



Criptografía y Seguridad

Criptografía:
Introducción

Criptografía

- Proviene del griego. Significa 'escritura secreta'
- Técnicas matemáticas
- Provee un conjunto básico de herramientas para implementar mecanismos de seguridad

Usos

- Comunicaciones seguras
 - Trafico web
 - Trafico inalámbrico



Usos

- Protección de archivos en disco



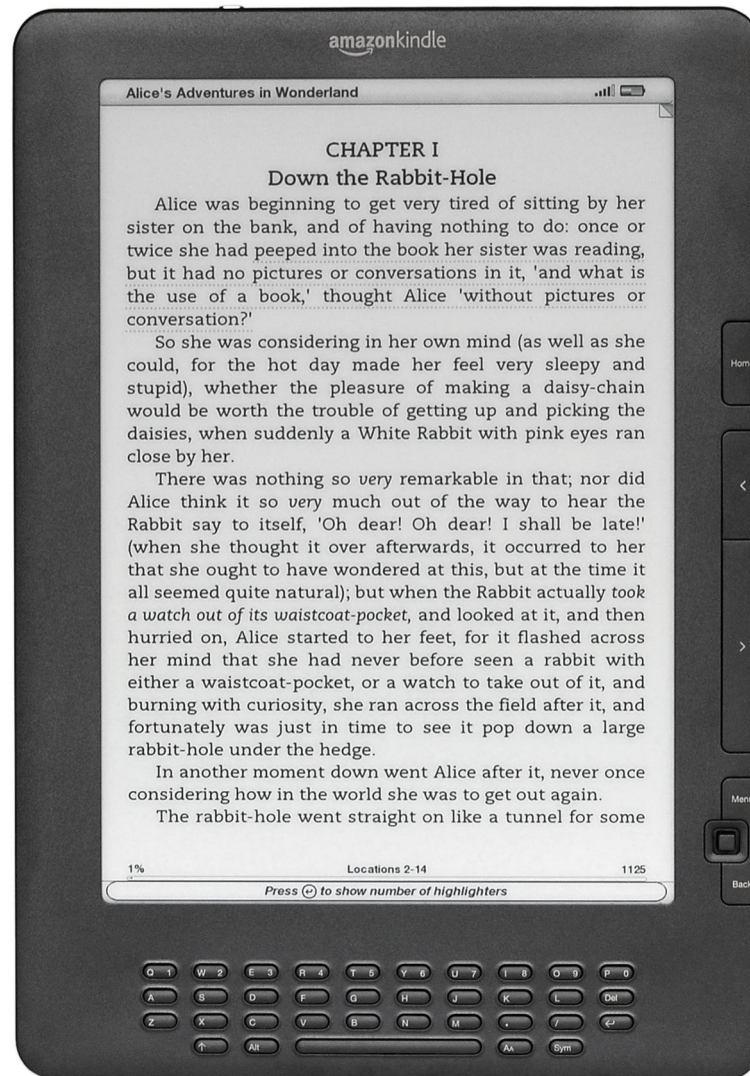
Usos

- Autenticación de usuarios



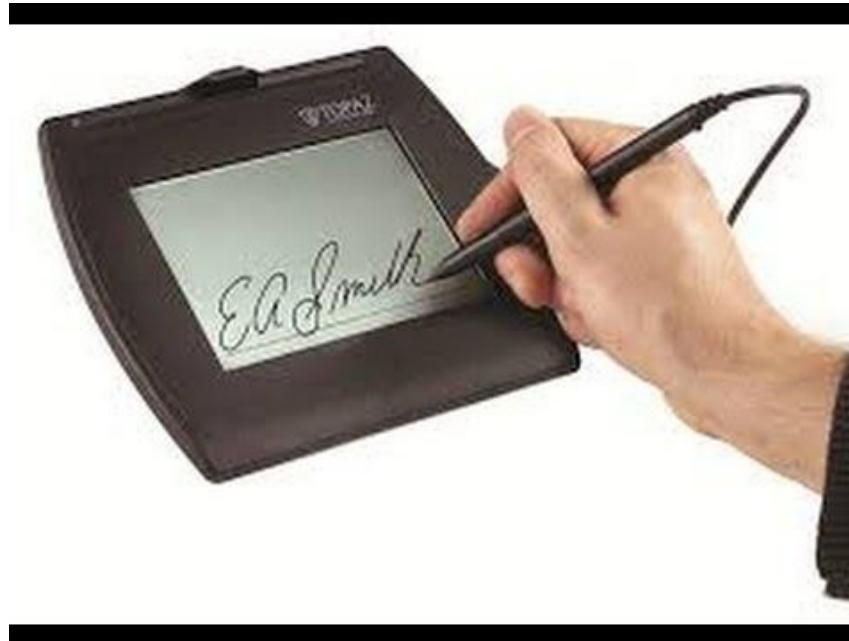
Usos

