Fundamentos de criptografía

Garantía y Seguridad de la Información.

Criptografía

- La palabra *criptografía* viene del griego *cripto* (ocultar) y *graphos* (escribir).
  - **escribir mensajes ocultos.**
- La criptografía consiste en
  - tomar el documento original
  - aplicarle un **algoritmo con una clave** y obtener un nuevo documento que no se puede entender

- La **clave del algoritmo**: un conjunto de valores que, combinados con el documento original como se indica en el algoritmo, generan un documento cifrado del que es imposible deducir ni el documento original ni la clave utilizada.
  - El destinatario sabe aplicar el algoritmo y la clave para recuperar el documento original.

La clave es la clave

- Combinaciones de símbolos (letras, números, signos de puntuación, etc.).
- **Ataques de fuerza bruta:** probar todas las combinaciones posibles de símbolos.
- Medidas de seguridad:
  - **Utilizar claves de gran longitud** (512-1024-2048-4096 bytes): el atacante necesita muchos recursos computacionales.
  - **Cambiar regularmente la clave.** Si alguien intenta cubrir todo el rango de claves, le limitamos el tiempo para hacerlo.
  - **Utilizar todos los tipos de caracteres posibles**
  - **No utilizar palabras fácilmente identificables:** palabras de diccionario, nombres propios, etc.
  - **Detectar repetidos intentos fallidos en un corto intervalo de tiempo.**

