CAPITULO I INTRODUCCIÓN A LA CRIPTOGRAFÍA

1. Introducción.

Desde la antigüedad hasta nuestros días se han mandado mensajes secretos. La necesidad de comunicarse secretamente ha ocurrido en la diplomacia y entre militares. Con la llegada de la comunicación electrónica el interés por mantener mensajes ininteligibles para todos salvo el receptor no ha hecho sino aumentar.

Para introducir unos términos antes de entrar en materia, diremos que ***criptología*** es la disciplina dedicada a comunicarse secretamente. ***Criptografía*** es la parte de la criptología que trata del diseño e implementación de sistemas secretos y criptoanálisis la que se dedica a "romper" dichos sistemas.

La criptografía se refiere a la capacidad de mantener un documento electrónico (o de cualquier otro tipo) inaccesible a todos, excepto a determinadas personas, la autenticidad es la capacidad para determinar si una persona determinada pertenece o no a la lista de personas autorizadas para acezar el documento o no.

Estos problemas de **confidencialidad** y **autenticidad** se resuelven mediante la criptografía, la cual en si es una rama de las matemáticas, la cual al aplicarse a un mensaje proporciona herramientas para la solución de los problemas ya mencionados. El problema de confidencialidad se relaciona comúnmente con técnicas denominadas **encripción** y por su lado la autenticidad mediante una ***firma digital***.

2. Historia de la criptografía.

La Criptografía moderna nace al mismo tiempo que las computadoras. Durante la Segunda Guerra Mundial, en un lugar llamado Bletchley Park, un grupo de científicos entre los que se encontraba Alan Turing, trabajaba en el proyecto ULTRA tratando de descifrar los mensajes enviados por el ejército Alemania con el más sofisticado ingenio de codificación ideado hasta entonces: la máquina ENIGMA. Este grupo de científicos empleaba el que hoy se considera el primer computador (aunque esta información permaneció en secreto hasta mediados de los 70). Su uso y la llegada del polaco Marian Rejewski tras la invasión de su país natal cambiaran para siempre el curso de la Historia.

Desde entonces hasta hoy ha habido un crecimiento espectacular de la tecnología criptográfica, si bien la mayor parte de estos avances se mantenían (y se siguen manteniendo, según algunos) en secreto. Financiadas fundamentalmente por la NSA (Agencia Nacional de Seguridad de los EE.UU.), la mayor parte de las investigaciones hasta hace relativamente poco tiempo han sido tratadas como secretos militares. Sin embargo en los últimos años, investigaciones serias llevadas a cabo en universidades de todo el mundo han logrado que la Criptografía sea una ciencia al alcance de todos, y que se convierta en la piedra angular de asuntos tan importantes como el comercio electrónico, la telefonía móvil, o las nuevas plataformas de distribución de contenidos multimedia.

3. Definición de Criptografía.

Criptografía es una palabra que viene del griego krypto=oculto, y graphos=escribir, literalmente “escritura oculta”), por la cual se entiende, el estudio de la ciencia que, mediante el tratamiento de la información, protege a la misma de modificaciones y utilización no autorizada, utilizando

algoritmos matemáticos complejos para la transformación de la información en un extremo y la realización del proceso inverso en el otro.

Por ello, la criptografía, además de ser una disciplina que estudia los principios, métodos y medios de transformar los datos para ocultar su significado, garantizar su integridad, establecer su autenticidad y prevenir su repudio, tiene bases matemáticas actuales que son: teoría de números, teoría de la complejidad algorítmica, teoría de la información, estadística.

Con más precisión, cuando se habla de esta área de conocimiento como ciencia se debería hablar de criptología, que engloba tanto las técnicas de cifrado, la criptografía propiamente dicha, como sus técnicas complementarias, ***el criptoanálisis***, que estudia los métodos que se utilizan para romper textos cifrados con objeto de recuperar la información original en ausencia de la clave.

La criptografía, mediante el ocultamiento de la información proporciona:

- ***Confidencialidad.*** Garantiza que solo las personas autorizadas tienen acceso a la información.
- ***Autenticación***. Mecanismo para verificar que la información proviene del lugar indicado y que esta no ha sido modificada.
- ***Integridad.*** Forma de detectar que la información no ha sido alterada por alguien no autorizado.
- ***Control de Acceso.*** Restringir el acceso a la información.
- ***No repudio.*** Servicio que garantiza la autoría del mensaje enviado.