- Protección de contenido



Usos

- Firmas digitales



Usos

- Voto electrónico



Usos

- Dinero electrónico

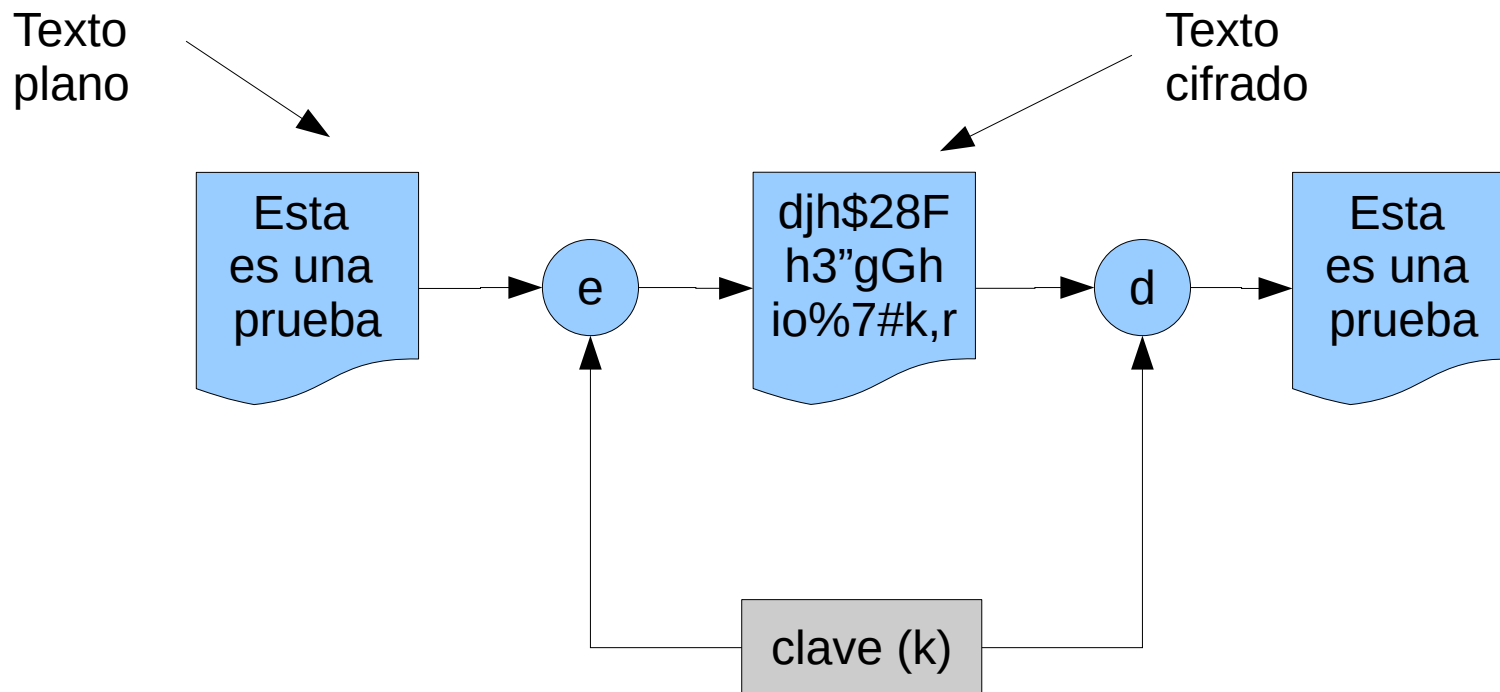


Es una ciencia dura

- Las construcciones deben pasar rigurosas pruebas matemáticas
- Lineamientos generales:
 - Definición precisa del modelo de amenaza
 - Proposición de construcción criptográfica
 - Demostración de que romper la construcción en función del modelo implica resolver algún problema complejo (reducción)

