algoritmos asimétricos *DES*. Este proceso es transparente, ya que *EFS* encripta y desencripta los archivos localizando las

claves del usuario, ya sea desde el almacén de claves del sistema o desde dispositivos de seguridad como las *Smart Cards*.

2.- **Corporativo**. Es la protección de datos en una LAN (Red de Área Local), ya que *Windows 2000* utiliza el protocolo *Kerberos* versión 5, un estándar de seguridad en redes LAN e intranets que verifica y hace un seguimiento de la actividad de cada usuario dentro de la red. Kerberos permite un control de acceso unificado a casi cualquier entorno en red eliminando la necesidad de obtener permisos y esperar respuesta cada vez que un usuario desea acceder a un nuevo recurso de la red.

3.- **Público**. Es la protección de conexiones Internet. *Windows 2000* utiliza también sistemas de claves públicas y protocolos de autenticidad para mantener la seguridad que se manejan por Internet, de manera que verifique la procedencia de mensajes de correo o garantice las fuentes de donde proceden aplicaciones y controladores; por otra parte, incluye redes privadas virtuales.

3.2.3. Correo electrónico y criptografía

El correo vuelve a ser el medio más fácil, rápido y económico que las personas tienen para comunicarse, sólo que en la actualidad, en vez de utilizar el papel como medio para transmitir ideas, pensamientos, requerimientos o información, ha cambiado la escritura tradicional por la escritura electrónica a través de Internet. El correo electrónico como “nuevo” medio de comunicación ofrece varias ventajas, por lo que puede llegar a ser considerado como el medio “ideal”; y esto es gracias

a la aportación que le da la criptografía logrando que además de ser un medio rápido y económico sea un medio seguro.

Como ya se comentó, la principal ventaja que ofrece el correo electrónico es la rapidez, por lo que no hay que esperar ni adelantar días para que la información importante llegue a tiempo a su destino; por otro lado, está la eficacia, ya que se puede escribir y enviar información desde un mismo sitio sin tener que trasladarse. Con la ventaja de que las pantallas de los *softwares* para correo electrónico son relativamente sencillos y existen diversos programas cuya utilidad es únicamente el envío y recepción de mensajes. Es en este punto donde la criptografía juega un gran papel en la diaria utilización del correo electrónico, ya que estos *softwares* especializados para correo, cuentan en su mayoría con sistemas de encripción tanto para los datos e información que viajan por la red, como para la identificación de los usuarios del correo.

Otro servicio valioso para aquellas personas cuya recepción de mensajes sea muy alta, se pueden crear filtros que automáticamente ordenan los mensajes dependiendo de algunas variables, como fecha, remitente, asunto, prioridad, etc., lo cual permite revisar el correo en orden de importancia, así como desechar toda la propaganda sin siquiera abrirla.

Cabe señalar que este medio de comunicación también tiene ciertas desventajas, como son la capacidad de almacenamiento y recepción de datos, ya que algunos administradores de correos electrónicos tienen definido un tamaño específico para los usuarios, de tal manera que no pueden recibir mensajes muy

grandes o bien no pueden recibir más información si su buzón ya está lleno. Por otra parte, están todos aquellos virus y gusanos que se envían por correo y que llegan a infectar gran número de computadoras en cuestión de minutos.

En realidad se trata de un medio bastante beneficioso, pero que puede llegar a ser perjudicial, si no se tiene cuidado en lo que se envía, cómo se envía, lo que se recibe y, por supuesto, lo que se abre.

La mayoría de los profesionistas y la gente, en general, cuenta hoy en día con un correo electrónico, así que cada vez que se utiliza la dirección electrónica y se agrega la contraseña, se está haciendo uso de la criptografía, ya que sólo contando con la clave personal o clave secreta, en este caso conocida como contraseña, se puede acceder a datos e información personal, que se encuentra resguardada por este sencillo pero efectivo sistema de claves, e incluso las personas se enfrentan diariamente a los criptoanalistas cibernéticos mejor conocidos como *hackers*.

Por lo tanto, es importante saber que si se está manejando información sensible, se deben tomar medidas de precaución como: contar con encriptación, manejo de claves públicas y privadas, mandar archivos compactados con clave o cualquier otra medida de seguridad que permita utilizar el correo electrónico de manera segura.

CAPÍTULO 4. CONCLUSIONES

El presente trabajo de investigación ha demostrado que la criptografía es una ciencia aplicada que compete a las ciencias de la comunicación ya que puede y debe analizarse no solo desde un punto de vista tecnológico, informático o matemático, sino también y con gran relevancia desde un punto de vista meramente comunicativo, que señale, explique y analice los elementos que intervienen con el uso de las técnicas criptográficas dentro del proceso comunicativo.

Con respecto al objetivo general planteado durante el trabajo de investigación éste se logró en su totalidad, ya que se ha podido elaborar un material comunicativo, que servirá como apoyo teórico para los interesados en el tema de estudio, brindando una explicación acerca de qué es la criptografía, además de que proporciona al lector un marco teórico acerca de esta disciplina, además se le analiza como proceso comunicativo, mencionando sus usos en el presente y sus proyecciones a futuro. En cuanto a los objetivos específicos del proyecto, estos también se cumplieron en su totalidad, dando como resultado un trabajo de investigación, ya que se ha definido y explicado qué es la criptografía, cuáles son el conjunto de técnicas que utiliza y en qué consiste cada una de ellas, además se ha dotado al lector de un breve glosario que comprende los conceptos básicos utilizados dentro del *argot* de esta disciplina.