4. Criptosistema.

Definiremos un criptosistema como una quíntupla (M;C;K;E;D), donde:

- ✓ ***M*** representa el conjunto de todos los mensajes sin cifrar (lo que se denomina texto claro, o texto plano) que pueden ser enviados.
- ✓ ***C*** representa el conjunto de todos los posibles mensajes cifrados, o ***criptogramas***.
- ✓ ***K*** representa el conjunto de claves que se pueden emplear en el criptosistema.
- ✓ ***E*** es el conjunto de transformaciones de cifrado o familia de funciones que se aplica a cada elemento de ***M*** para obtener un elemento de ***C***. Existe una transformación diferente E_k para cada valor posible de la clave k.
- ✓ ***D*** es el conjunto de transformaciones de descifrado, análogo a E.

Todo criptosistema ha de cumplir la siguiente condición:

$$D_k(E_k(m)) = m \qquad (1)$$

es decir, que si tenemos un mensaje m, lo ciframos empleando la clave k y luego lo desciframos empleando la misma clave, obtenemos de nuevo el mensaje original m.

Estos criptosistemas a su vez tienen dos tipos fundamentales que son los siguientes:

- ➢ ***Criptosistemas simétricos o de clave privada.*** Son aquellos que emplean la misma clave k tanto para cifrar como para descifrar. Presentan el inconveniente de que para ser empleados en

comunicaciones la clave k debe estar tanto en el emisor como en el receptor, lo cual nos lleva preguntarnos cómo transmitir la clave de forma segura.

- ***Criptosistemas asimétricos o de llave pública,*** que emplean una doble clave (k_p; k_P). k_p se conoce como clave privada y k_P se conoce como clave pública. Una de ellas sirve para la transformación E de cifrado y la otra para la transformación D de descifrado. En muchos casos son intercambiables, esto es, si empleamos una para cifrar la otra sirve para descifrar y viceversa. Estos criptosistemas deben cumplir además que el conocimiento de la clave pública k_P no permita calcular la clave privada k_p. Ofrecen un abanico superior de posibilidades, pudiendo emplearse para establecer comunicaciones seguras por canales inseguros (puesto que únicamente viaja por el canal la clave pública, que sólo sirve para cifrar), o para llevar a cabo autenticaciones.

En la práctica se emplea una combinación de estos dos tipos de criptosistemas, puesto que los segundos presentan el inconveniente de ser computacionalmente mucho más costosos que los primeros. En el mundo real se codifican los mensajes (largos) mediante algoritmos simétricos, que suelen ser muy eficientes, y luego se hace uso de la criptografía asimétrica para codificar las claves simétricas (cortas).

5. Criptoanálisis.

La criptología es el nombre genérico con el que se designan dos disciplinas opuestas y a la vez complementarias: ***criptografía*** que ya tenemos entendido de su significado y el ***criptoanálisis***. El criptoanálisis, se ocupa de romper esos procedimientos de cifrado para así recuperar la información original. Ambas disciplinas siempre se han desarrollado de forma paralela, pues cualquier método de cifrado lleva siempre emparejado su criptoanálisis correspondiente Criptoanálisis (del griego kryptos, "escondido" y analyein, "desatar") es el estudio de los métodos para obtener el sentido de una información cifrada, sin acceso a la información secreta requerida para obtener este sentido normalmente. Típicamente, esto se traduce en conseguir la clave secreta. En el lenguaje no técnico, se conoce esta práctica como romper o forzar el código, aunque esta expresión tiene un significado específico dentro del argot técnico.

Criptoanálisis también se utiliza para referirse a cualquier intento de sortear la seguridad de otros tipos de algoritmos y protocolos criptográficos en general, y no solamente el cifrado. Sin embargo, el criptoanálisis suele excluir ataques que no tengan como objetivo primario los puntos débiles de la criptografía utilizada; por ejemplo, ataques a la seguridad que se basen en el soborno, la coerción física, el robo, el keylogging y demás, aunque estos tipos de ataques son un riesgo creciente para la seguridad informática, y se están haciendo gradualmente más efectivos que el criptoanálisis tradicional.