Primera aproximación

- Construcción básica: Criptosistema



Cifrado

- Consiste en la transformación de un mensaje
- La transformación tiene dos parámetros
 - Mensaje
 - Clave
- Sin la clave, la transformación no puede ser invertida
- Principio de Kerckhoffs:
 - Un criptosistema debe ser seguro incluso si todo sobre el sistema, excepto la clave, es de público conocimiento.

La idea

- El mensaje cifrado
 - Puede publicarse
 - Puede enviarse por canales no seguros
- La seguridad reside en la clave
 - Que típicamente tiene un tamaño considerablemente menor al mensaje



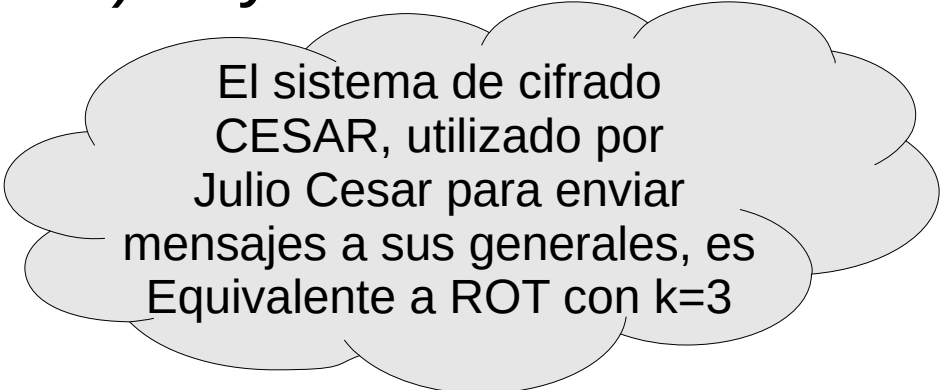
Orígenes

- Ocultar información
- Antiguo Egipto (2.500AC)
 - jeroglíficos no estándares
- Hebreos (600-500AC)
 - Atbash
- Griegos
 - Escitala



Un poco de historia

- Cifrado por rotación
 - Considerar cada letra como un número (su posición en el alfabeto, comenzando por 0)
 - La clave k es un número entre 1 y 26 (cantidad de letras - 1)
 - Cifrado: reemplazar cada letra por la que ocupa k posiciones a continuación en el alfabeto, volviendo a la 'a' luego de la 'z'
 - Si $k=4$. Entonces: e(prueba)=tvyife



El sistema de cifrado CESAR, utilizado por Julio Cesar para enviar mensajes a sus generales, es Equivalente a ROT con $k=3$

Seguridad del cifrado por rotación

- Objetivo del atacante
 - Recuperar el mensaje original
 - Recuperar la clave
- ¿Prueba y error? Considerar $c = \text{tv yife}$
 - ¿ $k=1$? $e^{-1}(\text{tv yife}) = \text{suxhed}$ <- sin sentido
 - ¿ $k=2$? $e^{-1}(\text{tv yife}) = \text{rtwgdc}$ <- sin sentido
 - ¿ $k=3$? $e^{-1}(\text{tv yife}) = \text{qsvfcb}$ <- sin sentido
 - ¿ $k=4$? $e^{-1}(\text{tv yife}) = \text{prueba}$ <- ¡Con sentido!
 - $K = 4$, $M = \text{prueba}$

Seguridad del cifrado por rotación

- ¿ROT-X es inseguro?
 - ¿Cual es el mensaje original p , si $e(p) = a$?
- Entonces ¿ROT-X es seguro?
 - ↳ la seguridad depende del contexto
- Se necesita poder discriminar un mensaje valido de uno inválido
 - Los lenguajes naturales tienen redundancia
 - Ejemplo: L csa azl → La casa azul
 - Los archivos tienen marcas conocidas
 - Ejemplo: Magic header PK en zips
- ¡Si el mensaje a cifrar fuese aleatorio, cualquier función seria segura!

