Criptografía

Introducción
Cifradores, clasificación
Modos de encriptación

Criptografía

Es el estudio de técnicas matemáticas relacionadas con aspectos de seguridad de la información como confidencialidad, integridad de los datos, autenticación de entidad y autentificación del origen de los datos

Objetivos de la criptografía

- **Confidencialidad**: es un servicio utilizado para mantener el contenido de la información para todos aquellos que estén autorizados a tenerla.
- **Integridad de los datos**: se dice que la integridad de estos datos ha sido preservada cuando los datos no han sido alterados sin autorización desde que fueron creados, transmitidos o guardados por una fuente autorizada. Para poder asegurar la integridad de los datos, se requiere la habilidad de detectar su manipulación por quien no posee la autoridad para hacerlo. La manipulación o alteración de los datos incluye inserción, borrado o sustitución parcial o total.

Objetivos de la criptografía

- **Autenticación**: se asocia a la identificación. Por autenticación entenderemos cualquier método que nos permita comprobar de manera segura alguna característica sobre un objeto. Dicha característica puede ser su origen, su integridad, su identidad, etc.
- **No repudio**: se trata de que una vez enviado un mensaje, el emisor no pueda negar haber sido el autor de dicho envío. El no repudio es condición suficiente para la autenticidad, por lo que si un mensaje es no repudiable es auténtico, pero no al revés.

Criptosistema

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

- *M* es el conjunto de todos los mensajes sin cifrar (lo que se denomina texto plano, o plaintext) que pueden ser enviados
- *C* es el conjunto de todos los posibles mensajes cifrados, o criptogramas
- *K* es el conjunto de claves que se pueden emplear en el criptosistema

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.

Todo criptosistema ha de cumplir que:

$$D_k(E_k(m)) = m$$

Tipos de criptosistema

- ***Criptosistemas simétricos (clave privada)***
  - Emplean la misma clave *k* tanto para cifrar como para descifrar
  - Presentan el inconveniente de que para ser empleados en canales de comunicación la clave *k* debe estar tanto en el emisor como en el receptor, lo cual nos lleva a preguntarnos cómo transmitir la clave de forma segura.

Tipos de criptosistema

- **Criptosistemas asimétricos (clave pública)**
  - Emplean una doble clave: una clave privada k_{pr} y una clave pública k_{Pu}
  - Una sirve para la transformación *E* y la otra para la transformación *D*. En muchos casos son intercambiables.
  - Sabiendo k_{Pu} no se debe poder calcular k_{pr}
  - Pueden emplearse para establecer comunicaciones seguras por canales inseguros (ya que únicamente viaja por el canal la clave pública), o para autenticación.

Tipos de criptosistema

- **Criptosistemas híbridos**
  - Los criptosistemas de clave pública son muy costosos computacionalmente
  - Los criptosistemas de clave privada tienen problemas para la transmisión segura de claves
  - Entonces se pueden encriptar claves simétricas con algoritmos asimétricos y utilizar las claves simétricas para encriptar los mensajes

Ataques

- Son intentos de comprometer la seguridad de un criptosistema
- Pueden involucrar métodos computacionales o no
- Como en la actualidad hay disponibles métodos criptográficos muy fuertes, se debe prestar más atención a la posibilidad de ataques no computacionales que computacionales

Ataques

- Algunos ejemplos de ataques
  - Amenazas
  - Corrupción
  - Robo físico de claves
  - Instalación de keyloggers o cámaras de seguridad
  - Ingeniería social
  - Órdenes judiciales
  - Monitoreo de las emisiones electromagnéticas del teclado

Ataques

- **Ataque por fuerza bruta**: si se tiene un mensaje cifrado (criptograma), mediante este método se probarán todas las claves posibles para obtener el texto plano. Si el conjunto de posibles claves es alto este sistema es inviable. Es decir, se inspecciona la componente *K* del criptosistema. Normalmente a este tipo de ataques no se les suele considerar como una forma de criptoanálisis ya que no busca puntos débiles, sino que únicamente utiliza todas las claves posibles

Ataques

- **Criptoanálisis**
  - Son ataques que comprometen la seguridad de un criptosistema
  - Se asume que el algoritmo de cifrado es conocido, el ataque intenta descifrar mensajes transmitidos o la clave utilizada
  - Buscan explotar puntos débiles en el algoritmo o en la selección de la clave

Tipos de criptoanálisis

- **Ataque por texto plano escogido**: consiste en elegir varios textos planos y obtener sus criptogramas asociados. Esto implica tener acceso al medio de encriptación, pero no a la clave. O sea, se hace una inspección selectiva de la componente *M* del criptosistema.