6. Bases fundamentales de la criptografía.

La ciencia de la criptografía se desarrolló, a raíz de los trabajos realizados por Claude Elwood, Shannon y Whitfield Diffie, y se fundamenta principalmente en tres áreas de las matemáticas:

Teoría de la información: Trata temas relacionados con la transmisión de mensajes, en la cual se manejan conceptos como la entropía (incertidumbre, relacionada con el número de estados posibles de un fenómeno).

Teoría de números: Esta rama también se denomina matemática discreta, y estudia las propiedades de los números enteros.

Teoría de la complejidad algorítmica: Trata sobre la dificultad de los algoritmos para tratar ciertos problemas. Hay problemas para los cuales un algoritmo es más eficiente que otro, dependiendo de todas las variantes del problema en sí.

7. Seguridad de la información.

El concepto de seguridad en la información es mucho más amplio que la simple protección de los datos a nivel lógico. Para proporcionar una seguridad real hemos de tener en cuenta múltiples factores, tanto internos como externos. En primer lugar habrá que caracterizar el sistema que va a albergar la información para poder identificar las amenazas, y en este sentido podríamos hacer la siguiente subdivisión:

- ***Sistemas aislados.*** Son los que no están conectados a ningún tipo de red. De unos años a esta parte se han convertido en minoría, debido al auge que ha experimentado Internet.
- ***Sistemas interconectados***. Hoy por hoy casi cualquier ordenador pertenece a alguna red, enviando y recogiendo información del exterior casi constantemente. Esto hace que las redes de ordenadores sean cada día más complejas y supongan un peligro potencial que no puede en ningún caso ser ignorado.

En cuanto a las cuestiones de seguridad que hemos de fijar podríamos clasificarlas de la siguiente forma:

- ***Seguridad física.*** Englobaremos dentro de esta categoría a todos los asuntos relacionados con la salvaguarda de los soportes físicos de la información, más que de la información propiamente dicha. En este nivel estarían, entre otras, las medidas contra incendios y sobrecargas eléctricas, la prevención de ataques terroristas, las políticas de backup, etc. También se suelen tener en cuenta dentro de este punto aspectos relacionados con la restricción de acceso físico a las computadoras únicamente a personas autorizadas.
- ***Seguridad de la información.*** En este apartado prestaremos atención a la preservación de la información frente a observadores no autorizados. Para ello podemos emplear tanto criptografía simétrica como asimétrica, estando la primera únicamente indicada en sistemas aislados, ya que si la empleáramos en redes, al tener que transmitir la clave por el canal de comunicación, estaríamos asumiendo un riesgo excesivo.
- ***Seguridad del canal de comunicación.*** Los canales de comunicación rara vez se consideran seguros. Debido a que en la mayoría de los casos escapan a nuestro control, ya que pertenecen a terceros, resulta imposible asegurarse totalmente de que no están siendo escuchados o intervenidos.
- ***Problemas de autentificación.*** Debido a los problemas del canal de comunicación, es necesario asegurarse de que la información que recibimos en la computadora viene de quien realmente

creemos que viene. Para esto se suele emplear criptografía asimétrica en conjunción con funciones resumen.

- ***Problemas de suplantación.*** En las redes tenemos el problema añadido de que cualquier usuario autorizado puede acceder al sistema desde fuera, por lo que hemos de confiar en sistemas fiables para garantizar que los usuarios no están siendo suplantados por intrusos. Normalmente se emplean mecanismos basados en password para conseguir esto.
- ***No repudio.*** Cuando se recibe un mensaje no solo es necesario poder identificar de forma unívoca al remitente, sino que este asuma todas las responsabilidades derivadas de la información que haya podido enviar. En este sentido es fundamental impedir que el emisor pueda repudiar un mensaje, es decir, negar su autoría sobre él.

CAPITULO II CRIPTOGRAFIA CLÁSICA

El ser humano siempre ha tenido secretos de muy diversa Índole, y ha buscado mecanismos para mantenerlos fuera del alcance de miradas indiscretas. Julio César empleaba un sencillo algoritmo para evitar que sus comunicaciones militares fueran interceptadas. Leonardo Da Vinci escribía las anotaciones sobre sus trabajos de derecha a izquierda y con la mano zurda.

