



Universidad de las Ciencias Informáticas Especialidad Seguridad Informática

ENTRENAMIENTO EN ELEMENTOS DE CRIPTOGRAFÍA

25 de junio del 2018

Conferencia

Sumario

1. Introducción
2. Conceptos básicos de criptografía.

Objetivos

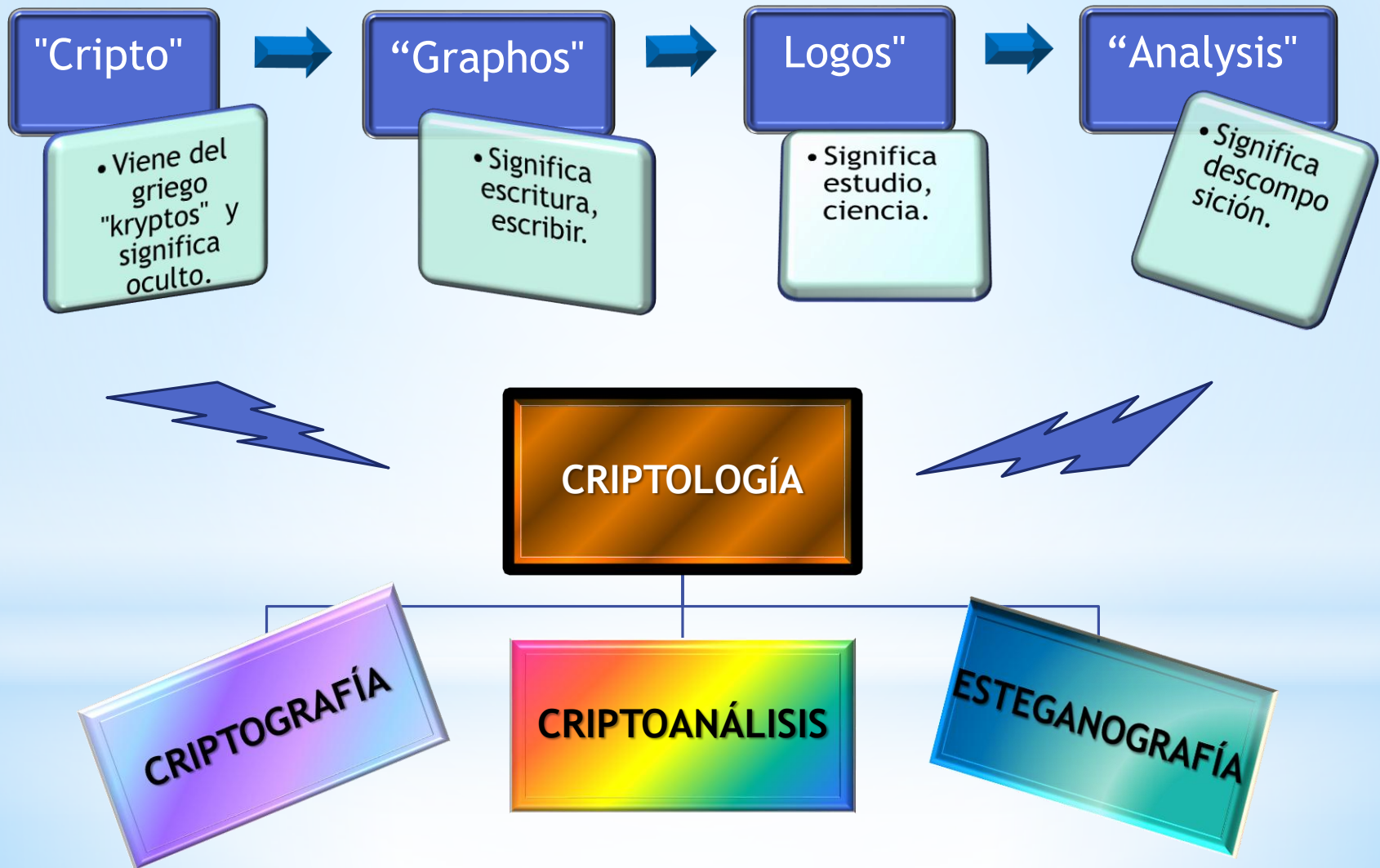
1. Estudiar elementos básicos de la criptografía

Bibliografía

Lucena López, Manuel. Criptografía y seguridad en computadores, 4ta edición, 2010.

