



Como crear conciencia de seguridad



1. Establecer los conocimientos básicos de la Criptología.
2. Crear conciencia de seguridad

Alguien conoce la Historia de la Criptología

- La máquina ENIGMA.



Sumario

- 1) Introducción a la Criptología
- 2) Criptografía y criptoanálisis

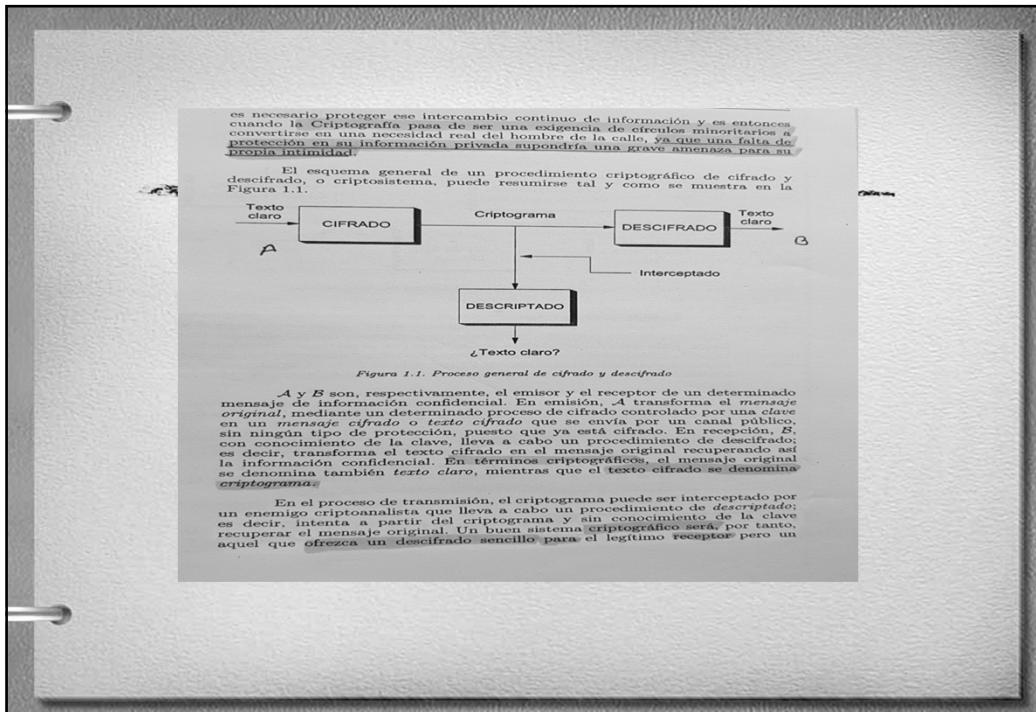
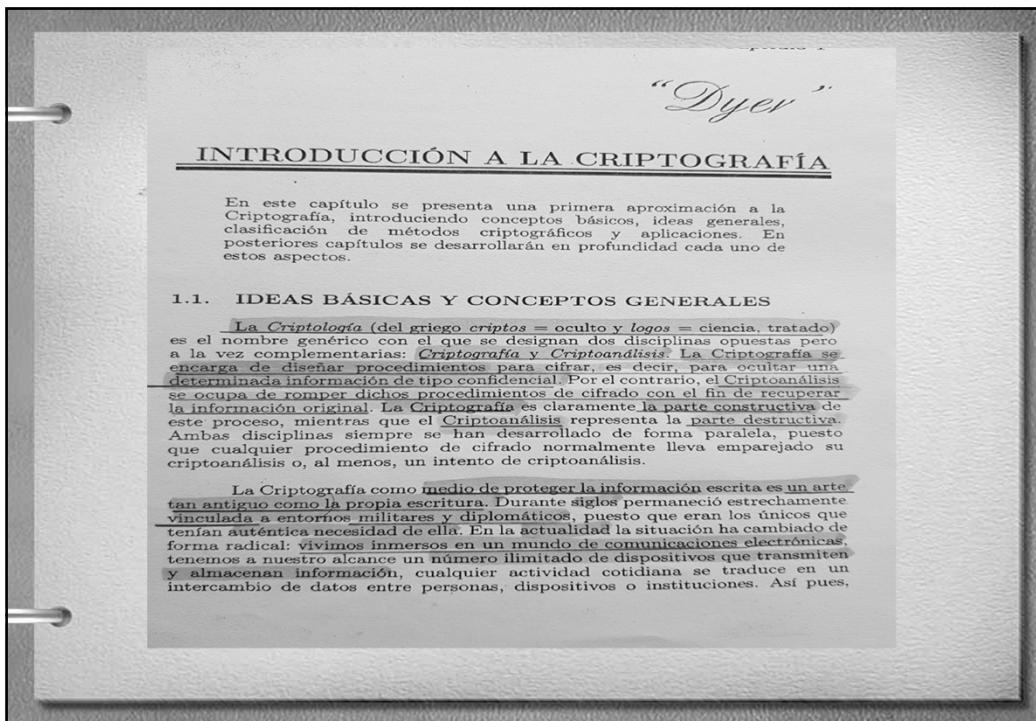


