

Contenido

1	Objetivos generales	3
2	Introducción al concepto de criptografía.....	4
2.1	¿Qué es la criptografía?	4
2.2	El comienzo de la criptografía.....	5
2.3	¿Por qué utilizar la criptografía?	7
3	Tipos.....	11
3.1	Criptografía simétrica	11
3.1.1	Concepto.....	11
3.1.2	Esquema de funcionamiento	12
3.1.3	Principales algoritmos	15
3.1.4	Ventajas e inconvenientes	23
3.2	Criptografía asimétrica	24
3.2.1	Concepto.....	24
3.2.2	Sistema asimétrico RSA.....	26
3.2.3	Ventajas e inconvenientes	29
3.3	Ejemplo didáctico de cifrado	30
3.4	Otras herramientas criptográficas	32
3.4.1	Compartición de secretos	32
3.4.2	Criptografía visual	33
3.4.3	Dinero electrónico	36
4	Funciones de autenticación e integridad	41
4.1	Concepto de autenticación e integridad.....	41
4.2	Funciones de autenticación.....	41
4.3	Funciones de integridad.....	42
4.4	Firma y certificados digitales	44
4.5	Firma digital	44
4.5.1	Significado de la firma digital	44
4.5.2	Procedimiento de la firma digital	46
4.5.3	Ejemplo didáctico de firma digital	47
4.6	Certificado digital	50
4.6.1	Certificado digital.....	50
4.6.2	Tipos de certificados	52
4.6.3	Contenido de un certificado	53
4.6.4	Ejemplo didáctico de un certificado digital.....	57
5	Resumen	63
6	Glosario	65
7	Bibliografía.....	67

1 Objetivos generales

Los objetivos de este curso son los siguientes:

- **Conocer** los conceptos generales de la criptografía y sus dos principales tipos.
- **Comprender** la aplicación de cifrado simétrico y asimétrico.
- **Identificar** los diferentes sistemas criptográficos tanto simétricos como asimétricos.
- **Descubrir** otros tipos de herramientas de criptografía.
- **Conocer** el uso de la criptografía sobre la firma y certificado digital.

2 Introducción al concepto de criptografía

Los objetivos de esta unidad son los siguientes:

- **Comprender** en qué consiste la criptografía.
- **Conocer** la evolución de la criptografía desde sus comienzos.
- **Identificar** los tipos de cifrado.

2.1 ¿Qué es la criptografía?

- La **criptografía** (del griego κρύπτω *krypto*, «oculto», y γράφω *graphos*, «escribir», literalmente «escritura oculta») es la técnica, bien sea aplicada al arte o la ciencia, que altera las representaciones lingüísticas de un mensaje.

La criptografía es la técnica que protege documentos y datos. Para ello existen distintos métodos, en donde el más común es el cifrado. Esta técnica enmascara las referencias originales de la lengua por un método de conversión gobernado por un algoritmo que permita el proceso inverso o descifrado de la información.

Funciona a través de la utilización de cifras o códigos para escribir algo secreto en documentos y datos confidenciales que circulan en redes locales o en internet. Su utilización es tan antigua como la escritura. Los romanos usaban códigos para ocultar sus proyectos de guerra de aquellos que no debían conocerlos, con el fin de que sólo las personas que conocían el significado de estos códigos descifrarán el mensaje oculto.



A partir de la evolución de los ordenadores, la criptografía fue ampliamente divulgada, empleada y modificada, y se constituyó luego con algoritmos matemáticos. Además de mantener la seguridad del usuario, la criptografía preserva la integridad de la Web, la autenticación del usuario así como también la del remitente, el destinatario y de la actualidad del mensaje o del acceso.

Un ejemplo cotidiano de criptografía es el que usamos cuando mandamos una carta por correo postal.

El mensaje origen queda enmascarado por una cubierta denominada sobre, la cual declara el destinatario coherente, que además conoce el proceso inverso para hacer público el mensaje contenido en el sobre.

2.2 El comienzo de la criptografía

La historia de la criptografía es larga y abunda en anécdotas. Ya las primeras civilizaciones desarrollaron técnicas para enviar mensajes durante las campañas militares, de forma que si el mensajero era interceptado la información que portaba no corriera el peligro de caer en manos del enemigo. Posiblemente, el primer criptosistema que se conoce fuera documentado por el historiador griego Polibio: un sistema de sustitución basado en la posición de las letras en una tabla. También los romanos utilizaron sistemas de sustitución, siendo el método actualmente conocido como César, porque supuestamente Julio César lo empleó en sus campañas, uno de los más conocidos en la literatura (según algunos autores, en realidad Julio César no usaba este sistema de sustitución, pero la atribución tiene tanto arraigo que el nombre de este método de sustitución ha quedado para los anales de la historia). César, es un tipo de cifrado por sustitución en el que una letra en el texto original es reemplazada por otra letra que se encuentra un número fijo de posiciones más adelante en el alfabeto. Por ejemplo, con un desplazamiento de 3, la A sería sustituida por la D (situada 3 lugares a la derecha de la A), la B sería reemplazada por la E, etc.