Otros personajes, como Sir Francis Bacon o Edgar Allan Poe eran conocidos por su afición a los códigos criptográficos, que en muchas ocasiones constituían un apasionante divertimento y un reto para el ingenio.

En este capítulo haremos un breve repaso de los mecanismos criptográficos considerados clásicos. Podemos llamar así a todos los sistemas de cifrado anteriores a la II Guerra Mundial, o lo que es lo mismo, al nacimiento de las computadoras. Estas técnicas tienen en común que pueden ser empleadas usando simplemente lápiz y papel, y que pueden ser criptoanalizadas casi de la misma forma. De hecho, con la ayuda de las computadoras, los mensajes cifrados empleando estos códigos son fácilmente descifrables, por lo que cayeron rápidamente en desuso.

La transición desde la Criptografía clásica a la moderna se da precisamente durante la II Guerra Mundial, cuando el Servicio de Inteligencia aliado rompe la máquina de cifrado del ejército alemán, llamada ENIGMA.

Todos los algoritmos criptográficos clásicos son simétricos, ya que hasta mediados de los años setenta no nació la Criptografía asimétrica, y por esa razón este capítulo se engloba dentro del bloque de la asignatura dedicado a los algoritmos de llave privada.

1. Clasificación de los algoritmos clásicos.

Esta sección muestra una clasificación de los sistemas clásicos, en donde se incluyen algunos cifradores típicos a modo de ejemplo. Estos sistemas se clasificarán, básicamente, en aquellos que utilizan técnicas de sustitución y aquellos que utilizan técnicas de transposición sobre los caracteres de un mensaje en claro, ambas técnicas propuestas por Shannon para lograr la confusión y difusión, respectivamente.

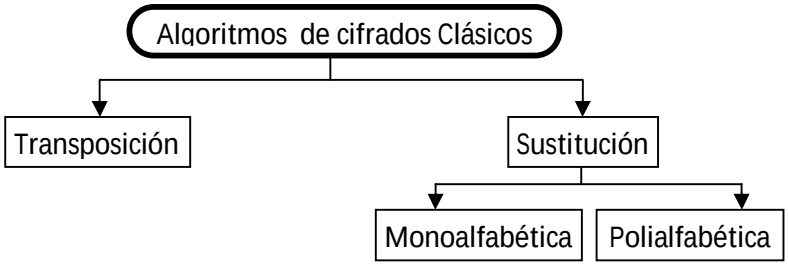

Figura 1. ***Clasificación de los algoritmos clásicos***

2. Algoritmos de cifrado por sustitución.

En esta sección se podrá observar algunos criptosistemas que en la actualidad han perdido su eficacia, debido a que son fácilmente criptoanalizables empleando cualquier computadora doméstica, pero que fueron empleados con éxito hasta principios del siglo XX. Algunos se remontan

incluso, como el algoritmo de César, a la Roma Imperial. Sin embargo mantienen un interés teórico, ya que nos van a permitir explotar algunas de sus propiedades para entender mejor los algoritmos modernos.

2.1. Cifrados Monoalfabéticos.

Se engloban dentro de este apartado todos los algoritmos criptográficos que, sin desordenar los símbolos dentro del mensaje, establecen una correspondencia única para todos ellos en todo el texto. Es decir, si al símbolo A le corresponde el símbolo D, esta correspondencia se mantiene a lo largo de todo el mensaje.

🗝 Algoritmo de César

El algoritmo de César, llamado así porque es el que empleaba Julio César para enviar mensajes secretos, es uno de los algoritmos criptográficos más simples. Consiste en sumar 3 al número de orden de cada letra. De esta forma a la A le corresponde la D, a la B la E, y así sucesivamente. Si asignamos a cada letra un número (A = 0,B = 1. . .), y consideramos un alfabeto de 26 letras, la transformación criptográfica será:

$$C = (M + 3) \bmod 26$$

Obsérvese que este algoritmo ni siquiera posee clave, puesto que la transformación siempre es la misma. Obviamente, para descifrar basta con restar 3 al número de orden de las letras del criptograma.

Ejemplo.

Texto a cifrar: Universidad
Clave: C=3
Texto cifrado: Xqlyhuvlgcg

2.2. Cifrados Polialfabéticos.

En los cifrados polialfabéticos la sustitución aplicada a cada carácter varía en función de la posición que ocupe éste dentro del texto claro. En realidad corresponde a la aplicación cíclica de n cifrados monoalfabéticos.