Ramió Aguirre, Jorge. Seguridad informática y criptografía, 6ta edición, 2006.

INTRODUCCIÓN

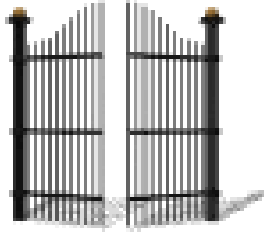


INTRODUCCIÓN

CRIPTOGRAFÍA



Es la ciencia de escribir mensajes que solo puedan ser legibles por el remitente y el destinatario previo conocimiento de la llave utilizada para el enmascaramiento.



CRIPTOANÁLISIS



Es la ciencia de descifrar y leer estos mensajes cifrados sin conocer la llave utilizada por el remitente.



ESTEGANOGRAFÍA



Es la disciplina en la que se estudian y aplican técnicas que permiten el ocultamiento de mensajes u objetos, dentro de otros, llamados portadores, de modo que no se perciba su existencia.

La Real Academia Española define criptografía como:

"EL ARTE DE ESCRIBIR CON CLAVE SECRETA O DE MODO ENIGMÁTICO".

ARTE:

La criptografía ha dejado de ser un arte: es una ciencia.

ESCRITURA:

No sólo se escriben mensajes; se envían o se guardan en un computador diversos tipos de documentos con distintos formatos (txt, doc, exe, jpg, ...).

**UNA CLAVE:
CLAVE
SECRETA:**

Los sistemas actuales usan una o dos claves.

**MODO
ENIGMÁTICO:**

Existirán sistemas de clave secreta que usan una sola clave y sistemas de clave pública que usan dos: una clave privada (secreta) y la otra pública.

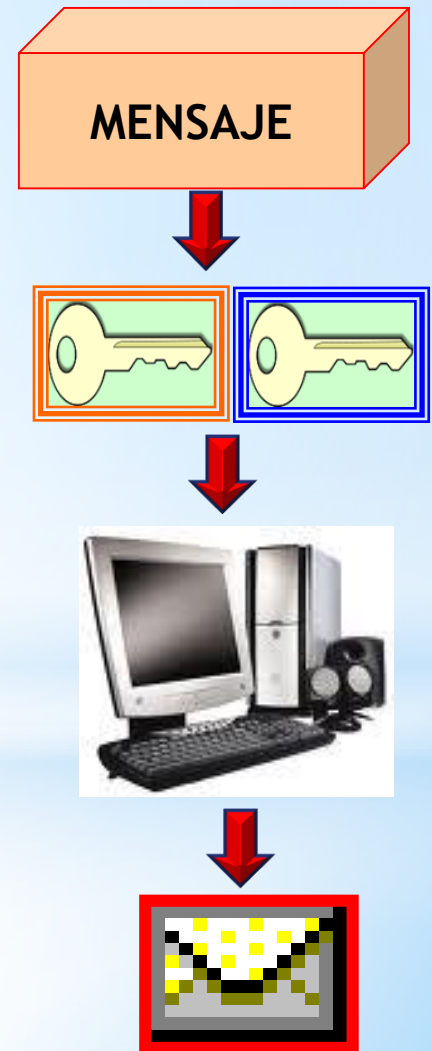
La representación binaria de la información podría ser enigmática para nosotros los humanos pero no para las computadoras. Es su lenguaje natural.

Desarrollo

Una definición más técnica de criptografía sería:

La Criptografía es una Ciencia.