Se describió el marco teórico de la criptografía a fin de que el lector tenga un mejor conocimiento de esta ciencia aplicada y se hizo un breve recorrido histórico de su evolución, desde las técnicas más primitivas hasta las actuales; también se expuso cómo, desde entonces hasta ahora, la criptografía ha sido de gran utilidad para la humanidad y de gran importancia en las decisiones que han cambiado el rumbo de la historia.

Igualmente se analizó a la criptografía como proceso de comunicación, para lo cual se tomaron en cuenta diversas perspectivas teóricas que autores como Shannon, Schramm, Berlo, Pino, Fuster y Escarpit, entre otros, abordan en sus obras y tratados acerca de la comunicación.

Se describió lo que es la criptografía hoy en día: cuáles son algunas de las ramas en las que se emplea con mayor frecuencia, así como las nuevas técnicas que se utilizan en este ámbito y las proyecciones que tendrá a futuro.

Además, se explicó el conjunto de técnicas y conceptos que se emplean en esta disciplina, tales como la criptología que es en realidad una ciencia más completa que comprende tanto las técnicas utilizadas por la criptografía para cifrar los mensajes secretos, como al criptoanálisis que es el conjunto de técnicas que se utilizan para romper los textos cifrados y poder leer la información original de estos cuando no se tiene al alcance la clave de cifrado, y descifrar los mensajes que han sido ocultos por medio de la criptografía.

Así mismo, se logró adentrar al lector en diversos conceptos relacionados con el tema como lo es el de los criptosistemas, la estenografía, los códigos, la claves, entre otros. Se mencionaron también las diferentes técnicas criptográficas que existen; su división y las diferencias que existen entre ellas, como son: la criptografía simétrica, la criptografía asimétrica y la criptografía híbrida; se llegó a la conclusión de que las técnicas criptográficas que existen, presentan diversos grados de dificultad, por lo que pueden adecuarse tanto a información de suma importancia en niveles jerárquicos muy altos, hasta información de carácter personal en la que el individuo tan sólo desea cierto grado de confidencialidad.

Se realizó también un breve resumen cronológico del desarrollo de la criptografía en la historia de la humanidad, dividiéndola en tres grandes etapas: la primera denominada criptografía antigua, que abarca el periodo que comprende desde los egipcios y su utilización de jeroglíficos, los babilónicos; quienes utilizaban escritura cuneiforme. Más adelante el método de la escítala, el conocido como “método César”, ya que, supuestamente, Julio César lo utilizó en sus campañas. Además de los avances que se dieron durante los siglos XVII, XVIII y XIX, con los sistemas criptográficos utilizados por Felipe II e Isabel I.

A la segunda etapa histórica se la ha denominado criptografía moderna y abarca principalmente el periodo comprendido durante las dos guerras mundiales, con los inventos como la máquina *Enigma* y la revolucionaria invención del primer diseño lógico de un cifrador, realizado por la NBS (Oficina Nacional de Estándares, por sus siglas en inglés, actualmente conocida como Instituto

Nacional de Estándares y Tecnología), que produjo aquél que fuera el principal sistema criptográfico de finales de siglo: el conocido como Estándar de Encriptado de Datos o DES.

A la tercera etapa se le conoce como criptografía contemporánea, en la que las tecnologías de la comunicación juegan un papel de suma importancia, puesto que se ha visto impulsada por inventos tales como el de la Internet pero, a la vez, se ve perjudicada, ya que aumenta considerablemente el riesgo de intercepción y desciframiento de los mensajes secretos por parte de intrusos. Por este motivo, ha sido necesario avanzar aún más en las técnicas criptográficas actuales y se ha logrado lo que podría definirse como el inicio de una nueva faceta criptográfica: la criptografía cuántica que utiliza para su funcionamiento el uso de fotones, y que permitirá, entre otras cosas, que en el caso de un intento de intercepción, los fotones sean alterados y se alerte tanto al emisor como al receptor del suceso. Esto permitirá detener el tránsito de información antes de que el intruso conozca el mensaje.

Por lo anterior, se puede concluir que la criptografía es una ciencia aplicada que resuelve el problema de la inseguridad que existe durante un proceso de comunicación en el que se maneja información de carácter confidencial, y que ésta ha sido necesaria para el hombre prácticamente desde que empezaron a surgir las primeras comunidades organizadas y empezó a existir una distribución jerárquica en la sociedad; y que sin duda sigue y seguirá siendo necesaria para

proteger y garantizar la integridad de dicha información, así como la legitimación de la fuente de procedencia.