🗝 Cifrado de Vigénere

Es un ejemplo típico de cifrado polialfabético que debe su nombre a Blaise de Vigénere, su creador, y que data del siglo XVI. La clave está constituida por una secuencia de símbolos $K=\{k_0; k_1;\ldots\ldots;k_{d-1}\}$, y que emplea la siguiente función de cifrado:

$$E_k(m_i) = m_i + k_{(i \bmod d)} \pmod n$$

siendo m_i el iésimo símbolo del texto claro y n el cardinal del alfabeto de entrada.

Para criptoanalizar este tipo de claves basta con efectuar *d* análisis estadísticos independientes agrupando los símbolos según la k_i empleada para codificarlos. Para estimar *d*, buscaremos la periodicidad de los patrones comunes que puedan aparecer en el texto cifrado.

Obviamente, para el criptoanálisis, necesitaremos al menos d veces más cantidad de texto que con los métodos monoalfabéticos.

Ejemplo.

Texto a cifrar: *Universidad*
Clave: *PotosiPotos*
Texto cifrado: *Jbbjwzhwwov*

3. Algoritmos de cifrado por transposición

Este tipo de mecanismos de cifrado no sustituye unos símbolos por otros, sino que cambia su orden dentro del texto. Quizás el más antiguo conocido sea el *escitalo*, formado por un bastón cilíndrico con un radio particular y una tira de piel que se enrollaba alrededor de aquél. El texto se escribía a lo largo del bastón y sólo podía ser leído si se disponía de otro bastón de dimensiones similares. Un mecanismo de transposición sencillo, que no precisa otra cosa que lápiz y papel, podría consistir en colocar el texto en una tabla de ***n*** columnas, y dar como texto cifrado los símbolos de una columna(ordenados de arriba abajo) concatenados con los de otra, etc. La clave k se compondría del número ***n*** junto con el orden en el que se deben leer las columnas.

Por ejemplo, Se quiere cifrar el texto "Ingeniería de Sistemas", con n = 5 y la permutación {3; 2; 5; 1; 4} como clave. Colocamos el texto en una tabla y obtenemos:

1	2	3	4	5
I	n	g	e	n
I	e	r	i	a
	d	e		s
I	s	t	e	m
A	s			

Tendríamos como texto cifrado la concatenación de las columnas 3,2,5,1 y 4 respectivamente: "Gret nedssnasm Ii iaei e ". Nótese que hemos de conservar los espacios del texto cifrado para que el mecanismo surta efecto.

Criptoanálisis

Este tipo de mecanismos de cifrado se puede criptoanalizar efectuando un estudio estadístico sobre la frecuencia de aparición de pares y tripletas de símbolos en el lenguaje en que esté escrito el texto claro. Suponiendo que conocemos ***n***, que en nuestro es igual a 5, tenemos 5! = 120 posibles claves. Descifraríamos el texto empleando cada una de ellas y comprobaríamos si los pares y tripletas de símbolos consecutivos que vamos obteniendo se corresponden con los más frecuentes en castellano. De esa forma podremos asignarle una probabilidad automáticamente a cada una de las posibles claves.

Si, por el contrario, desconocemos ***n***, basta con ir probando con n = 2, n = 3 y así sucesivamente. Este método es bastante complejo de llevar a cabo manualmente, a no ser que se empleen ciertos trucos, pero una computadora puede completarlo en un tiempo más que razonable sin demasiados problemas.

- ***Transposición Inversa.***

  Es el algoritmo más simple. Lo requerido para poder ejecutar el algoritmo, se debe saber donde inicia y donde termina nuestro mensaje. Se trata de invertir el inicio y el final de nuestro mensaje, cabe destacar que el algoritmo de cifrado es igual al de descifrado.

  Ejemplo.

  Mensaje a cifrar: *Hola mundo*
  Mensaje cifrado: *Odnumaloh*

- ***Transposición Simple.***

  El algoritmo divide un mensaje en claro símbolo por símbolo, si el número de símbolos es impar, el primer grupo de símbolos tendrá un elemento más. Podemos ver el algoritmo como si numeráramos los elementos, en el primer bloque tendremos los elementos impares mientras en el segundo estarán los elementos pares. Para finalizar concatenamos los bloques y así tendremos el criptograma.