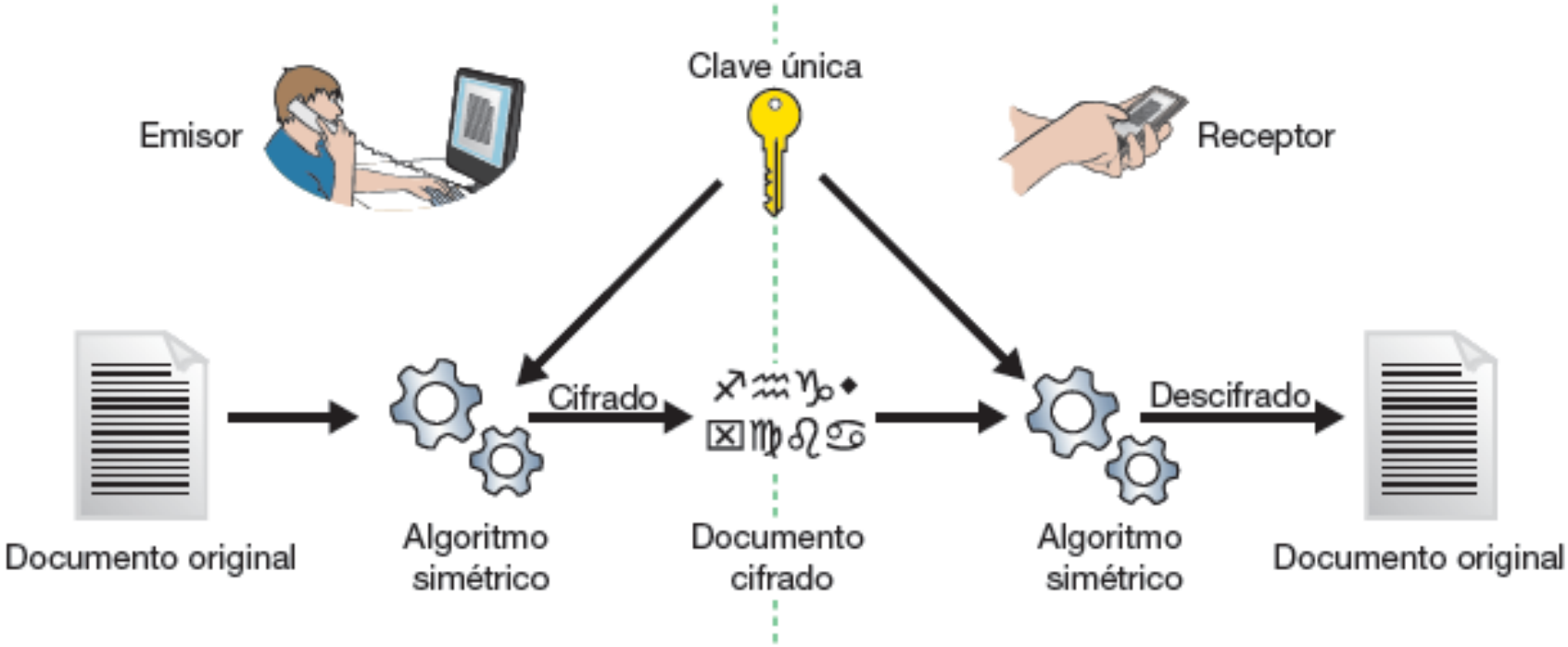
Criptografía clásica

- Todos los sistemas de cifrado anteriores a la II Guerra Mundial, o lo que es lo mismo, al nacimiento de los ordenadores.
- Se basa en algoritmos sencillos y claves muy largas para la seguridad.
- Perdieron su eficacia, debido a que son fácilmente **criptoanalizables** por los ordenadores.
- Todos los algoritmos criptográficos clásicos son simétricos

Algoritmos simétricos

- Utilizan la **misma clave** para cifrar y descifrar.
- Son sencillos de utilizar y resultan bastante **eficientes**
- Los más utilizados actualmente son DES, 3DES, AES, Blowfish e IDEA.
- El funcionamiento es simple:
  - el emisor toma un documento y le aplica el algoritmo, usando la clave única, que también conoce el receptor.
  - el receptor recibe el documento cifrado, le aplica el mismo algoritmo con la misma clave, pero ahora en función de descifrar.
- Si el documento cifrado no ha sido alterado en el camino y la clave es la misma, el resultado será el documento original.