Tipos de criptoanálisis

- **Ataque por texto plano**: el atacante tiene acceso a textos planos y a sus correspondientes criptogramas, pero no al medio de encriptación.

Tipos de criptoanálisis

- **Ataque por criptogramas**: el atacante tiene acceso a criptogramas generados por el criptosistema, pero no al medio de encriptación ni a sus textos planos correspondientes. Es posible que el atacante conozca alguna característica común a los textos planos, como el idioma de los mismos.

Tipos de criptoanálisis

- **Análisis de frecuencias**: se utiliza para romper sistemas criptográficos simétricos y se basa en estudiar la frecuencia con la que aparecen los distintos símbolos en un lenguaje determinado y luego estudia la frecuencia con la que aparecen en los criptogramas para establecer una relación entre ambos

Criptografía clásica

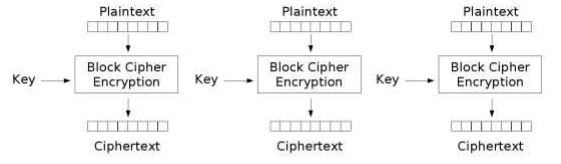
- Se denomina así a los sistemas de cifrado surgidos antes de la 2da Guerra Mundial, es decir, antes del nacimiento de las computadoras
- Todos los métodos clásicos son simétricos, ya que la criptografía asimétrica nació en los años 70

Criptografía clásica: clasificación

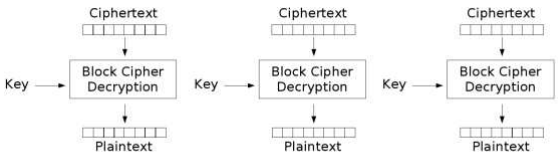
- Cifrados por bloque
  - Cifrados por sustitución
    - Sustitución simple o monoalfabéticos
    - Homofónicos
    - Polialfabéticos
    - Poligráficos
  - Cifrados por transposición
  - Cifrado de producto
- Cifrado de flujo
  - One Time Pad