  Ejemplo:

  Mensaje a cifrar: *Hola mundo*
  Bloque 1(pares): *hlmno*
  Bloque 2(impares): *oaud*
  Mensaje cifrado: *hlmnooaud*

  El proceso de descifrado, es similar, dividimos el criptograma en dos partes iguales, la primera mitad del criptograma será el primer bloque. Teniendo ambos bloques, se intercalan uno a uno los elementos de cada bloque, puede leerse el ejemplo de abajo hacia arriba, para ver la operación.

- ***Transposición Doble.***

  Supone una transposición simple, después aplica nuevamente una transposición simple al criptograma, esto nos dará nuestro criptograma final. Es un algoritmo sencillo si se conoce la transposición simple. Es de utilidad principalmente para despistar a un cripto-analista que intente descifrar nuestro criptograma suponiendo que este fue cifrado mediante transposición simple.

- ***Transposición por grupos.***

  Utiliza la técnica de permutación de forma que los caracteres del texto se reordenan bloques de ***n*** caracteres pero reordenados (permutados) éstos de forma que su posición en el criptograma sea, por ejemplo, 43521; es decir, el cuarto carácter del bloque en claro se transmite primero, a continuación el tercero, después el quinto, luego el segundo y, por último, el primero. Esta operación se repetirá en cada bloque de 5 caracteres del mensaje. Por lo tanto, la transposición implica que los caracteres del criptograma serán exactamente los mismos que los del texto en claro.

Ejemplo:

Clave: 43521.
Texto a Cifrar: *UNIVERSIDAD AUTÓNOMA TOMAS FRÍAS1.*
Dividido en bloques: *UNIVE RSIDA DAUTO NOMAT OMASF RIAS1*
Texto Cifrado: *VIENU DIASR TUOAD AMTON SAFMO SA1IR*

Para descifrar se seguirá el mismo algoritmo, reordenando la clave en el orden original en este caso 54213.

- ***Transposición por series.***

En este algoritmo debemos ordenar el mensaje de tal manera que el criptograma está formado por la secuencia de mensajes que se haya considerado para conformarlo. Cada cadena sigue una función específica.

Ejemplo: Se tiene que tomar en cuenta funciones muy sencillas como en este ejemplo se muestra.

Texto a cifrar: hola mundo
f(1) = números primos = 1,2,3,5 = holm
f(2) = números pares = 4,6,8 = aud
f(3) = números impares = 9 = o
Texto cifrado: holmaudo

Para descifrar solo debemos saber el orden en el que están las funciones y cuáles son, así podremos tener el número correspondiente a cada símbolo y reordenar el mensaje sin problemas.

- ***Máscara rotativa.***

En este algoritmo se crea una matriz A de nxn, A cada Aij le corresponderá un símbolo que puede o no, pertenecer al mensaje. Se crea una matriz B de nxn donde se escogen ciertos componentes de la matriz que corresponderán a los elementos de la matriz A que pertenecen al mensaje, de tal manera que estos elementos queden seleccionados cada vez que la matriz B se sobrepone a la matriz A, en cualquiera de sus 4 lados, tomando como referencia inicial uno de sus lados.

Ejemplo como gira la matriz B:

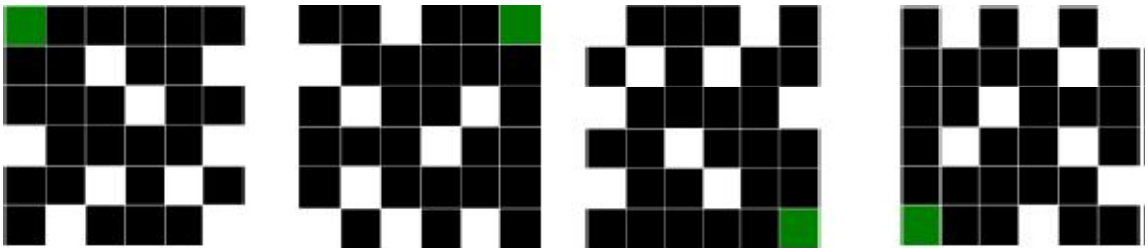

Figura 2. Mascara rotativa