Rama inicial de las Matemáticas y en la actualidad de la Informática y la Telemática, que hace uso de métodos y técnicas con el objeto principal de cifrar y/o proteger un mensaje o archivo por medio de un algoritmo, usando una o más claves. Esto da lugar a diferentes tipos de sistemas de cifra, denominados criptosistemas, que nos permiten asegurar tres de los cuatro aspectos básicos de seguridad informática: la **confidencialidad o secreto, la integridad o autenticidad, y el no repudio de emisor y de receptor.**



HISTORIA DE LA CRIPTOGRAFÍA

**Niños y adultos
gustan (o necesitan)
de secretos.**



**El origen del baile de máscaras
fue la necesidad de esconder la
propia identidad - en este caso la
llave es la fantasía y la máscara.**



**Hoy día la criptografía
volvió a ser muy utilizada
debido a la evolución de
los medios de
comunicación, a la
facilidad de acceso a estos
medios y al volumen muy
grande de mensajes
enviados.**

**Debido a esto, la
criptografía evolucionó
mucho en los últimos
tiempos y se ha convertido
en una herramienta
imprescindible para los
medios de comunicación.**

HISTORIA DE LA CRIPTOGRAFÍA

- La criptografía es una ciencia muy antigua, cuyas primeras manifestaciones históricas se remontan al Antiguo Egipto y datan de hace más de 4000 años.
- Las matemáticas son todavía más antiguas y su origen se entremezcla con el de la humanidad como especie inteligente. Sin embargo, hasta hace muy poco tiempo ambas disciplinas no convergieron, un hecho que cambió profundamente la criptografía, que hoy en día puede, en gran medida, ser considerada como una disciplina matemática

HISTORIA DE LA CRIPTOGRAFÍA

- Una de las razones por las que la criptografía ha permanecido aislada de las matemáticas durante tanto tiempo es que, al ser su utilización tradicional la de comunicarse en secreto, fue hasta tiempo muy reciente un patrimonio casi exclusivo de las organizaciones de inteligencia que operan en los ámbitos militar y diplomático.
- Aún a principios de los años 70 del siglo pasado, la criptografía no existía como disciplina académica y era muy difícil adquirir conocimientos sobre la misma porque casi todo el material criptográfico que tenía algún interés estaba clasificado.

HISTORIA DE LA CRIPTOGRAFÍA

- Esta fue la situación con la que se encontraron los pioneros como W. Diffie, M. Hellman, R. Merkle y R. Rivest, que estaban interesados en la criptografía y en su uso civil pero encontraban todo tipo de dificultades e incluso amenazas cuando pretendían desarrollarla.
- No sólo la criptografía se usaba para guardar los “secretos de estado” sino que ella misma era un gran secreto.
- Hoy en día, las cosas han cambiado mucho y, aunque siguen existiendo organizaciones poderosas que mantienen sus conocimientos criptográficos en secreto, la criptografía es una disciplina con un gran desarrollo en el ámbito académico y, está estrechamente vinculada a las matemáticas.

HISTORIA DE LA CRIPTOGRAFÍA

La Criptografía moderna nace al mismo tiempo que las computadoras.

Durante la Segunda Guerra Mundial, 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 alemán 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 cambiarían para siempre el curso de la Historia.

Máquina Enigma

Máquina de rotores que permitía usarla tanto para cifrar como para descifrar mensajes.

Fue patentada en 1918 por la empresa alemana Scherbius & Ritter, cofundada por Arthur Scherbius , quien había comprado la patente de un inventor neerlandés, y se puso a la venta en 1923 para un uso comercial.

En 1926, la Armada alemana la adopta para uso militar y poco después su uso se extendió a las demás fuerzas armadas alemanas, siendo su uso extendido antes de y durante la IIGM.

Máquina Enigma

Su facilidad de manejo y supuesta inviolabilidad fueron las principales razones para su amplio uso.