En este trabajo, se le proporcionó al lector la definición y explicación de lo que se debe entender por modelo de comunicación, y se han definido, explicado y analizado los elementos que intervienen dentro del proceso de comunicación criptográfico, tomando como referencia tres de los principales modelos de comunicación que abarcan el estudio de la comunicación secreta como lo son los modelos de *La teoría de la información* de Shanon y Weaver, la *teoría de la comunicación* de Wilbur Schramm, y la *teoría del proceso de la comunicación* de David K. Berlo. Tomando estos modelos como base, se pueden rescatar 11 elementos existentes en el proceso de comunicación criptográfico, los cuales son: fuente, codificador, emisor, mensaje, canal, contexto, ruido, receptor, decodificador, destinatario y retroalimentación. En conclusión se puede decir que para que se dé un proceso criptográfico se requiere forzosamente de un acto comunicativo, y de la intervención e interrelación de los elementos anteriormente mencionados.

Se abordaron las aplicaciones de la criptografía como una técnica para el presente y el futuro, así como la importancia que ésta ha adquirido en las actividades comunes en las sociedades actuales. Se explicaron las tres principales funciones de la criptografía actual, como lo son la autenticación, la firma digital y la identificación del usuario. Además se ejemplificaron algunas de las ramas en las que la criptografía tiene un extenso e importante uso dentro de la sociedad

moderna como lo son la medicina, el ámbito empresarial e incluso el sistema de correo electrónico que se refiere mayormente al respaldo de la privacidad de los individuos.

Por lo expuesto anteriormente, se puede concluir que el campo de acción de la criptografía es cada vez más amplio, y que conforme avanza la tecnología se incrementa también el riesgo de pérdida en la privacidad de los individuos, lo que hace que el uso de las técnicas criptográficas no sea cada vez más frecuente sino necesario. Anteriormente, las técnicas criptográficas eran utilizadas únicamente por los grupos que ocupaban un lugar jerárquico importante o que ostentaban el poder, y eran únicamente estos sectores los que tenían acceso a ellas. Sin embargo, en la actualidad, con el uso de tecnologías de comunicación como Internet, existen flujos de información de enormes dimensiones en todas partes del mundo circulando por la red y alguna parte de esta información es de carácter confidencial o privado, no sólo a niveles empresariales, financieros o políticos, sino también e igualmente importante a nivel personal de todos los usuarios de la red. Al respecto, basta imaginar por un momento que el historial médico de un paciente con VIH puede ser leído por cualquier persona que lo desee, o que los estados financieros de las personas están al alcance de grupos de secuestradores, o simplemente que los correos privados pueden ser leídos por alguien más aparte del destino legítimo.

Todas estas situaciones pueden ser evitadas debida a la evolución que han tenido las técnicas criptográficas que, hoy por hoy, siguen y seguirán siendo un

excelente medio para proteger la información transmitida dentro de un proceso comunicativo.

FUENTES CONSULTADAS

Bibliográficas

Berlo, David K. (1980). *El proceso de la comunicación*, editorial El Ateneo, Buenos Aires.

Drosnin, Michael. (1997). *El código secreto de la Biblia,* 9ª ed., editorial Planeta, Barcelona.

Escarpit, Robert. (1990). *Teoría general de la información y la comunicación*, 2ª ed., ICARA editorial, S.A., Barcelona.

Fúster, Sabater, Amparo *et al*. (2001). *Técnicas criptográficas de protección de Datos,* 2ª ed., editorial Alfaomega, Madrid.

Perseo, Abramo. (1979). *Investigación en ciencias sociales,* BBCS. TA. Queiroz, Sao Paulo.

Pino, Caballero, Gil. (2003). *Introducción a la criptografía*, 2ª ed. actualizada, editorial Alfaomega, Madrid.

Schawanitz, Dietrich. (2002). *La cultura, todo lo que hay que saber,* editorial Santillana, S. L., Madrid.

Schram, Wilbur. (1965). *La ciencia de la comunicación humana,* CIESPAL, Quito Ecuador.

Universidad Autónoma de Veracruz *Villa Rica*. *Manual para la elaboración de tesis de licenciatura.*

Electrónicas

ForoMsn.com Estilo Live, disponible en: [http://www.foromsn.com/index.php?Ver=Mensaje&Id=118752]

Guinness world record, disponible en: [www.albertocoto.com]
___, disponible en: [http://www.albertocoto.com/secciones/cripto.htm]

Red española de I + D, disponible en: [www.rediris.com]

Wikipedia, la enciclopedia libre, disponible en:
[http://es.wikipedia.org/wiki/criptografía]

___, disponible en:
[http://es.wikipedia.org/wiki/Enigma (m%C3%A1quina)]

ANEXOS

A continuación se presentan tres anexos en donde se ejemplifican usos de técnicas criptográficas en diferentes etapas históricas, con el fin de ilustrar la importancia que esta disciplina ha tenido en la historia de la humanidad, además de su evolución.

Anexo 1. El código secreto de la Biblia

El hallazgo de un código secreto en la Biblia, es muestra de que desde tiempos inmemorables la criptografía y los mensajes ocultos han estado presentes en la comunicación del hombre; este ejemplo no pretende ser de índole religioso sino histórico, ya que aborda uno de los documentos más antiguos, más leídos y con mayor influencia en la historia de la humanidad que, ya sea por medio de la "iluminación divina" como algunos afirman o por medio simplemente de la imaginación, fue escrito hace tres mil años, y tiene indicios del uso de elementos criptográficos para codificar información de manera secreta.