Otro de los métodos criptográficos utilizados por los griegos fue la escítala espartana, un método de trasposición basado en un cilindro que servía como clave en el que se enrollaba el mensaje para poder cifrar y descifrar.

En 1465 el italiano Leon Battista Alberti inventó un nuevo sistema de sustitución polialfabética que supuso un gran avance de la época. Otro de los criptógrafos más

importantes del siglo XVI fue el francés Blaise de Vigenère que escribió un importante tratado sobre "la escritura secreta" y que diseñó una cifra que ha llegado a nuestros días asociada a su nombre. ASelenus se le debe la obra criptográfica "Cryptomenytices et Cryptographiae" (Luneburgo, 1624). Durante los siglos XVII, XVIII y XIX, el interés de los monarcas por la criptografía fue notable. Las tropas de Felipe II emplearon durante mucho tiempo una cifra con un alfabeto de más de 500 símbolos que los matemáticos del rey consideraban inexpugnable. Cuando el matemático francés François Viète consiguió criptoanalizar aquel sistema para el rey de Francia, a la sazón Enrique IV, el conocimiento mostrado por el rey francés impulsó una queja de la corte española ante del papa Pío V acusando a Enrique IV de utilizar magia negra para vencer a sus ejércitos. Por su parte, la reina María Estuardo, reina de Escocia, fue ejecutada por su prima Isabel I de Inglaterra al descubrirse un complot de aquella tras un criptoanálisis exitoso por parte de los matemáticos de Isabel.

Durante la Primera Guerra Mundial, los Alemanes usaron el cifrado ADFGVX. Este método de cifrado es similar a la del tablero de ajedrez Polibio. Consistía en una matriz de 6 x 6 utilizado para sustituir cualquier letra del alfabeto y los números 0 a 9 con un par de letras que consiste de A, D, F, G, V, o X..

Desde el siglo XIX y hasta la Segunda Guerra Mundial, las figuras más importantes fueron la del holandés Auguste Kerckhoffs y la del prusiano Friedrich Kasiski. Pero es en el siglo XX cuando la historia de la criptografía vuelve a experimentar importantes avances. En especial durante las dos contiendas bélicas que marcaron al siglo: la Gran Guerra y la Segunda Guerra Mundial. A partir del siglo XX, la criptografía usa una nueva herramienta que permitirá conseguir mejores y más seguras cifras: las máquinas de cálculo. La más conocida de las máquinas de cifrado posiblemente sea la máquina alemana Enigma: una máquina de rotores que automatizaba considerablemente los cálculos que era necesario realizar para las operaciones de cifrado y descifrado de mensajes. Para vencer al ingenio alemán, fue necesario el concurso de los mejores matemáticos de la época y un gran esfuerzo computacional. No en vano, los mayores avances tanto en el campo de la criptografía como en el del criptoanálisis no empezaron hasta entonces.

Tras la conclusión de la Segunda Guerra Mundial, la criptografía tiene un desarrollo teórico importante, siendo Claude Shannon y sus investigaciones sobre teoría de la información esenciales hitos en dicho desarrollo. Además, los avances en computación automática suponen tanto una amenaza para los sistemas existentes como una oportunidad para el

desarrollo de nuevos sistemas. A mediados de los años 70, el Departamento de Normas y Estándares norteamericano publicó el primer diseño lógico de un cifrador que estaría llamado a ser el principal sistema criptográfico de finales de siglo: el Estándar de Cifrado de Datos o DES. En esas mismas fechas ya se empezaba a gestar lo que sería la, hasta ahora, última revolución de la criptografía teórica y práctica: los sistemas asimétricos. Estos sistemas supusieron un salto cualitativo importante, ya que permitieron introducir la criptografía en otros campos que hoy día son esenciales, como el de la firma digital.

2.3 ¿Por qué utilizar la criptografía?

La criptografía ha sido usada a través de los años para mandar mensajes confidenciales cuyo propósito es que sólo las personas autorizadas puedan entender el mensaje. Alguien que quiere mandar información confidencial aplica técnicas criptográficas para poder “esconder” el mensaje (lo llamaremos cifrar o encriptar), manda el mensaje por una línea de comunicación que se supone insegura y después solo el receptor autorizado pueda leer el mensaje “escondido” (lo llamamos descifrar o desencriptar).

Las razones de usar esta técnica pueden ser muchas, por ejemplo:

- *Si el PC de trabajo es compartido y en él se almacena información personal, por lo que cualquiera podría tener acceso a ella. Encriptando los ficheros y/o carpetas, se impide que terceras personas sin la clave puedan tener acceso a dicha información.*
- *Como último ejemplo, está el caso del envío de información importante por correo electrónico. En este caso, si se encriptan los ficheros antes de enviarlos, el emisor se asegura que nadie pueda tener acceso a los datos enviados.*

Pero también hay que ser cauto a la hora de encriptar, porque la criptografía no es un juego. Cuando se encripta un archivo, se usa una clave que sólo la persona que lo hace conoce. Si un día se olvida de ella, resultará imposible recuperar la información. Nadie podrá desencriptar un archivo sin la clave.