Gracias a las investigaciones llevadas a cabo por los servicios de inteligencia polacos, fue finalmente descubierto y la lectura de la información que contenían los mensajes supuestamente protegidos es considerado como una de las causas de haber podido concluir la IIGM al menos dos años antes de lo que hubiera acaecido sin su descifrado.

Máquina Enigma

A pesar de tener algunas debilidades criptográficas, el descifrado se facilitó por fallos de procedimientos y uso por parte de los operadores alemanes, como el no desarrollar modificaciones continuas en el cifrado, además de la captura, por parte de los Aliados, de tablas de descifrado y las propias máquinas.



HISTORIA DE LA CRIPTOGRAFÍA

Desde entonces hasta hoy

- crecimiento espectacular de la tecnología criptográfica.
- 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 *pedra angular de asuntos tan importantes como el comercio electrónico, la telefonía móvil, o las nuevas plataformas de distribución de contenidos multimedia.*
- muchos claman por la disponibilidad pública de la Criptografía. La experiencia ha demostrado que la única manera de tener buenos algoritmos es que estos sean accesibles, para que puedan ser sometidos al escrutinio de toda la comunidad científica

HISTORIA DE LA CRIPTOGRAFÍA

- La seguridad no debe basarse en mantener los algoritmos ocultos sino en su resistencia demostrada tanto teórica como prácticamente, y la única manera de demostrar la fortaleza de un algoritmo es sometiéndolo a todo tipo de ataques.
- Otro aspecto es la longitud de las claves. Por ejemplo, el algoritmo DES tenía 2^{56} posibles claves. Probarlas todas si, dispusiéramos de un computador capaz de hacer un millón de operaciones por segundo tardaría. ¡más de 2200 años! Pero si la clave tuviera 128 bits, el tiempo requerido seria de 10^{24} años.

Etapas de desarrollo de la Criptografía

1. Hasta la II Guerra Mundial : cifrados clásicos.
2. Desde la II Guerra Mundial hasta los años 70: intensa comunicación radial. Cifradores electrónicos. Shannon – Fundador de la Criptografía como ciencia
3. Desde los años 70 : Aumento brusco de la demanda de protección de la información . Redes electrónicas de comunicación. La Criptografía es utilizada fuera del sector estatal. Conferencias y publicaciones abiertas. Masiva atracción o participación de matemáticos profesionales

Hitos históricos en la criptografía

- La criptografía clásica abarca desde tiempos inmemoriales hasta la mitad del siglo XX.
- El punto de inflexión en esta clasificación la marcan tres hechos relevantes:
 - En el año 1948 se publica el estudio de Claude Shannon sobre la Teoría de la Información.
 - En 1974 aparece el estándar de cifra DES.
 - Y en el año 1976 se publica el estudio realizado por Whitfield Diffie y Martin Hellman sobre la aplicación de funciones matemáticas de un solo sentido a un modelo de cifra, denominado cifrado con clave pública.

Cifrados clásicos

1. Primer cifrador por transposición: escítala
2. Primer cifrador por sustitución: Polybios
3. El cifrador del César - Es un cifrador por sustitución monoalfabético en el que las operaciones se realizan módulo n , siendo n el número de elementos del alfabeto (en aquel entonces el latín).
4. El cifrador de Vigenère
5. Cifrador poligrámico de Playfair
6. El cifrador de matrices de Hill
7. El cifrador de Vernam

Herramientas de la criptografía clásica

Tanto máquinas, artilugios de cifra, como los algoritmos que trabajaban matemáticamente dentro de un cuerpo finito n , hacen uso de dos técnicas básicas orientadas a caracteres y que, muchos siglos después, las propondrá Shannon como herramientas para fortalecer la cifra:

Herramientas de la criptografía clásica

Técnicas de sustitución: Los caracteres o letras del mensaje en claro se modifican o sustituyen por otros elementos o letras en la cifra. El criptograma tendrá entonces caracteres distintos a los que tenía el mensaje en claro.