Modos de encriptación por bloque

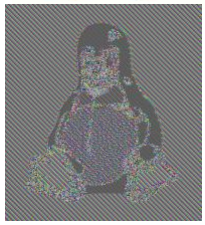
- **ECB (Electronic code book)**



Electronic Codebook (ECB) mode encryption

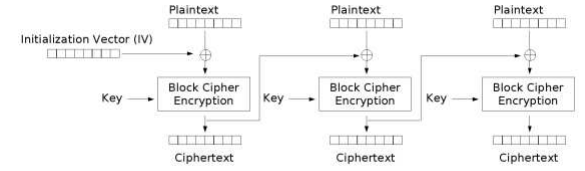


Electronic Codebook (ECB) mode decryption

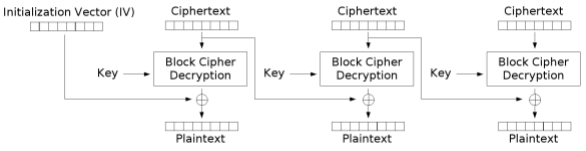


Modos de encriptación por bloque

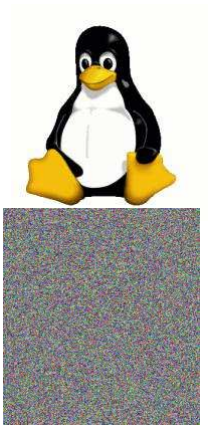
- **CBC (Cipher-block chaining)**



Cipher Block Chaining (CBC) mode encryption

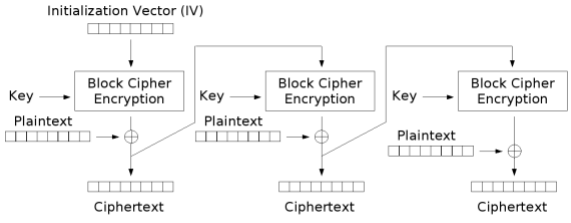


Cipher Block Chaining (CBC) mode decryption

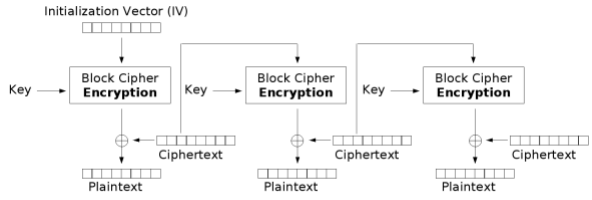


Modos de encriptación por bloque

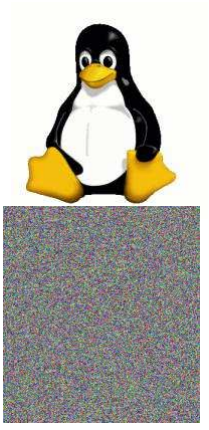
- **CFB (Cipher feedback)**



Cipher Feedback (CFB) mode encryption

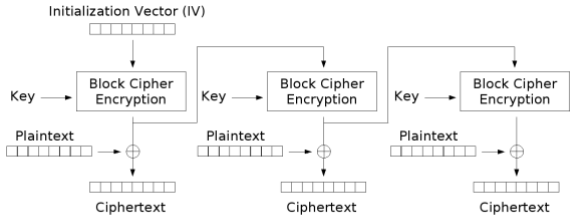


Cipher Feedback (CFB) mode decryption

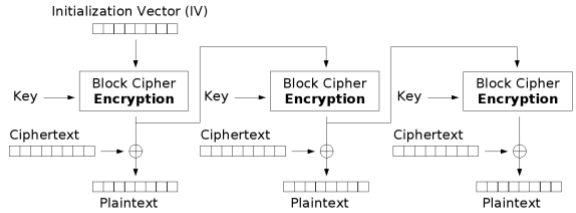


Modos de encriptación por bloque

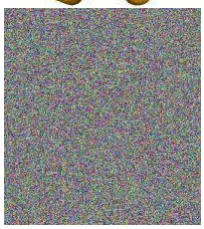
- **OFB (Output feedback)**



Output Feedback (OFB) mode encryption



Output Feedback (OFB) mode decryption



Sustitución simple o monoalfabética

- Se utiliza una función que sustituye cada carácter del alfabeto por otro del mismo alfabeto o de otro
- La clave es la tabla de sustitución
- Un caso particular de este cifrador es la rotación ROT(n) o cifrado de César, que reemplaza cada carácter por el que tiene a n lugares de distancia en el alfabeto
- Es muy fácil de criptoanalizar

Sustitución homofónica

- A cada carácter de M se le asigna un conjunto de símbolos de C
- Cuanto más frecuente sea m en el texto a cifrar, mas cantidad de símbolos de C se le asignarán, proporcionalmente
- Permite evitar análisis de frecuencias ya que las ocurrencias de cada c en el criptograma tendrán aproximadamente igual frecuencia
- Criptoanálisis: análisis de patrones de ocurrencia en lugar de ocurrencias simples

Sustitución homofónica

- Clave ejemplo:

A_i	$H(A_i)$
a	12 29 25 43 71 80 89 95
b	05 92
c	19 37 36
d	23 41 61 66
e	16 30 47 59 72 83 90 60 69 88 99 00
f	17 49
g	02 31
h	04 45 55 63 76 82
i	15 34 56 97 77 86
j	03
k	11
l	24 38 48 64
m	65 46
n	26 42 53 70 73 98
o	10 44 50 94 78 85 91
p	06 39

…

Sustitución polialfabética

- Se utiliza una clave de longitud *t* tal que la encriptación de un mensaje m = $(m_1 m_2 ... m_t)$ bajo la clave e = $(p_1, p_2, \ldots, p_t)$ es dado por $E_e(m) = (p_1(m_1)p_2(m_2)\ldots p_t(m_t))$
- La sustitución aplicada a cada carácter varía en función de la posición que ocupe éste dentro del mensaje. A diferencia de una sustitución homofónica, no se tiene un conjunto o secuencia fija de sustituciones posibles para cada carácter.

Cifrado de Vigenère

- Cifrador polialfabético del siglo XVI
- Sea el alfabeto A con una cantidad de símbolos *q*, la clave K = $(k_1 k_2 \ldots k_t)$ de longitud *t* y el mensaje que se desea encriptar m = $(m_1 m_2 ... m_t)$, entonces:
  - $E_K(m) = (\varphi_1 \varphi_2 \ldots \varphi_t) = c$
  - $D_K(c) = (\varphi_1^{-1} \varphi_2^{-1} \ldots \varphi_t^{-1}) = m$
  - Donde $\varphi_i = (m_i + K_i) \bmod q \qquad 1 \le i \le t$

    $\varphi_i^{-1} = (\varphi_i - K_i) \bmod q$

Cifrado de Vigenère: ejemplo

Supongamos que tenemos el alfabeto A = {A,B,…,Z} con q = 26 (longitud del alfabeto en inglés), nuestra clave es *datos* y el mensaje a encriptar es: *demostraciondelteorema*.

datos → K = (3,0,19,14,18) t = 5 (cantidad de símbolos que tiene la clave)