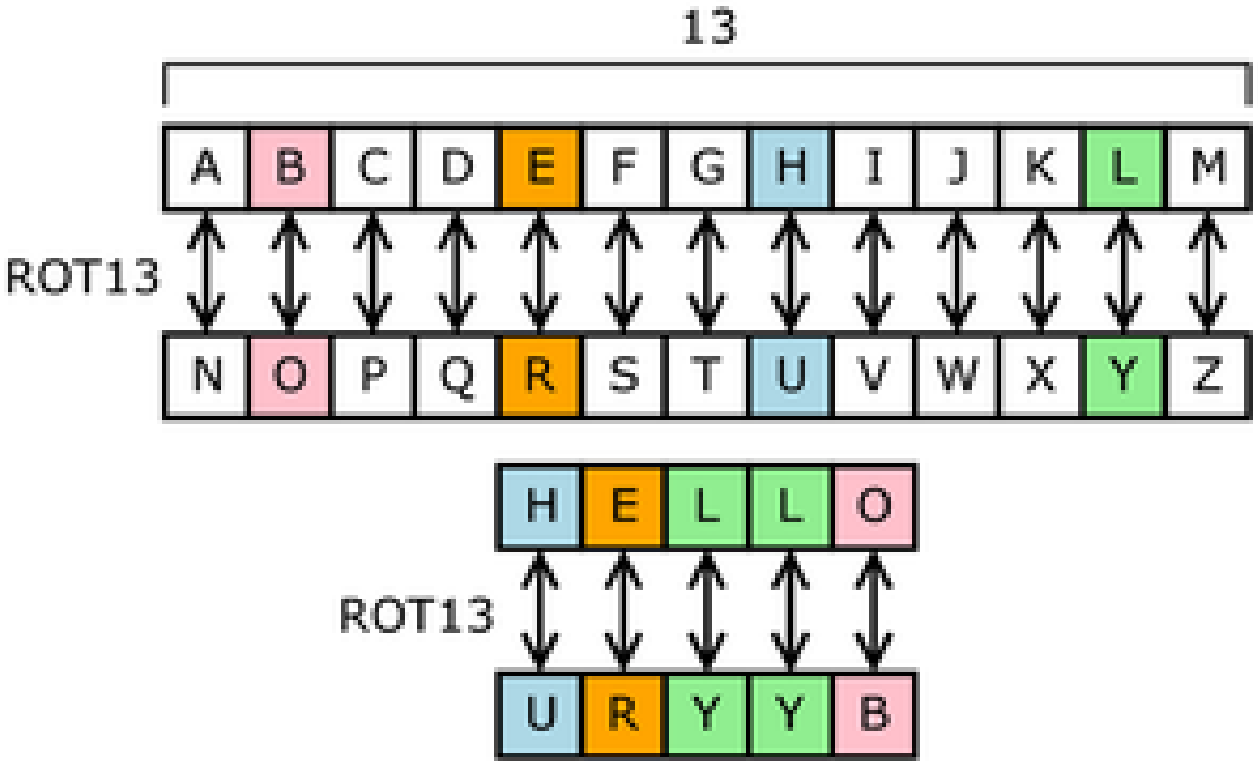
Algoritmos simétricos



Técnicas clásicas

- *SUSTITUCIÓN*
  - Los caracteres del mensaje original se intercambian por otros que pueden ser del mismo alfabeto o de uno diferente.
  - La sustitución causa **confusión**
    - oculta la relación que existe entre el texto claro y el texto cifrado.

Técnicas clásicas. Sustitución



Técnicas clásicas

- *TRASPOSICIÓN*
  - Se intercambian de lugar los caracteres que conforman un mensaje
  - el criptograma contiene los mismos caracteres que el mensaje en claro pero resultan incomprensibles a simple vista ya que están desordenados.
  - causa **difusión**
    - elimina la redundancia (demasiada abundancia de las mismas palabras).

Técnicas clásicas. Trasposición

Utilizando la permutación 24531, el mensaje
“MANOS ARRIBA ESTO ES UN ATRACO”,
se transforma en
“AOSNM RIBRA ETOSA SNAUE RCOAT”

Algoritmos que usan sustitución

- Sustitución de cada letra por otra letra para disfrazarla pero conservando el orden de los símbolos de texto normal.
- Los más importantes:

  - algoritmo de César,
  - métodos de cifrado monoalfabéticos,
  - métodos polialfabéticos..

Algoritmo de César

- Era usado por Julio César para enviar mensajes secretos
- 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.
- Este algoritmo no posee clave, puesto que la transformación siempre es la misma.
- Para descifrar basta con restar 3 al número de orden de las letras del criptograma.

Métodos de cifrado monoalfabéticos (I)

- Sustituyen cada letra por otra que ocupa la misma posición en un **alfabeto desordenado** y esta correspondencia se mantiene a lo largo de todo el mensaje.

- El *problema* está en cómo recordar la clave (el alfabeto desordenado).

Métodos de cifrado monoalfabéticos (II)

- El procedimiento es el siguiente:
  1. Se busca una palabra (clave) fácil de recordar y se le quitan las letras duplicadas.

     SEGURIDAD $\Rightarrow$ SEGURIDA
  2. Se añaden al final de la palabra las restantes letras del alfabeto (sin duplicar letras).

     SEGURIDABCFH.....XYZ

Métodos de cifrado monoalfabéticos (III)

3. Se ordenan en una matriz cuya primera fila es la palabra clave

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

4. El nuevo alfabeto se lee por columnas:
   SBNYECOZGFPUHQRJTIKVDLWAMX

- ¿En qué se convertiría el mensaje *ataque?*

Métodos de cifrado polialfabéticos (I)

- Corresponde a la aplicación cíclica de **n** cifrados monoalfabéticos (con varios abecedarios desordenados).
- A una letra de un mensaje le pueden corresponder tantas asignaciones como alfabetos cifrados se quieran emplear.
- Para encriptar el texto se cambia de uno a otro alfabeto cifrado según se pasa de una letra del texto en claro a otra.