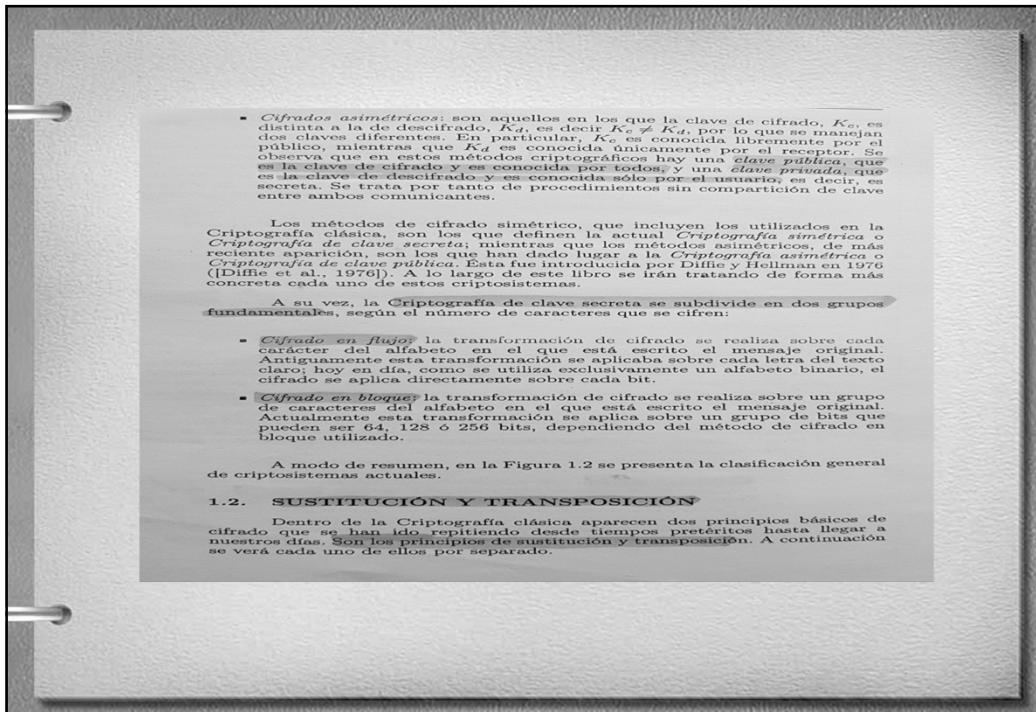
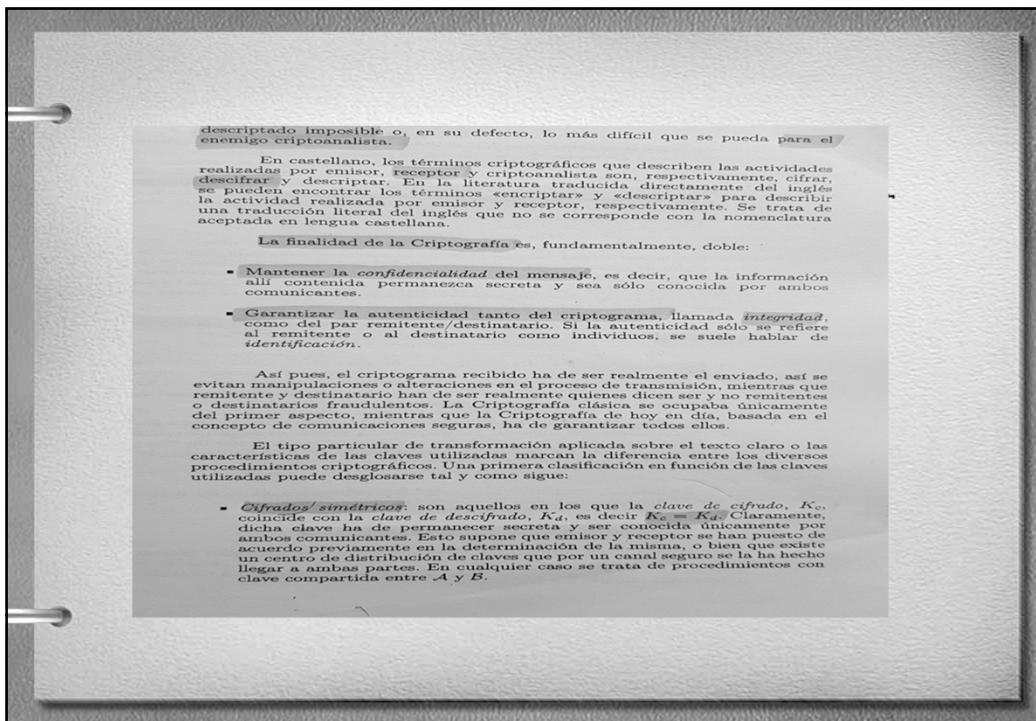
Criptología