Cifrado de Sustitución

- Reemplaza un símbolo por otro
- Ejemplo:



Criptograma encontrado en una tumba en el cementerio de Trinity (NY, USA) en 1794

Descifrado en 1986

À	Ā	Ĉ	Ĭ	Ĺ	Ļ	T	U	V
Ď	Ē	Ĝ	Ŋ	Ŏ	Ŗ	W	X	Y
Ġ	Ĥ	İ	Ų	Ŵ	Ŷ	Z	-	-

Cifrado de Sustitución

- Reemplaza un símbolo por otro

k= d u b l c m f t h i j n z p x q e a o s v k r w g y
↑ ↑ ... ↑
↓ ↓ ... ↓
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

esto es una prueba

cosx co vpd qavcud

Cifrado de Sustitución

- Identificación
 - Las propiedades estadísticas del lenguaje no se ven alteradas
- Análisis
 - Obtener la frecuencia estimada de cada símbolo en el lenguaje del mensaje.
 - Calcular la frecuencia de cada símbolo el texto cifrado.
 - Asumir que los símbolos de mayor probabilidad son se corresponden
 - Formar grupos de dos y tres letras comunes (el, la, de, las, los, etc).

Frecuencias de letras

E	13,11	C	4,85	Y	0,79
A	10,60	L	4,42	Q	0,74
S	8,47	U	4,34	H	0,60
O	8,23	M	3,11	Z	0,26
I	7,16	P	2,71	J	0,25
N	7,14	G	1,40	X	0,15
R	6,95	B	1,16	W	0,12
D	5,87	F	1,13	K	0,11
T	5,40	V	0,82	Ñ	0,10
Frec. Alta		Frec. Media		Frec. Baja	

Ejercicio

- Descifrar el siguiente mensaje:

⬅>]👉0 ➡34⬅3 44]>} >{:⬅⬅⬆ {4➡3>
34]02 014:0 34(⬆4 ➡👉>⬆) 0[]4
03401 4}034 ⬅344] 0➡1>]

Ayudas

- * El mensaje original esta en castellano.
- * La separación en grupos de 5 simbolos no es parte del problema, simplemente ayuda a contar mejor.
- * Gancho: "LACABEZA"

Cifrado Vigenere

- Es una sustitución polialfabética
 - Un mismo símbolo puede transformarse a diferentes
- Clave compuesta por n números
- Aplicación de ROT-X según la clave.

K=ECFD (long 4)

esto	es	una	prueba
iuyr	dgxc	yofc	ttzhfc

Obs: primera letra de cada bloque se rota 4 veces, la segunda 2 veces, la tercera 5 veces y la cuarta 3 veces

Cifrado Vigenere

- Creado en 1553
- ¿Es seguro?
- Durante casi 300 años se lo consideró seguro
- Pero ...

En 1863 Friedrich Kasiski publica un metodo para resolverlo

Cifrado Vigenere

- Ataque:
 - Determinar longitud de bloque
 - Analizar la clave de cada bloque por separado
- Aparecen n-gramas repetidos al transformar los mismos símbolos en la misma posición (Test de Kasiski)
 - Buscar secuencias repetidas
 - Calcular la distancia entre las secuencias
 - La longitud de la clave es múltiplo del MCD entre las distancias halladas

Cifrado Vigenere

- Ejemplo

PBVRQ VICAD SKAÑS DETSJ PSIED BGGMP SLRPW RÑPWY EDSDE ÑDRDP
CRCPQ MNPWK UBZVS FNVRD MTIPW UEQVV CBOVN UEDIF QLONM WNUVR
SEIKA ZYEAC EYEDS ETFPH LBHGU ÑESOM EHLBX VAEPP UÑELI SEVEF
WHUNM CLPQP MBRRN BPVIÑ MTIBV VEÑID ANSJA MTJOK MDODS ELPWI
UFOZM QMVNF OHASE SRJWR SFQCO TWVMB JGRPW VSUEX INQRS JEUEM
GGRBD GNNIL AGSJI DSVSU EEINT GRUEE TFGGM PORDF OGTSS TOSEQ
OÑTGR RYVLP WJIFW XOTGG RPQRR JSKET XRNBL ZETGG NEMUO TXJAT
ORVJH RSFHV NUEJI BCHAS EHEUE UOTIE FFGYA TGGMP IKTBW UEÑEN
IEEU