Dicho hallazgo dio la vuelta al mundo gracias a diversas publicaciones que avalaban su credibilidad, una de las principales investigaciones que se realizaron acerca del caso, la hizo el destacado periodista estadounidense Michael Drosnin, quien, entre otras actividades, ha trabajado en los periódicos *Washington Post* y en el *Wall Street Journal*, y dedicó cinco años al seguimiento de lo que en un primer momento fuera un encuentro casual con el recién descubierto código secreto de la Biblia:

> *El 1 de septiembre de 1994 volé a Jerusalén para encontrarme con el poeta Chaim Hurí, amigo íntimo de Itzhak Rabin. Un matemático israelí ha descubierto en la Biblia un código secreto que parece revelar hechos ocurridos miles de años después de su escritura –decía mi carta a Rabin -. Si me he permitido escribirle es porque la única vez que su nombre completo (Itzhak Rabin) aparece codificado en la Biblia, las palabras asesino que asesinará lo atraviesan. El 4 de noviembre de 1995 llegaba la terrible confirmación. Un hombre que se creía enviado por Dios le había disparado por la espalda. Durante tres mil años, el atentado había permanecido oculto en el código secreto de la Biblia.* (Drosnin, 1997:13).

El descubrimiento de un código secreto presente en la Biblia se debe al matemático Eliyahu Rips, quien al percatarse de ello realizó todas las pruebas y experimentos necesarios para confirmar la presencia del código, y asegurarse de que no fueran meras coincidencias. Por este motivo, elaboró un sofisticado modelo matemático que, aplicado por computadora, confirmaba la codificación del *Antiguo Testamento.* Este descubrimiento después fue avalado por varios matemáticos de gran prestigio a nivel internacional, como Harold Gans experimentado descodificador de la ultra secreta Agencia Nacional de Seguridad Estadounidense, quien tras crear su propio programa de cómputo para tratar de desenmascarar lo que él creía era una farsa, no tuvo más remedio que corroborar la existencia de un código secreto en la Biblia.

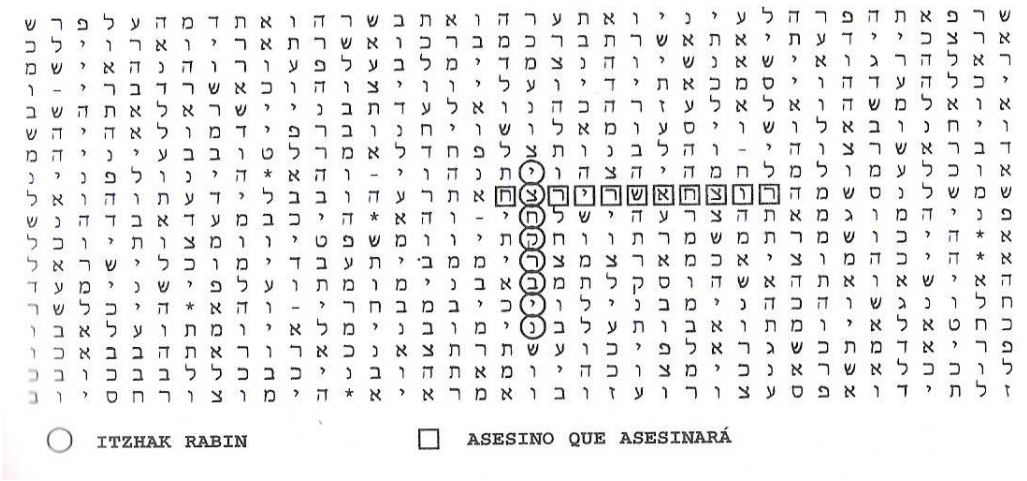
La existencia de dicho código fue también confirmada por la destacada publicación científica norteamericana, la revista *Statistical Science*, cuando su editor, el profesor Robert Kass, mandó el artículo del descubrimiento de Rips a revisión, con tres de los mejores matemáticos que colaboraban en las publicaciones científicas más serias de los Estados Unidos, y el resultado fue la confirmación de los tres; por lo cual se decidió publicar el artículo. Para dar con el código, el Dr. Rips eliminó los espacios entre las palabras convirtiendo al texto en una “hebra continua” de 304,805 letras, un bloque continúo de letras sin solución de palabras, lo que varios expertos en el tema atribuyen como la forma primigenia del texto original.

Posteriormente, ese texto, en su forma original, es procesado por la computadora que verifica todas las secuencias existentes, hasta encontrar si hay combinación alguna que dé como resultado la conformación de palabras cuya formación se dé gracias a una secuencia matemáticamente establecida. Después de identificarlas, la computadora las somete a una doble verificación para corroborar la información obtenida.

