SAD - U2.1. Criptografía

Descargar estos apuntes

Índice

- 1. Criptografía

1. Criptografía

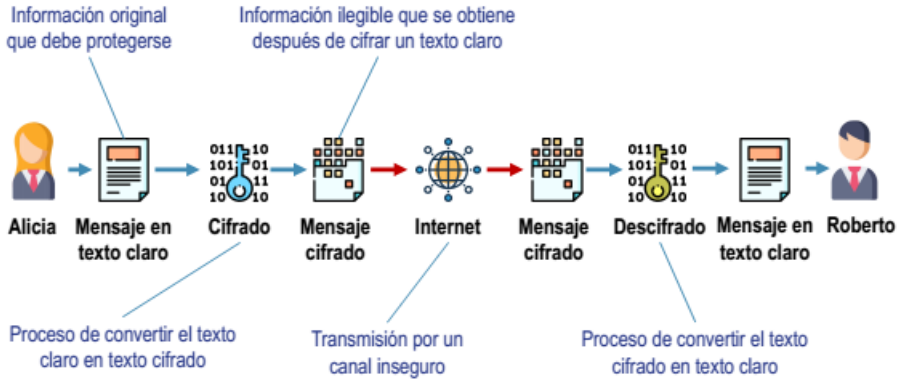
La criptografía es una disciplina que se encarga de **garantizar la confidencialidad, integridad y autenticidad de la información**. Para ello, se utilizan técnicas que permiten cifrar y descifrar la información, de forma que solo las personas autorizadas puedan acceder a ella. La criptografía se ha utilizado desde la antigüedad, aunque en la actualidad ha evolucionado mucho y se ha convertido en una disciplina muy compleja y especializada.

1.1. Definiciones

Esta materia utiliza una terminología específica con la que debemos familiarizarnos:

- **Criptología**: La criptografía (del griego κρύπτος (kryptós), `secreto`, y γραφή (graphé), `grafo o escritura`, literalmente *escritura secreta*).
  Se trata del estudio de los criptosistemas. Sus áreas principales de estudio son, entre otros:
  - **Criptografía**: del griego κρύπτος (kryptós), `secreto`, y γραφή (graphé), `grafo o escritura`, literalmente *escritura secreta*. El diccionario de la RAE lo define como
    > el arte de escribir con clave secreta o de un modo enigmático.

    La criptografía no pretende ocultar un mensaje, sino únicamente su significado, a través de la codificación.
  - **Criptoanálisis**: es la ciencia encargada de buscar vulnerabilidades en los sistemas criptográficos y acceder a la información secreta sin disponer de la o las claves de cifrado.
- **Criptosistema**: según el Centro Criptológico Nacional (CCN), es el conjunto de claves y equipos de cifra que, utilizados coordinadamente, ofrecen un medio para cifrar y descifrar.



Relacionando todos estos conceptos, podemos decir que la criptografía está integrada por las técnicas utilizadas para, utilizando una `clave`, convertir un mensaje inteligible (llamado `texto en claro`) en otro `(texto cifrado`), cuyo contenido solo puede ser comprendido por quienes conozcan la clave. Los algoritmos de cifrado son el método utilizado para ocultar el contenido del mensaje y el criptosistema es el conjunto de equipos y claves usados para cifrarlo.

> **Note**
>
> **Cifrar/descifrar**: transcribir, utilizando una `clave`, un mensaje cuyo contenido se quiere ocultar/mostrar.
> **Clave**: conjunto de signos utilizados para la transmisión de un mensaje privado cuyo contenido se quiere ocultar/recuperar.