Métodos de cifrado polialfabéticos (II)

- Un ejemplo es el Cifrado de De Vigenère (1523):
  - La plantilla de cifrado se compone de un alfabeto en claro de n caracteres bajo el que se distribuían n alfabetos cifrados, cada uno de ellos desplazados una letra a la izquierda

Cifrado de De Vigenére

A	B	C	D	E	F	G	H	I	J	…
B	C	D	E	F	G	H	I	J	K	…
C	D	E	F	G	H	I	J	K	L	…
D	E	F	G	H	I	J	K	L	M	…
E	F	G	H	I	J	K	L	M	N	…
F	G	H	I	J	K	L	M	N	O	…
G	H	I	J	K	L	M	N	O	P	…
H	I	J	K	L	M	N	O	P	Q	…
I	J	K	L	M	N	O	P	Q	R	…
J	K	L	M	N	O	P	Q	R	S	…
…	…	…	…	…	…	…	…	…	…	…

BECADA:
Correspondencia de B en la fila 2: C
Correspondencia de E en la fila 3: G
Correspondencia de C en la fila 4: F
Correspondencia de A en la fila 5: E
Correspondencia de D en la fila 6: I
Correspondencia de A en la fila 7: G

CGFEIG

Cifrado de De Vigenére mejorado

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

M. Original	A	T	A	C	A	D	E	L	L	U	N	E	S
Clave	A	D	I	O	S	A	D	I	O	S	A	D	I
M. Cifrado	A	W	I	Q	S	D	H	T	Z	M	N	H	A

AWIQSD HT ZMNHA

Algoritmos que usan trasposición

- Utilizan la técnica de *permutación:* los caracteres del texto **se reordenan** mediante un algoritmo específico.
- Transmitir el mensaje en bloques de cinco caracteres, reordenados (permutados) según la clave 43521:
  - el cuarto carácter del bloque en claro se trasmite primero, luego el tercero, después el quinto, luego el segundo y, por último, el primero.
  - Esto se repetirá en cada bloque de 5 caracteres del mensaje.
- Los caracteres del criptograma son exactamente los mismos que los del texto en claro

Cifrados por trasposición

- Cifrar mediante trasposición de bloques de cinco caracteres el siguiente mensaje, usando la permutación 43521.

  M = AL GRITO DE VIVA ZAPATA SE ARMÓ UNA GORDA.

  M = ALGRI TODEV IVAZA PATAS EARMO UNAGO RDAXX

  C = RGILA EDVOT ZAAVI ATSAP MROAE GAONU XAXDA

Principios de Shannon

- **Confusión:** ocultar la relación que existe entre el texto normal, el texto cifrado y la clave, realizando sustituciones simples
  - la relación entre el texto cifrado y la clave debe ser lo más compleja posible
    - **Sustitución:** sustituir cada elemento de un texto en claro por otro u otros elementos en el texto cifrado.

Principios de Shannon

- **Difusión:** repartir la influencia de cada carácter del mensaje original lo más posible en el mensaje cifrado, realizando permutaciones
  - dispersar las propiedades estadísticas del lenguaje
    - **Transposición:** cambiar de posición en el texto cifrado los elementos correspondientes a un texto en claro.

El mejor secreto

- Libreta de un solo uso (*one-time pad)*
  - El texto en claro se combina con una **clave aleatoria** igual de larga que el texto en claro y sólo se utiliza una vez.
  - Si la clave es verdaderamente aleatoria, nunca se reutiliza y se mantiene en secreto
    - es indescifrable.