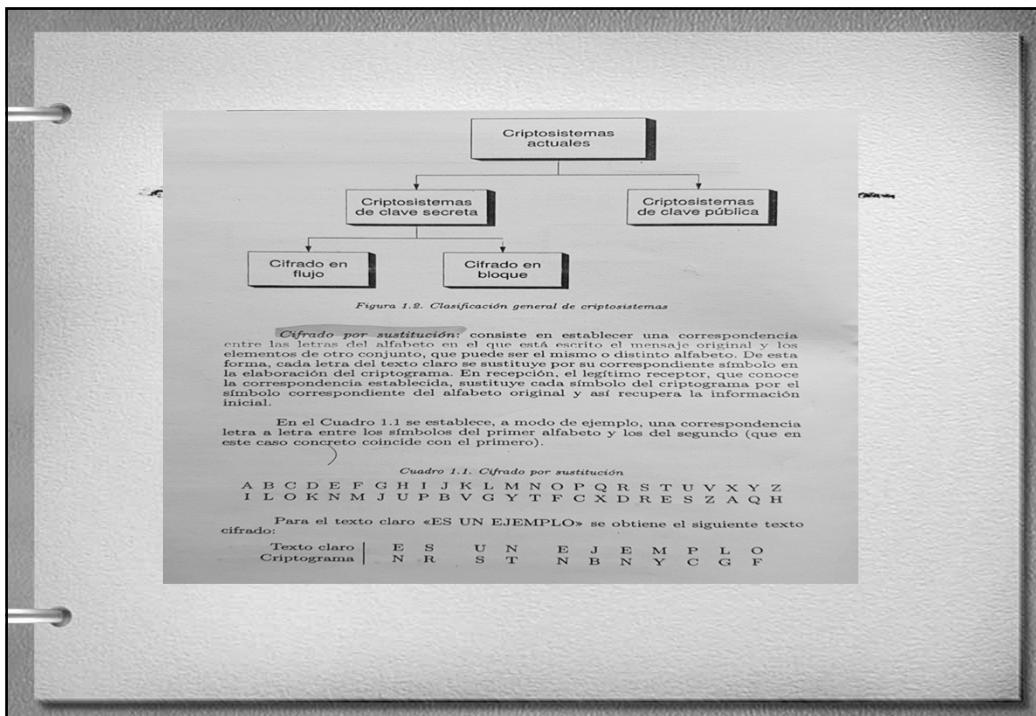
La **criptología** (del griego *krypto*: 'oculto' y *logos*: 'estudio') es, tradicionalmente, la disciplina que se dedica al estudio de la escritura secreta, es decir, estudia los mensajes que, procesados de cierta manera, se convierten en difíciles o imposibles de leer por entidades no autorizadas.