En criptografía siempre se cumple la siguiente relación:

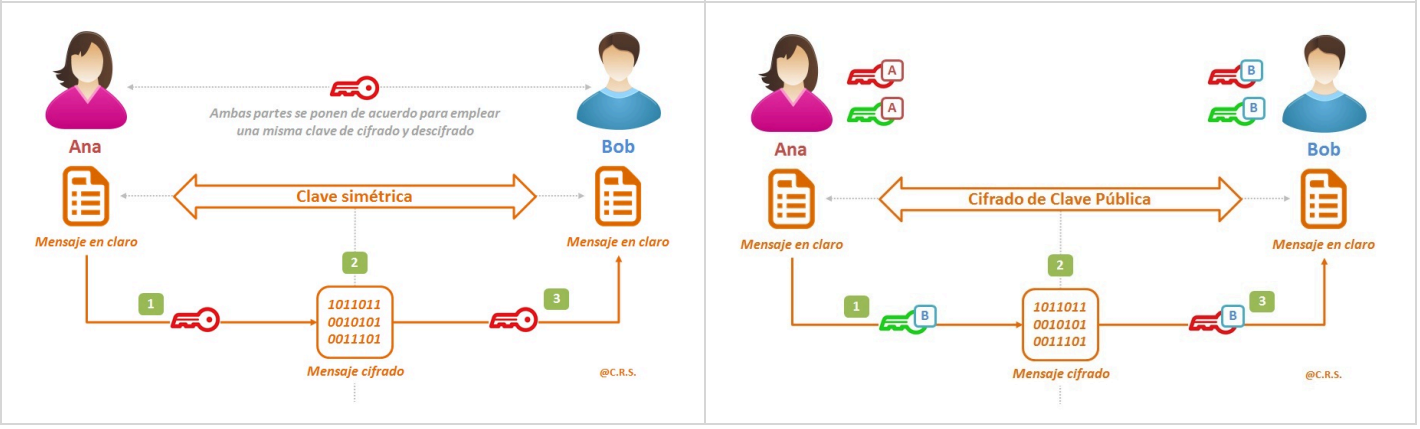
> **Descifrado(k,Cifrado(k,m)) = m**

Es decir, si se tiene un mensaje m y se cifra utilizando la clave k, se obtiene un mensaje cifrado. Si a ese mensaje cifrado se le aplica la transformación de descifrado para esa misma clave (Dk), se obtiene el mensaje original m.

1.2. Tipos de cifrado

Existen dos tipos de criptografía, **según el tipo de clave utilizada**:

- **Criptografía simétrica o de clave secreta**: en la que se utiliza la misma clave para cifrar y descifrar el mensaje. Es más rápida que la asimétrica, pero presenta el problema de la distribución de claves.
- **Criptografía asimétrica o de clave pública**: en la que se utilizan dos claves, una pública y otra privada. La clave pública se puede distribuir libremente, mientras que la clave privada debe ser conocida únicamente por el receptor del mensaje. Es más segura que la simétrica, pero más lenta. Lo que el emisor cifra con una clave, el receptor lo descifra con la otra clave.
  La seguridad de este tipo de sistemas radica en la dificultad de averiguar la clave privada a partir de la pública.



Existen varias técnicas de cifrado, **según la forma en la que operan los algoritmos de cifrado o descifrado**:

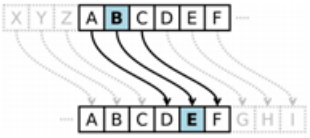
- **Cifrado por transposición**: los signos o símbolos del mensaje original se cambian de posición.
- **Cifrado por sustitución**: los signos o símbolos del mensaje original son sustituidos por otros.
- **Cifrado por bloques**: El cifrado se realiza bloque a bloque. En primera instancia, se descompone el mensaje en bloques de la misma longitud. A continuación, cada bloque se va convirtiendo en un bloque del mensaje cifrado mediante una secuencia de operaciones. Ejemplos típicos de operaciones realizadas para conseguir cada mensaje cifrado son la sustitución y la transposición de elementos.
- **Cifrado por flujo**: En estos algoritmos el cifrado se realiza bit a bit. Están basados en la utilización de claves muy largas que son utilizadas tanto para cifrar como para descifrar.
  El cifrado se realiza bloque a bloque. En primera instancia, se descompone el mensaje en bloques de la misma longitud. A continuación, cada bloque se va convirtiendo en un bloque del mensaje cifrado mediante una secuencia de

operaciones. Ejemplos típicos de operaciones realizadas para conseguir cada mensaje cifrado son la sustitución y la transposición de elementos.