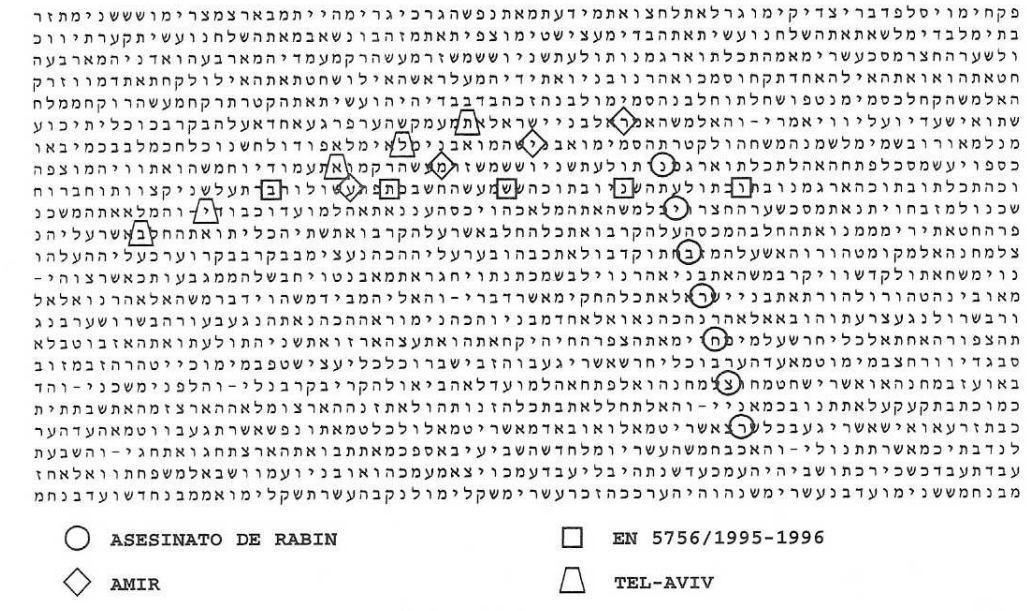
De esta manera, en el código secreto de la Biblia se ha encontrado información codificada que está conformada por datos específicos de acontecimientos importantes en la historia de la humanidad en los que aparecen nombres, fechas y lugares relacionados con eventos como: el holocausto alemán; el asesinato del presidente de los Estados Unidos, John F. Kennedy; la bomba nuclear lanzada sobre Hiroshima; la llegada del hombre a la Luna; el nombre del legendario poeta y escritor inglés William Shakespeare; el nombre del científico Isaac Newton quien descubriera la ley de la gravitación universal; el nombre del científico e inventor Thomas A. Edison; el científico Albert Einstein; el escándalo estadounidense de espionaje presidencial de *Watergate*; la depresión económica estadounidense de1929, y el asesinato del primer ministro israelí Itzhak Rabin, entre muchísimos otros hechos.

Este tipo de codificación se puede ver claramente en los siguientes tres ejemplos, donde se presenta información relacionada con el asesinato de Itzhak Rabin. En uno de los muchos experimentos realizados por Rips en conjunto con el reportero Michael Drosnin, se buscó por medio de la computadora el nombre de Itzhak Rabin en el código de la Biblia y este sólo aparecía una vez, con una secuencia alterna de 4,772 espacios. Entrecruzadas con éste aparecían las palabras *asesino que asesinará*.

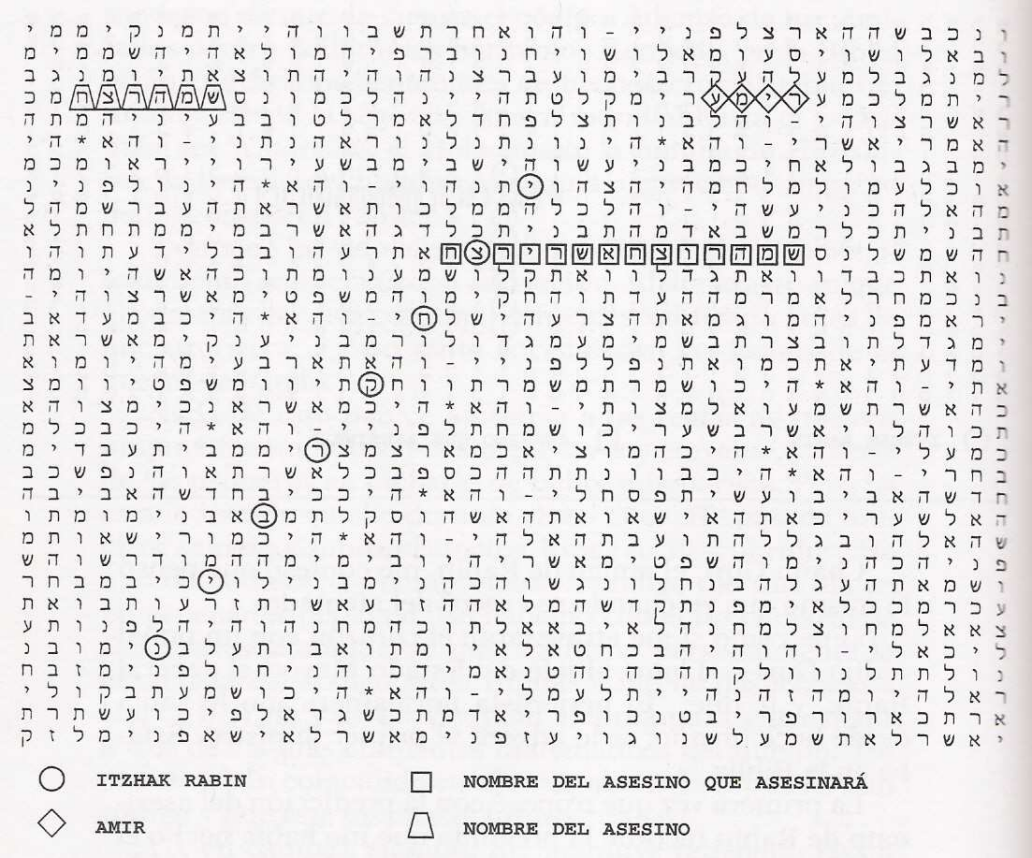
Ejemplo 1. Descodificación de una parte del texto secreto de la Biblia. (Drosnin, 1997:15)