Criptografía y Criptoanálisis

1. *Se ocupa del estudio de los algoritmos, protocolos y sistemas que se utilizan para proteger la información y dotar de seguridad a las informaciones. (crear claves)*
2. *Se dedica al estudio de sistemas criptográficos con el fin de encontrar debilidades en los sistemas y romper su seguridad sin el conocimiento de información secreta. (Romper claves)*







Cifrado por el sustituto: consiste en establecer una correspondencia entre las letras del alfabeto, en el que está escrito el mensaje original y los elementos dentro del mismo, que pueden ser el mismo alfabeto (cifrado), o bien, cada letra del texto claro es sustituida por su correspondiente simbolo en la elaboración del criptograma. En efecto, el legítimo receptor que conoce la correspondencia establecida, sustituye cada simbolo del criptograma por el simbolo correspondiente del alfabeto original y así recupera la información inicial.

En el Cuadro 1.1 se establece, a modo de ejemplo, una correspondencia letra a letra entre los símbolos del primer alfabeto y los del segundo (que en este caso concreto coincide con el primero).

Cuadro 1.1. Cifrado por sustitución

Para el texto claro «ES UN EJEMPLO» se obtiene el siguiente texto cifrado:

Texto claro	E	S	U	N	E	J	E	M	P	L	O
Criptograma	N	R	S	T	N	B	N	Y	C	G	F

En este caso la clave es la correspondencia entre los dos alfabetos, que tiene que ser conocida únicamente por ambos comunicantes. La debilidad de estos métodos radica en que la clave es fija y no se refleja adecuadamente en el criptograma. Conociendo las letras de mayor frecuencia en el alfabeto utilizado puede inferirse la correspondencia establecida en la clave.

Como ejemplos literarios de este tipo de criptoanálisis pueden citarse el relato de Edgar A. Poe *El escarabajo de oro* ([Poe, 1996]) y *La aventura de los hombres danzantes* de Sir Arthur Conan Doyle, dentro de la serie de relatos de Sherlock Holmes ([Doyle, 2008]).

El método clásico de cifrado por sustitución más conocido es el *cifrado de César* (siglo I a. C.), que sustituía la primera letra del alfabeto latino, A, por la cuarta, D; la segunda, B, por la quinta, E, y así sucesivamente con todas las demás. Para una visión en profundidad sobre procedimientos clásicos de sustitución, el lector interesado puede remitirse a [Fuster Sabater et al., 2004] [Kahn, 1967] y [Sgarro, 1990].

Algunas veces se presenta un ejemplo sencillo; se divide el mensaje original en grupos de 4 letras y se permuta el orden de las mismas, de modo que las características que definen este cifrado por transposición son:

Grupos de: 4 letras. Transposición: 1234 → 4321.

Es decir, las letras de cada uno de los grupos se escriben en orden inverso. Para el mensaje original «**CRYPTOGRAFIA**» se obtiene el siguiente criptograma:

Texto claro | C R I P T O G R A F I A

Criptograma | P I R O G O T A
En este caso la clave secreta es el número de letras en cada grupo y orden en el que se coloca cada una de ellas. El conocimiento de la clave permite al emisor barajar las letras del mensaje y al receptor el poder recolocarlas en su lugar de origen. Como referencia, clasifico de cifrado por transposición, puede rescribirse la escifra lademónica, que data del siglo v a. C. La escifra era una vara o bastón de la que se preparaban dos ejemplares idénticos (del mismo diámetro) y alrededor de la cual se envolvía una tira de pergamo. P