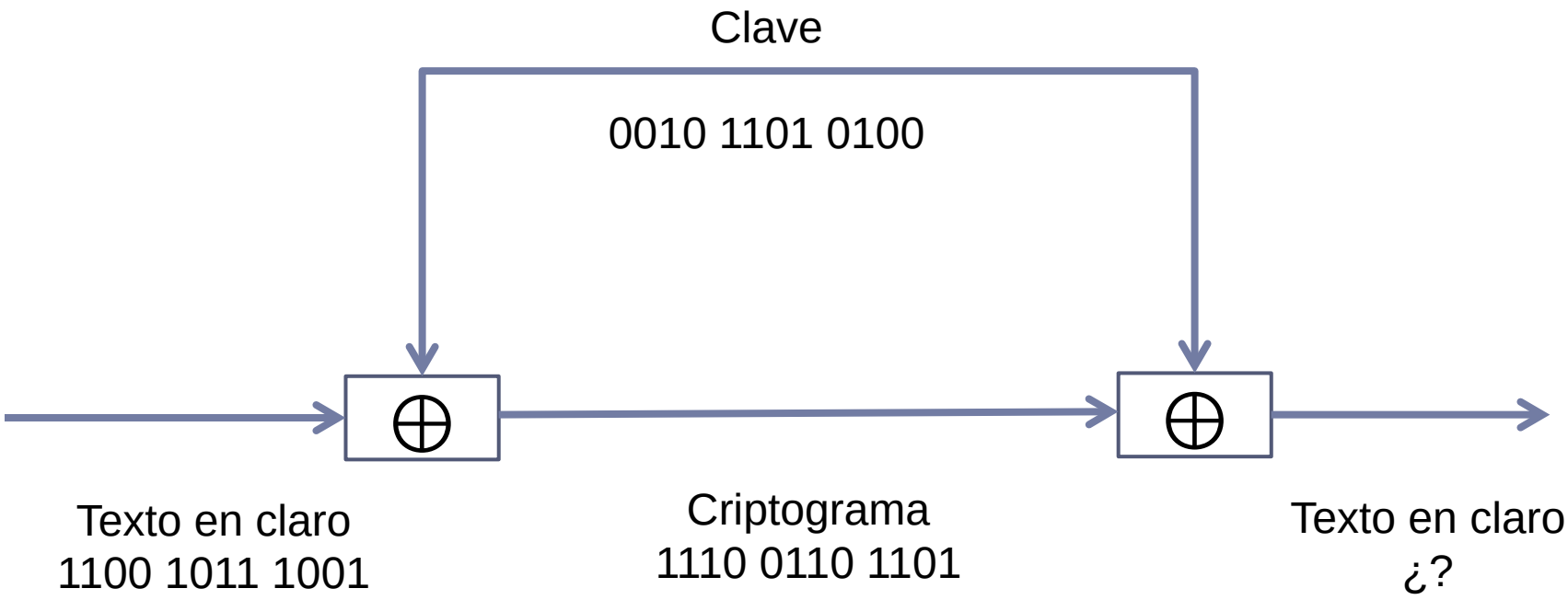
El mejor secreto

- Libreta de un solo uso
- Usar una clave continua para cifrar el texto en claro, carácter a carácter, y obtener el texto cifrado.
  - *Secreto perfecto*: el texto cifrado no da información acerca del texto en claro.
  - Fundamental:
    - Generación e intercambio de la LSU, seguras.
    - LSU tan larga como el mensaje

Cifrador de Vernam

- Representa cada carácter M_i con 5 bits en código Baudot
- Se suma or-exclusivo (XOR) con la clave k_i de una secuencia binaria aleatoria.
- Se obtiene
  - $C_i = M_i \oplus k_i$
  - $C = C_1C_2C_3\ldots C_n$

Cifrador de Vernam



Cifrador de Vernam

- Encriptar M = BYTES con la clave K = VERNAM

  B $\oplus$ V =

  Y $\oplus$ E =

  T $\oplus$ R =

  E $\oplus$ N =

  S $\oplus$ A =

  C =