Técnicas de transposición o permutación: los caracteres o letras del mensaje en claro se redistribuyen sin modificarlos y según unas reglas, dentro del criptograma. El criptograma tendrá entonces los mismos caracteres del mensaje en claro pero con una distribución o localización diferente.

Conceptos básicos

TEXTO
CLARO



Información original que debe protegerse.

INFORMACIÓN



TEXTO
CIFRADO



Información ilegible que se obtiene después de cifrar un texto claro.

YTJHND DHD

CIFRADO



Que está escrito en clave. Operación consistente en escribir un mensaje con cifras. Proceso de convertir el texto claro en texto cifrado.

INFORMACIÓN



YTJHND DHD

DESCIFRADO



Conjunto de palabras que componen un escrito. Proceso de convertir el texto cifrado en texto claro.

YTJHND DHD



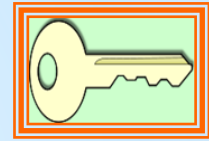
INFORMACIÓN

CONCEPTOS BÁSICOS

CLAVE Ó
LLAVE



Información **SECRETA** que se utiliza durante el proceso de Cifrado ó Descifrado de los mensajes. Solo es de conocimiento del Emisor y el Receptor. En los criptosistemas asimétricos existe la llave publica que es de total conocimiento.

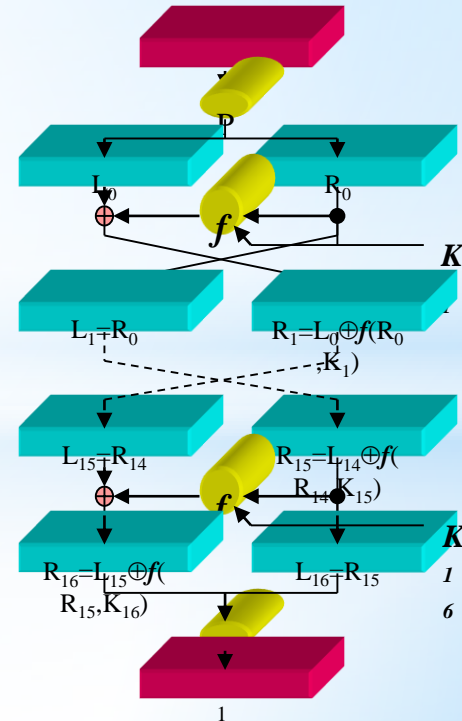


ALGORITMO
CRIPTOGRÁFICO



Conjunto de reglas operatorias cuya aplicación permite resolver un problema mediante un número finito de operaciones.

Un algoritmo criptográfico es un conjunto de operaciones matemáticas bien definidas y finitas que utilizando una llave convierte un mensaje original en claro en un mensaje cifrado.