Ejemplo 2. Descodificación de una parte del texto secreto de la Biblia. (Drosnin, 1997:16)



Ejemplo 3. Descodificación de una parte del texto secreto de la Biblia. (Drosnin, 1997:17)



La probabilidad de que el nombre completo de Rabin apareciera entrelazado con la predicción de su muerte eran de una en tres mil, y para los matemáticos todo lo que pasa de una en un centenar resulta altamente improbable; aumenta la probabilidad cuando la distancia suele ser de una entre mil o menor. Este caso, en particular, ha servido para ilustrar uno de los muchos ejemplos comprobados que están presentes en el código secreto de la Biblia, lo cual demuestra que a lo largo de la historia el hombre ha encontrado diversos

medios para mantener segura la información importante y que quien tiene la capacidad de descodificar los mensajes secretos tiene el poder que le brinda la información obtenida. En el caso del código secreto de la Biblia se utilizó la criptografía para descifrar mensajes secretos implícitos en el texto, sean estos creíbles o no.

Anexo 2. El método César

Es uno de los métodos más antiguos de criptografía, su nacimiento u origen se sitúa en el Siglo I a.c. y recibe este nombre gracias a que su invención se le atribuye al emperador romano Julio César; y se dice que éste era el método que él mismo utilizaba para comunicarse de forma segura con sus generales durante las guerras gálicas. Es un método de sustitución monoalfabética, ya que el proceso de sustitución se lleva a cabo en cada uno de los elementos del texto en claro o texto original, que tiene su proceso en la utilización de un alfabeto que se desplazaba un cierto número de puestos; en el método César se utilizaban tres puestos de desplazamiento, por ejemplo para expresar A se escribía la letra D, que se encuentra tres puestos después.

Se puede decir que era un proceso circular, ya que recorre todo el alfabeto y si se llega al final por ejemplo en el caso de la Z, se entiende que volvemos al principio del mismo y al contar tres lugares de desplazamiento que le corresponden a la letra Z dentro de este proceso su equivalente en el Método César sería la letra C:

> *Como puede apreciarse, este método arrastra las debilidades propias de los algoritmos de sustitución. En vez de utilizar siempre la suma de 3 posiciones podría cambiarse este valor por otro cualquiera. En cualquier caso, y para dar con la solución, podemos acudir a un sencillo criptoanálisis basado en la frecuencia de los elementos del criptograma.* (ForoMsn.com Estilo Live, disponible en red: http://www.foromsn.com/index.php?Ver=Mensaje&Id=118752 octubre 2006).

Para explicar este método se utiliza comúnmente el alfabeto anglo, ya que su uso es más extendido en informática que el del alfabeto en español y la única diferencia con este radica en el uso de la letra ñ que no se ocupa en el alfabeto anglo. Se puede explicar el procedimiento que se sigue en el Método César de la siguiente manera: el primer paso consiste en asignar a cada letra un entero, como se ilustra en el siguiente cuadro:

Asignación numérica del alfabeto en el Método César.

Red Española Académica y de Investigación Nacional

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

Posteriormente se elije la combinación de cifrado, suponiendo que la clave de cifrado fuera (1,4) para cifrar la palabra COCINA si se tomara el valor de cada letra de la tabla de asignación numérica del alfabeto, el equivalente numérico para la palabra COCINA sería el siguiente:

2	14	2	8	13	0

A estos números que corresponden a la palabra sin encripción o texto en claro es necesario aplicarles la combinación de la clave de cifrado, en este caso (1,4), de tal manera que a cada número entero dado a las letras de las palabras se le suma el valor 4, como se muestra a continuación:

6	18	6	12	17	4

El código anterior daría como resultado el conjunto de letras GSGMRE, que si se lee de esta manera no significa nada, pero al aplicarle la formula dada (1,4), y utilizando la tabla de valores del alfabeto, el destinatario real del mensaje puede fácilmente descifrarlo. Como se puede observar el método de cifrado César tiene tan sólo 26 claves diferentes en el caso del alfabeto inglés, incluyendo la

clave de identidad en la que el texto cifrado es idéntico al texto original. Por lo que un ataque que permita violar la seguridad de este sistema y ponga en peligro la información es bastante probable, si se toma en cuenta que una búsqueda exhaustiva de la clave correcta no requiere más que de 26 intentos, lo que lo convierte en un método muy vulnerable.