GGMP (3 veces): separadas por 256 y 104 ca
YEDS (2 veces): separadas por 72 caracteres
HASE (2 veces): separadas por 156 caracteres
VSUE (2 veces): separadas por 32 caracteres.

$$\text{MCD}(32, 72, 104, 156, 256) = 4$$

Cifrado Vigenere

- Método de coincidencia mutua:
 - Determinar estadísticamente las letras más probables en cada grupo
 - Estimar las rotaciones que llevan a cada grupo a equipararse con las estadísticas del lenguaje
 - Probar las rotaciones, eliminando caminos al encontrar combinaciones sin sentido

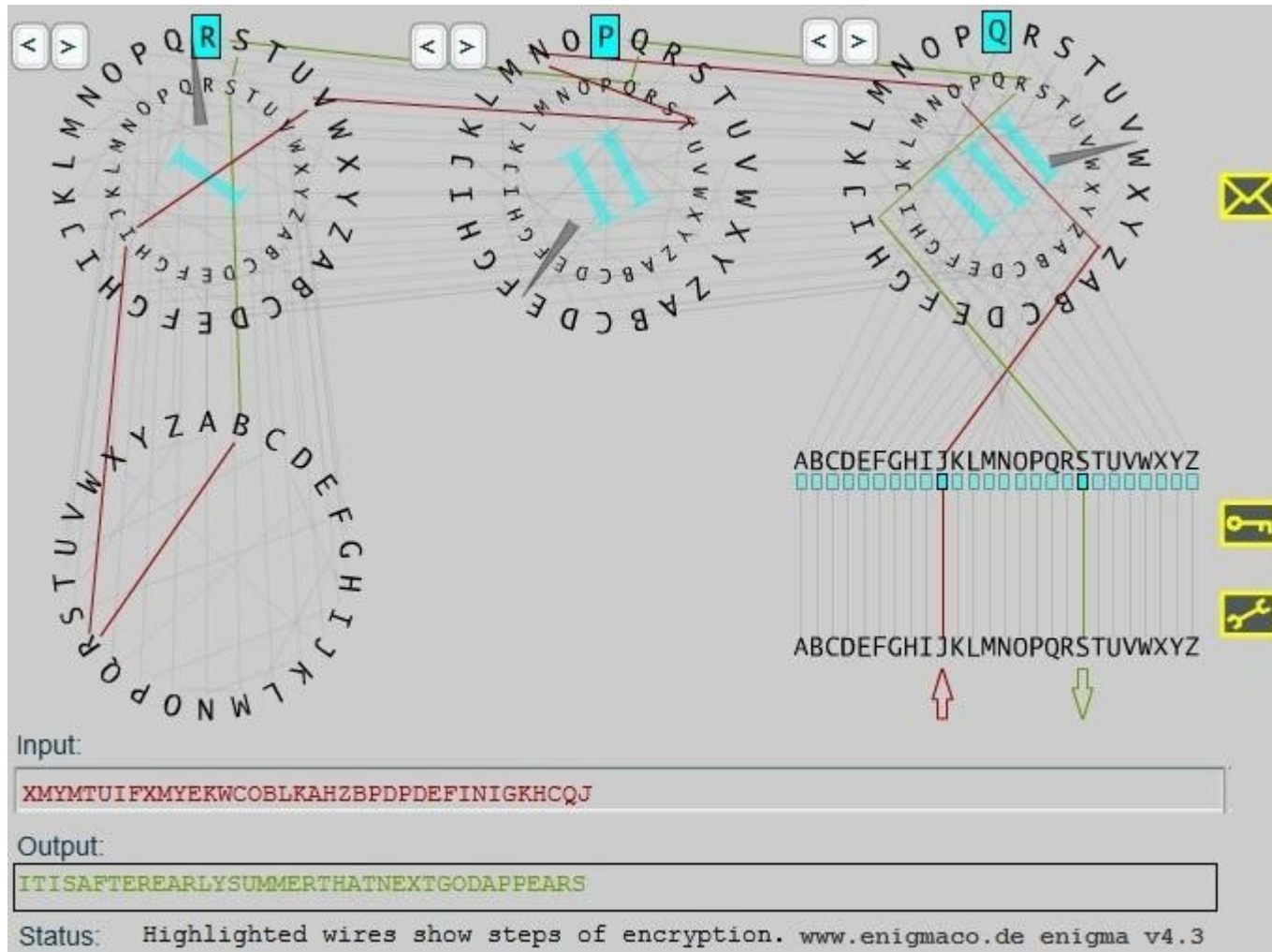
Sustitución polialfabética

- Maquina enigma



Sustitución polialfabética

- Maquina enigma



¿Hay criptosistemas seguros?

- Primero hay que definir que consideramos un criptosistema seguro.
- Por mucho tiempo algo era seguro si no lo lograban analizar.
- Los avances de la 2da guerra mundial nos llevan a la criptografía moderna:
 - Representaciones formales de criptosistemas
 - Definiciones del modelo de amenaza
 - Pruebas de seguridad formales

Criptosistema simétrico (def.)

- Es una terna de algoritmos
 - Gen (algoritmo de generación de claves)
 - Enc (cifrado): $\text{Enc}_k(m)$
 - Dec (descifrado): $\text{Dec}_k(c)$
- } tienen que ser funciones inversas
- Propiedades
 - La salida de Gen define K el espacio de claves.
 - La entrada de Enc define el espacio de mensajes
 - La entrada de Dec define el espacio de mensajes cifrados
 - Para todo m y k válidos: $\text{Dec}_k(\text{Enc}_k(m))=m$

Escenarios de ataques

- Ataque de texto cifrado
 - Ciphertext-only attack
 - El adversario solo dispone de mensajes cifrados y busca obtener los mensajes
- Ataque de texto plano conocido
 - Known-plaintext attack
 - El adversario conoce pares (mensaje, mensaje cifrado) con la misma clave, y busca obtener un mensaje a partir de otro texto cifrado

Escenarios de ataques

- Ataque de texto plano escogido