Criptosistema

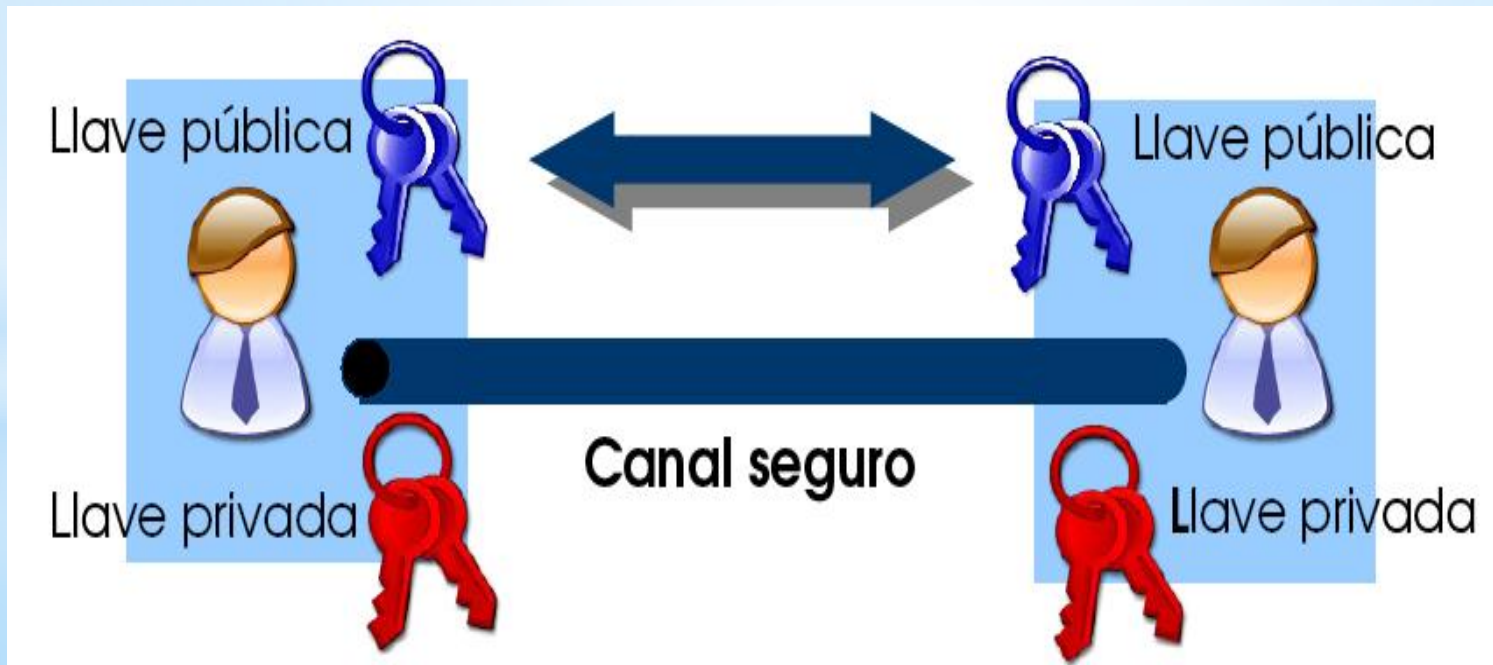
Es una quintupla (M, C, K, E, D) , donde:

- M representa el conjunto de todos los mensajes sin cifrar (lo que se denomina texto claro, o *plaintext*) 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 .

CRIPTOSISTEMAS ASIMÉTRICOS



Sistema Criptográfico donde cada usuario crea un par de claves, una privada y otra pública, inversas dentro de un cuerpo finito. Lo que se cifra en emisión con una clave, se descifra en recepción con la clave inversa. Se conoce como criptografía de Llave Pública.



CRIPTOSISTEMAS SIMÉTRICOS



Sistema criptográfico donde la clave para descifrar un criptograma (K') se calcula a partir de la clave (K) que se utilizó para cifrar el texto en claro, y viceversa.

Lo habitual en los criptosistemas de este tipo es que ambas claves (K y K') coincidan, es decir, que se utilice la misma clave para cifrar un mensaje y para su descifrado.

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 como transmitir la clave de forma segura.