Sin embargo, la mayoría de los historiadores han registrado que el Método César no fue roto durante la época de Julio César, lo que significa que cumplió con su objetivo en su tiempo histórico. En la actualidad, los métodos de sustitución que forman parte de la criptografía clásica, han dejado de ser confiables, debido a la gran capacidad de búsqueda de combinaciones que tienen los programas de cómputo que les permiten romper claves muy grandes en tan sólo minutos, por lo que la criptografía híbrida y, en los últimos años, la criptografía cuántica son la mejor opción para la protección de información de carácter confidencial.

Anexo 3. La máquina *Enigma*

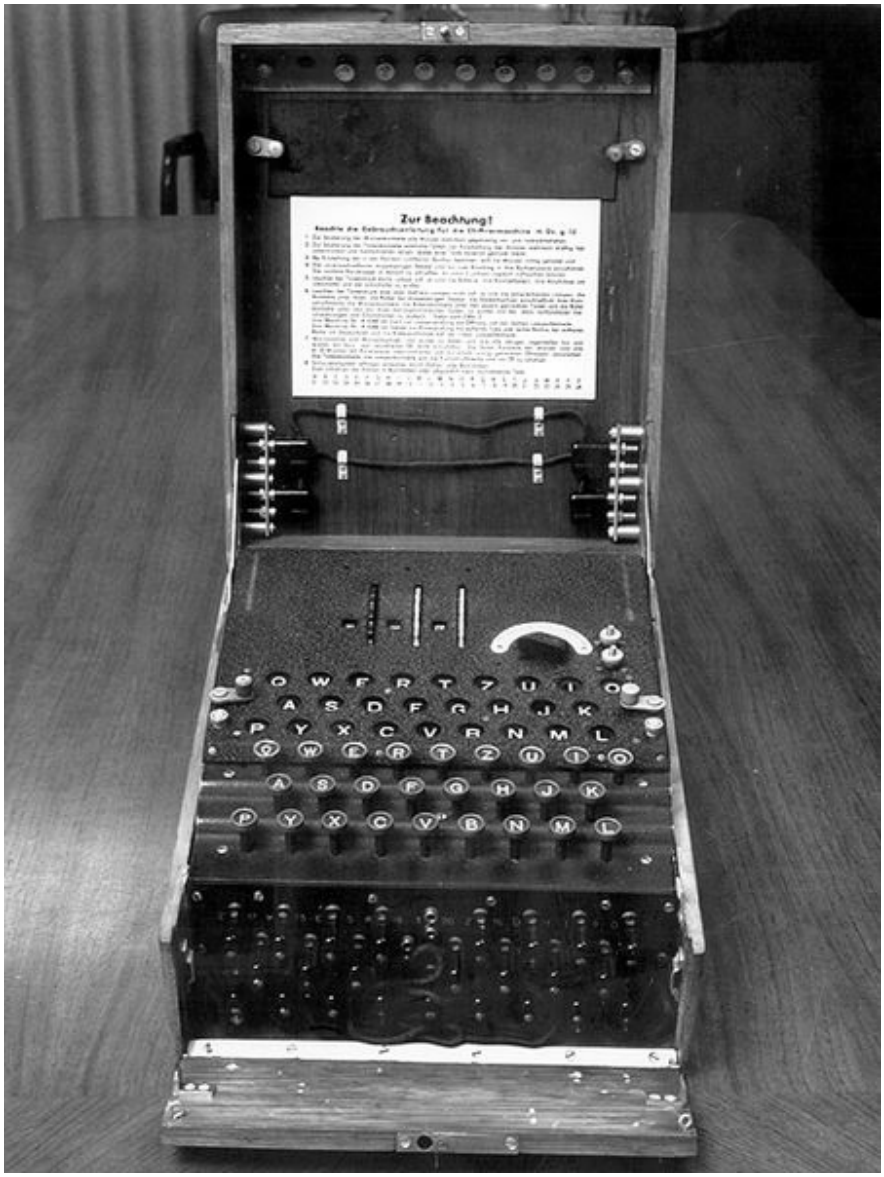
Durante la Segunda Guerra Mundial la comunicación secreta jugó un papel crucial en el curso que tomaban las batallas; varios historiadores atribuyen el término de dicha guerra a la ruptura del método que ofrecía la máquina *Enigma* y, por ende, la lectura de la información que ofrecía en los mensajes que no pudo proteger, por lo que consideran esto como la causa para acabar la guerra al menos un año antes de lo que pudo ser de otra manera.

La máquina *Enigma* es un mecanismo de cifrado rotativo que se utilizaba tanto para realizar un cifrado a un texto en claro como para descifrar el contenido del mismo. Se empezó a usar en Europa a partir de 1920 en adelante, aunque su mayor uso se dio cuando las fuerzas militares alemanas la emplearon como su medio de comunicación secreta más importante a partir de 1930.

La primera patente data de 1919, obra del holandés Alexander Koch; posteriormente el alemán Arthur Scherbius desarrolló varias versiones de *Enigma* y junto con el ingeniero Richard Ritter, fundaron en Berlín la empresa *Chiffriermaschinen Aktien Gesellschaft* y realizaron la producción de lo que sería la primera versión comercial de la máquina conocida como *Enigma-A.* La principal función de ésta fue dar una opción a los comerciantes y hombres de negocios para realizar la comunicación de documentos importantes de manera secreta y segura.