 - Chosen-plaintext attack
 - El adversario puede obtener el cifrado de los mensajes que desee, y busca obtener el descifrado de un mensaje cifrado diferente
- Ataque de texto cifrado escogido
 - Chosen-ciphertext attack
 - El adversario puede obtener el descifrado de los mensajes que desee, y busca obtener el descifrado de un mensaje diferente

Seguridad para cifrados simétricos

- Definición: Un criptosistema es seguro si ningún adversario puede computar cualquier función del texto plano a partir del mensaje cifrado que posee.

Esta condición se puede formular matemáticamente gracias al aporte de Claude Shannon, y se conoce como condición de **secreto perfecto**.

Secreto perfecto

- Criptosistema:

- Gen: $k \leftarrow K$
- Enc: $c \leftarrow \text{Enc}_k(m)$ (potencialmente prob.)
- Dec: $m = \text{Dec}_k(c)$ (determinística)

- Probabilidades:

- $\Pr[M=a]$: probabilidad de que el mensaje sea a
- $\Pr[K=x]$: probabilidad de que la clave sea x
- $\Pr[C=b]$: probabilidad de que el mensaje cifrado sea b

($a \leftarrow A$: Tomar un elemento al azar de un conjunto)

Secreto perfecto

- Definición: Un criptosistema (gen , enc , dec) posee la propiedad de secreto perfecto sobre un espacio de mensajes M si:
 - Para toda distribución de probabilidades en M , cada mensaje m y cada mensaje cifrado c tal que $\Pr[C = c] > 0$:
 - $\Pr[M=m \mid C = c] = \Pr[M=m]$
 - Es una forma de decir que el texto plano y el cifrado son probabilísticamente independientes

Indistinguibilidad de mensajes

- Si un criptosistema tiene secreto perfecto \leftrightarrow para cualquier par de mensajes m_1 y m_2 :
 - $\Pr[C=c \mid m=m_1] = \Pr[C=c \mid m=m_2]$

Ejercicio: Demostrarlo

Ayuda:

- Secreto perfecto $\leftrightarrow \Pr[C = c \mid M=m \mid] = \Pr[C=c]$

Lectura Recomendada

Capítulo 1

Introduction to Modern Cryptography
Katz & Lindell