D	E	M	O	S	T	R	A	C	I	O
3	4	12	14	18	19	17	0	2	8	14
3	0	19	14	18	3	0	19	14	18	3
6	4	5	2	10	22	17	19	16	0	17

N	D	E	L	T	E	O	R	E	M	A
13	3	4	11	19	4	14	17	4	12	0
0	19	14	18	3	0	19	14	18	3	0
13	22	18	3	22	4	7	5	22	15	0

Entonces el criptograma es: **gefckwrtqarnwsdwehfwpa**

Cifrado de Vigenère: criptoanálisis

- Ataque de Kasiski (1863):
  - Se buscan strings repetidos, la distancia entre ocurrencias es probablemente un múltiplo de la longitud de la clave
  - Se factorizan todas las distancias encontradas, los factores más frecuentes son candidatos a ser la longitud de la clave
  - Teniendo longitudes candidatas para la clave, se trata cada columna como un cifrador monoalfabético (ROT(n)), muy fácil de romper, y si el correspondiente análisis de frecuencia tiene éxito para alguna de las longitudes candidatas, se ha roto el cifrador

Sustitución poligráfica

- En vez de sustituir caracteres por otros, sustituyen *grupos de caracteres* por otros
- Ejemplos:
  - Cifrado de Hill (1929)
  - Playfair (1854)

Cifrado de Hill

- Se utilizan bloques de *t* caracteres
- La clave es una matriz K de dimensión *t* x *t*
- Todas las operaciones se hacen en módulo 26, ya que el alfabeto tiene 26 símbolos
- La matriz debe ser inversible en módulo 26, para ello su determinante mod 26 debe ser 1
- E_K (m) = mK = c
- D_K (c) = cK^{-1} = m

Cifrado de Hill: ejemplo

O	R	G	A	N	I	Z	A	C	I	O	N
14	17	6	0	13	8	25	0	2	8	14	13

- Siendo: $K = \begin{pmatrix} 4 & 1 \\ 1 & 20 \end{pmatrix}$ det(K) mod 26 = 79 mod 26 = 1
- Para matrices de 2x2, es: $K^{-1} = \begin{pmatrix} a_{22} & -a_{12} \\ -a_{21} & a_{11} \end{pmatrix}$
- Entonces: $K^{-1} = \begin{pmatrix} 20 & -1 \\ -1 & 4 \end{pmatrix}$
- Y el primer paso de encriptación y desencriptación es:

$$c_1 = (14 \quad 17).\begin{pmatrix} 4 & 1 \\ 1 & 20 \end{pmatrix} = (21 \quad 16) \qquad m_1 = (21 \quad 16).\begin{pmatrix} 20 & -1 \\ -1 & 4 \end{pmatrix} = (14 \quad 17)$$

Cifrado de Hill: criptoanálisis

- Fuerza bruta es viable para longitudes pequeñas de clave
- Texto plano conocido: basta con conocer t^2 textos planos y sus correspondientes criptogramas para poder armar un sistema de ecuaciones lineales, fácil de resolver

PlayFair

- Se separa el texto plano en digramas y se cifra con una matriz de 5x5, donde se encuentran las 26 letras del alfabeto inglés:

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

- La clave es el orden que se le da a los caracteres en la matriz

PlayFair

- Cifrado:
  1. Si los símbolos en el diagrama son iguales, se reemplaza el segundo símbolo por otro acordado con anterioridad (por lo general es "X"). Se encripta el nuevo par.
  2. Si los caracteres aparecen en la misma fila de la matriz, para cada carácter del par la sustitución se realiza con el carácter ubicado inmediatamente a la derecha. En el caso que se termine la fila se continúa para abajo.

PlayFair

- Cifrado:
  3. Si los caracteres aparecen en la misma columna de la matriz, para cada carácter del par la sustitución se realiza con el carácter ubicado inmediatamente abajo. Si se termina la columna se continúa hacia la derecha.
  4. Si los caracteres aparecen en distinta fila y columna, se arma un rectángulo en la matriz que contiene a dichos caracteres como vértices. La sustitución para cada carácter del par se realiza tomando, de los dos vértices restantes, el que esta ubicado en la misma fila.

PlayFair: ejemplo

- Encriptar organización usando:

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

Paso	Diagrama	Matriz	Regla	Sustitución	Cifrado
1	OR	D P **F** U T H C **R** Q K W Y X **O** E G I/J M N B A L Z S V	4	R → Q O → X	**XQ**
2	GA	**D** P F U T **H** C R Q K **W** Y X O E **G** I/J M N B **A** L Z S V	3	G → A A → P	**AP**
3	NI	D P F U T H C R Q K W Y X O E G **I/J** M **N** B A L Z S V	2	N → B I → M	**BM**

...