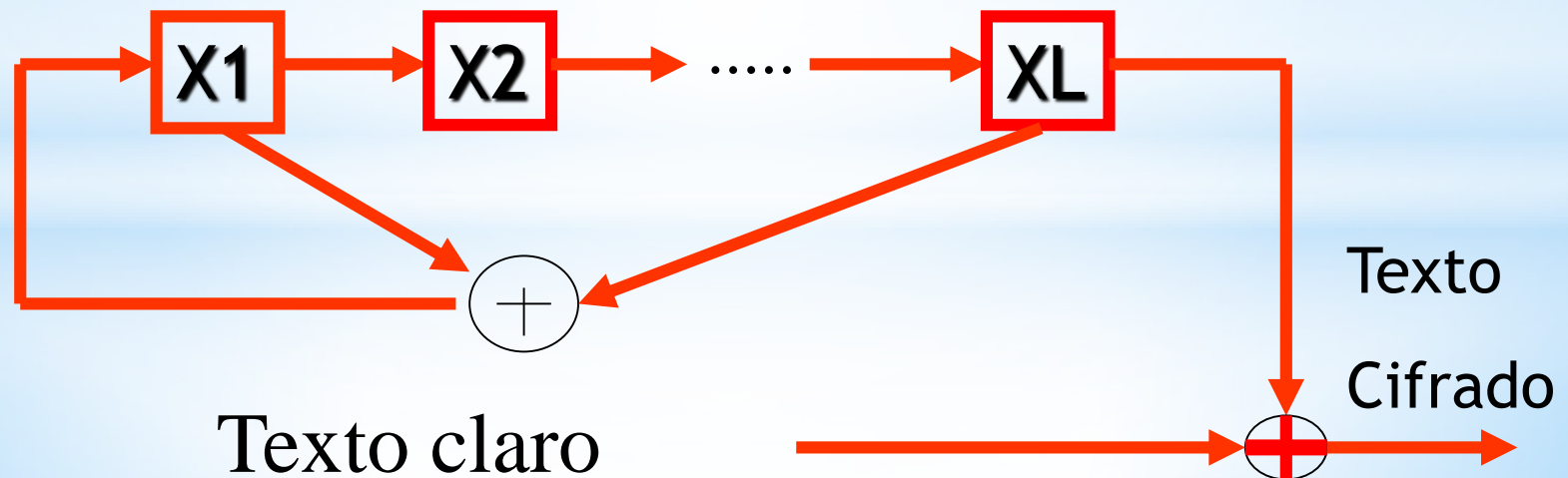
CIFRADO SIMÉTRICO

Una gran parte de los algoritmos de cifrado simétrico operan dividiendo el mensaje que se pretende codificar en bloques de tamaño fijo y aplican sobre cada uno de ellos una combinación más o menos compleja de operaciones de confusión —sustituciones— y difusión —transposiciones—. Estos algoritmos se denominan, en general, cifrados por bloques.

En muchos casos el criptosistema no es más que una operación combinada de sustituciones y permutaciones, repetida n veces.

CIFRADO EN FLUJO

Es el proceso de cifrado donde la sucesión aleatoria es generada por un algoritmo criptográfico que se alimenta de una llave. A este algoritmo criptográfico se le conoce también como generador de la secuencia pseudo aleatoria o generador del stream de llave (Keystream generator).



CIFRADO EN BLOQUES

Un algoritmo criptográfico de cifrado en bloques es aquel que tiene las siguientes características.

Características de los cifrados por bloques :

1. Los textos claros y cifrados están formados por bloques de n bits cada uno.
2. El algoritmo de cifrado usa una llave fija para todos los textos claros formando una permutación de grado elevado (2^n) para cada llave.

Propiedades necesarias en el diseño de algoritmos criptográficos

DIFUSIÓN



Transformación sobre el texto claro con el objeto de dispersar las propiedades estadísticas del lenguaje sobre todo el texto cifrado. Se utilizan las transposiciones o permutaciones.

CONFUSIÓN



Transformación sobre el texto claro con objeto de mezclar los elementos de éste, aumentando la complejidad de la dependencia funcional entre la llave y el texto cifrado. Se utilizan las sustituciones.

IDEAS

- El AES tiene una estructura algebraica bastante sencilla, que se basa en la aritmética del campo finito $GF(2^8)$
- Una de las ideas de Diffie y Hellman es la de construir criptosistemas cuyo criptoanálisis sea, en la medida de lo posible, equivalente a la resolución de un problema matemático difícil.
- La idea fue utilizar problemas computacionales difíciles, en el sentido de que, aun conociendo algoritmos para resolverlos, no podemos hacerlo por no ser factible ejecutarlos en tiempo razonable.

Gracias