Esta versión salió a la venta por primera vez en 1923, la máquina tuvo una notable evolución, por lo que se fueron creando diversos modelos hasta llegar al más conocido de todos, el modelo *Enigma-D* que fue adquirido por la marina alemana en 1926, y que fue utilizado por las organizaciones militares alemanas y la jerarquía Nazi, donde fue conocida como la máquina “M”:

Máquina *Enigma* utilizada durante la Segunda Guerra Mundial, por el ejército NAZI.



La máquina *Enigma* era un dispositivo electro-mecánico, lo que significa que utilizaba una combinación de partes mecánicas y eléctricas. El mecanismo estaba constituido fundamentalmente por un teclado, similar al de las máquinas de escribir, que controlaba una serie de interruptores eléctricos y un engranaje mecánico. La parte eléctrica consistía en una batería que se conectada a una de las lámparas, que representaban las diferentes letras del alfabeto. Se puede

observar, en la parte inferior de la imagen, el teclado, y las lámparas son los minúsculos círculos que aparecen encima de éste.

El corazón de la máquina *Enigma* era mecánico y consistía de varios *rotores* conectados entre sí. Un rotor es un disco circular plano con 26 contactos eléctricos en cada cara, uno por cada letra del alfabeto. Cada contacto de una cara está conectado o cableado a un contacto diferente de la cara contraria. Por ejemplo, en un rotor en particular, el contacto número 1 de una cara puede estar conectado con el contacto número 14 en la otra cara, y el contacto número 5 de una cara con el número 22 de la otra. Cada uno de los rotores proporcionados con la máquina Enigma estaba cableado de una forma diferente y los rotores utilizados por el ejército alemán poseían un cableado distinto al de los modelos comerciales. Dentro de la máquina había, en la mayoría de las versiones, tres ranuras para poder introducir los rotores. Cada uno de los rotores se encajaba en la ranura correspondiente de forma que sus contactos de salida se conectaban con los contactos de entrada del rotor siguiente. El tercer y último rotor se conectaba, en la mayoría de los casos, a un *reflector* que conectaba el contacto de salida del tercer rotor con otro contacto del mismo rotor para realizar el mismo proceso, pero en sentido contrario y por una ruta diferente.

La existencia del reflector diferencia a la máquina *Enigma* de otras máquinas de cifrado basadas en rotores de la época. Este elemento, que no se incluía en las primeras versiones de la máquina, permitía que la clave utilizada para el cifrado se pudiera utilizar en el descifrado del mensaje.

Se pueden observar en la parte superior de la imagen los tres rotores con sus correspondientes protuberancias dentadas que permitían girarlos a mano, colocándolos en una posición determinada. Cuando se oprimía una tecla, por ejemplo la correspondiente a la letra A, la corriente eléctrica procedente de la batería se dirigía hasta el contacto correspondiente a la letra A del primer rotor. La corriente atravesaba el cableado interno del primer rotor y se posicionaba, por ejemplo, en el contacto correspondiente a la letra J en el lado contrario.

Supongamos que este contacto del primer rotor estaba alineado con el contacto correspondiente a la letra X del segundo rotor. La corriente atravesaba el segundo rotor y seguía su camino a través del segundo y tercer rotor, el reflector y de nuevo a través de los tres rotores en el camino de vuelta. Al final del trayecto, la salida del primer rotor se conectaba a la lámpara correspondiente a una letra, distinta de la A, en el panel de luces. El mensaje de cifrado se obtenía por tanto mediante la sustitución de las letras del texto original por las proporcionadas por la máquina.

Cada vez que se introducía una letra del mensaje original, pulsando la tecla correspondiente en el teclado, la posición de los rotores variaba. Debido a esta variación, a dos letras idénticas en el mensaje original, por ejemplo AA, le correspondían dos letras diferentes en el mensaje cifrado, por ejemplo QL. En la mayoría de las versiones de la máquina, los rotores avanzaban una posición con cada letra. Cuando se habían introducido 26 letras y, por tanto, el primer rotor había completado una vuelta completa, se avanzaba en una muesca la posición del segundo rotor, y cuando éste terminaba su vuelta se variaba la posición del tercer rotor. El número de *pasos* que provocaba el avance de cada uno de los rotores, era un parámetro configurable por el operario. Debido a que el cableado de cada rotor era diferente, la secuencia exacta de los alfabetos de sustitución variaba en función de qué rotores estaban instalados en las ranuras, la posición inicial de esto y su orden de instalación. A estos datos se les conocía con el nombre de *configuración inicial*, y eran distribuidas, mensualmente al principio y con mayor frecuencia a medida que avanzaba la guerra, en libros a los usuarios de las máquinas. El funcionamiento de las versiones más comunes de la máquina *Enigma* era simétrico en el sentido de que el proceso de descifrado era análogo al proceso de cifrado. Para obtener el mensaje original sólo había que introducir las letras del mensaje cifrado en la máquina, siempre y cuando la *configuración inicial* de la máquina fuera idéntica a la utilizada al cifrar la información.