Escítala espartana
(siglo V a. C.)

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

Cifrador de Polibio
(siglo II a. C.)



Cifrado César
(siglo I a. C.)

Orígenes y evolución de la criptografía

La criptografía es una disciplina muy antigua. El primer método de criptografía conocido fue la **escitala**, utilizado en Esparta en el siglo V a. de C., que utilizaba técnicas de transposición. Los sistemas evolucionaron hacia el uso de la sustitución de caracteres, como por ejemplo en el **cifrado César**, utilizado en Roma por Julio César.

Si quieres profundizar en los cifrados por sustitución, puedes leer este artículo de wikiwand

La **máquina Enigma** se usó en la Segunda Guerra Mundial por las fuerzas militares de Alemania para cifrar los mensajes. Usaba un mecanismo de cifrado rotatorio que le permitía tanto cifrar como descifrar. Su sistema de cifrado fue finalmente descubierto.

1.3 Comunicaciones seguras

La criptografía es una disciplina fundamental para garantizar la seguridad en las comunicaciones. En la actualidad, la mayoría de las comunicaciones se realizan en red, por lo que es necesario garantizar la seguridad de las mismas. Para ello, se utilizan protocolos de seguridad que permiten cifrar la información que se envía y se recibe, de forma que solo el emisor y el receptor puedan acceder a ella.

Decimos que la comunicación es segura si se verifica confidencialidad, integridad y disponibilidad, además de la autenticación y el no repudio.

- Las técnicas de **cifrado** garantizan la `confidencialidad` de la información, pero no la integridad ni la autenticidad.
- Para garantizar la `integridad` de la información se utilizan **funciones hash**, que permiten verificar que la información no ha sido alterada.
- Por otro lado, la `autenticación` se consigue mediante la **firma digital**, que permite verificar la identidad del emisor de un mensaje. El `no repudio` se verifica implícitamente con la autenticación.
- La `disponibilidad`, por su parte, permite que la comunicación en sí se lleve a cabo. Si no se cumple disponibilidad no existe tal comunicación, por lo que no se puede verificar seguridad.

¿Cómo se logra esto con mecanismos de criptografía moderna?

Existen diversos mecanismos criptográficos para lograr la seguridad de una comunicación, en términos de confidencialidad, autenticidad e integridad.

Los mecanismos principales son tres:

1. Criptografía simétrica: los algoritmos de cifrado usados serán simétricos si se utiliza la misma clave para encriptar el contenido y para desencriptarlo. Ejemplos de algoritmos simétricos son AES, 3DES, Blowfish, Twofish.
2. Criptografía asimétrica: En este caso los algoritmos utilizan dos claves, una para cifrar, y otra para descifrar. A estos algoritmos también se los denomina de clave pública, ya que a una de las claves se la denomina pública, y a la otra privada. Son la base de la firma digital. Ejemplos de algoritmos asimétricos son RSA, DSA o variantes como ECDSA.
3. Funciones hash: Las funciones hash, o resumen, permiten realizar cálculos para mapear un determinado dato de entrada en una cadena fija de bytes de salida (independientemente de la longitud del dato de entrada). Ejemplos de funciones hash tenemos MD5, la serie SHA y la serie SHA-3, entre otros.

Criptografía postcuántica

Uno de los retos de la criptografía actual es la aparición de los ordenadores cuánticos, que podrían romper los sistemas de cifrado actuales.

Por ello, se están investigando nuevos algoritmos de cifrado que sean resistentes a los ordenadores cuánticos.

Más información

Cifrados clásicos

Actividad U1.1: Usando el cifrado César, ¿cómo se cifraría el mensaje "SEGURIDAD" con un desplazamiento de 3 posiciones? ¿Y cómo se descifraría?

Actividad U2.2: Investigar sobre el **cifrado de Vigenère**, que fue utilizado por Blaise de Vigenère en el siglo XVI. Puedes ver este vídeo de Youtube para entender cómo funciona.

¿Usando la clave BALMIS, y un alfabeto de 26 letras, cómo sería el cifrado del mensaje "SEGURIDAD"?
¿Y cómo lo descifrarías?