Cifrados por transposición

- En vez de sustituir símbolos por otros, cambia su orden dentro del bloque a encriptar
- Un cifrado por transposición simple tiene como clave una tabla que apunta a las posiciones finales para cada carácter dentro del bloque

Cifrados por transposición

- Ejemplo de transposición simple (t=6, m=establecerelprecio):

P_K	
M	**C**
1	4
2	1
3	3
4	6
5	2
6	5

P_K^{-1}	
C	**M**
1	2
2	5
3	3
4	1
5	6
6	4

Paso	Mensaje	Cifrado
1	establ	sbtela
2	ecerel	ceeelr
3	Precio	riepoc

Cifrados por transposición

- Transposición por columnas:
  - Se toma una clave sin caracteres repetidos, y se utiliza el orden de sus caracteres para enumerar las columnas. Ejemplo:

establecenlassiguientescaracteristicasimportantes

Clave: segunda

s	e	g	u	n	d	a
e	s	t	a	b	l	e
c	e	n	l	a	s	s
i	g	u	i	e	n	t
e	s	c	a	r	a	c
t	e	r	i	s	t	i
c	a	s	i	m	p	o
r	t	a	n	t	e	s

Cifrado de producto

- Combinan una o más vueltas de un cifrado por sustitución con un cifrado de transposición
- La clave puede cambiar entre una vuelta y otra del mismo algoritmo
- Se debe evitar que el cifrado tenga **estructura de grupo**

Estructura de grupo

- Un cifrador de producto tiene estructura de grupo si:

$$\forall k_1, k_2 \quad \exists k_3 \text{ tal que } \quad E_{k_2}(E_{k_1}(m)) = E_{k_3}(m)$$

- Esto es, si hacemos dos cifrados encadenados con k_1 y k_2, existe una clave k_3, generalmente de igual longitud que realiza la transformación equivalente
- Esta propiedad es indeseable ya que implica que al volviendo a encriptar no se logra aumentar la fuerza de la encriptación, porque equivale a encriptar una vez con una clave de igual longitud que la original

Cifrado de flujo: one time pad

- El texto plano se combina con una clave secreta, de igual longitud que el texto, que se utiliza una sola vez
- Al ser tan larga la clave, es imposible de memorizar, entonces es posible utilizar como clave la semilla de un generador pseudoaleatorio
- Si la clave es aleatoria, secreta, y única, el método es incondicionalmente seguro

Seguridad incondicional

- Este algoritmo no se puede atacar ni siquiera con fuerza bruta: durante la prueba de todas las claves que existen se obtendrán todos los mensajes que existen
- Como la clave se usa una vez, los ataques por texto plano conocido/escogido no aportan valor
- Los ataques por frecuencia son inútiles ya que el criptograma generado es indistinguible de una cadena aleatoria

One time pad

- La función que combina la clave y el texto (encripta) es el XOR binario, y la función que desencripta es la misma.
- Ejemplo: encriptar “criptografia”

	c	r	i	p	t	o
Mensaje	01100011	01110010	01101001	01110000	01110100	01101111
S.Aleatoria	01011010	01110001	10100000	00101000	00010010	10101110
Criptograma	00111001	00000011	11001001	01011000	01100110	11000001

	g	r	a	f	i	a
Mensaje	01100111	01110010	01100001	01100110	01101001	01100001
S.Aleatoria	10101001	11110000	01111111	11111111	11100101	00100011
Criptograma	11001110	10000010	00011110	10011001	10001100	01000010

One time pad

- Desventajas:
  - Los números aleatorios o pseudoaleatorios de calidad criptográfica son muy difíciles de generar
  - La distribución de las claves se vuelve un problema crítico, dado su tamaño
  - Asegurar la no reutilización implica generar una clave, y distribuirla, para cada mensaje que se quiera transmitir, y destruirla después del uso
  - No se provee autenticación

Referencias

Criptografía y Seguridad en Computadores, tercera edición. Manuel José Lucena Lopez. Dpto. de Informática Universidad de Jaén. Edición virtual - 2003. http://www.loba.es/flossic/Contenidos/Manuales/Criptografia.pdf

Aplicaciones Criptográficas, segunda edición. Departamento de Publicaciones de la Escuela Universitaria de Informática de la Universidad Politécnica de Madrid, España. http://www.criptored.upm.es/descarga/CriptoClasicapdf.zip

Una introducción a la criptografía. Eugenio García, Miguel Ángel López, Jesús Ortega. Dpto. De Matemáticas Universidad de Castilla.

http://www.criptored.upm.es/descarga/UnaIntroduccionCriptografia.zip