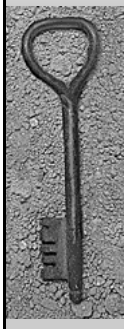
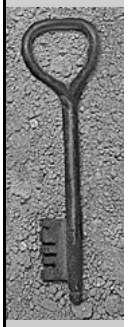
Criptografía

1. Introducción
2. Bases Teóricas
3. Criptografía Simétrica: Cifrado en Flujo
4. Criptografía Simétrica: Cifrado en Bloque
5. Criptografía Asimétrica
6. Aplicaciones Criptográficas



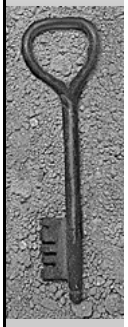
Programa de Prácticas

1. Herramientas de Criptoanálisis Estadístico.
2. Exponenciación Rápida.
3. Algoritmo de Euclides y Cálculo de Inversos Modulares.
4. Tests de Primalidad.
5. Cifrado de Playfair.
6. Cifrado de Vigenere.
7. Postulados de Golomb.
8. Generación de Polinomios Primitivos.
9. Algoritmo de Berlekamp-Massey.
10. Generador de Geffe.
11. Generador de Beth-Piper.
12. Algoritmo de Diffie-Hellman. Cifrado de Elgamal.
13. Cifrado RSA.
14. Cifrado de la Mochila.
15. Compartición de Secretos



Bibliografía

- Introducción a la Criptografía. *Caballero, P.* Editorial Ra-Ma, 2ª Edición. 2002.
- Técnicas Criptográficas de Protección de Datos. *Fúster, A.; De la Guía, D.; Hernández, L.; Montoya, F.; Muñoz, J.* Ra-Ma, 2000.
- Seguridad y Protección de la Información. *Morant J.L; Ribagorda A.; Sancho J.* Editorial Centro de Estudios Ramón Areces; 1994.
- Criptografía Digital. *Pastor, José; Sarasa, Miguel Angel*. Colección Textos Docentes; Prensas Universitarias de Zaragoza; 1998.
- Aplicaciones Criptográficas. Segunda Edición. *Ramió Aguirre, Jorge*. Dpto. de Publicaciones EUI-UPM, 1999.
- Applied Cryptography. Protocols, Algorithms, and Source Code in C. 2nd ed. *Schneier, Bruce*. John Wiley & Sons, Inc., 1996.
- Criptografía per las serveis telematics. *J. Domigo, J. Herrera*. Edicions de la Universitat Oberta de Catalunya. 1999



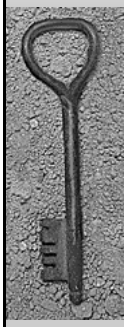
Necesidades

- Criptografía: Vulnerabilidad de la **información**
- Seguridad Informática: Vulnerabilidad del **sistema**

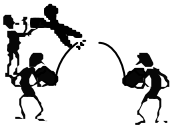
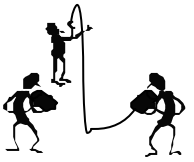
•**Hardware**: aislamiento, medidas contra incendios, etc.

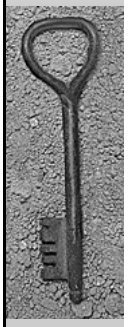
• **Software**: S. O., Programas de utilidades y programas de usuarios (Bombas lógicas, troyanos, gusanos, puertas falsas, etc.).

• **Datos**: Necesidad de la Criptografía.



Algunas Amenazas

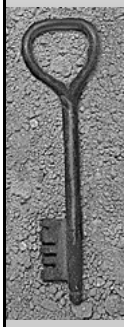
- **Intercepción:** 
- **Modificación:** 
- **Interrupción:** 
- **Generación:** 



Declaración Universal de los Derechos del Hombre

Artículo 12.-

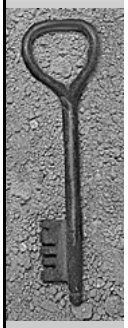
Nadie será objeto de ingerencias arbitrarias en su vida privada, su familia, su domicilio o **su correspondencia**, ni de ataques a su honra o a su reputación. Toda persona tiene derecho a la protección de la ley contra tales ingerencias o ataques.



¿Qué protege la Criptografía?

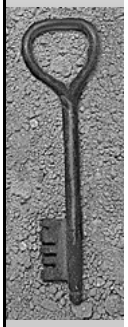
- **Confidencialidad:** Disponibilidad de la información sólo para usuarios autorizados.
- **Integridad:** Garantía de la imposibilidad de modificar la información.
- **Autenticidad:** Legitimidad del origen de la información.
- **No repudio:** Imposibilidad de negación ante terceros del envío y/o recepción por parte del emisor y/o receptor de la información.

- **Anonimato**: Secreto de identidad del emisor de un mensaje o usuario de un sistema.
- **Accesibilidad:** Posibilidad de acceso eficiente sólo para entidades autorizadas.

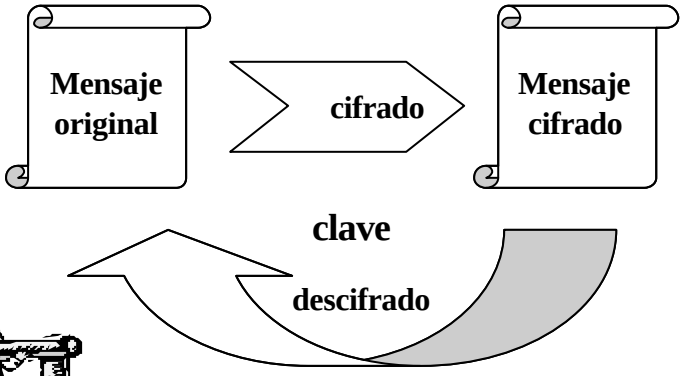


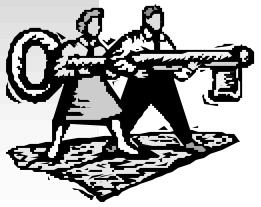
Seguridad en Internet

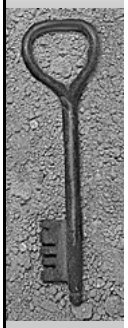
Sistema	¿Qué es?	Algoritmos	Protege
PGP	Aplicación de correo-e	RSA, MD5, IDEA	Confidencialidad, Integridad, Autenticidad, No repudio
S/MIME	Formato de correo-e	A especificar por el usuario	Confidencialidad, Integridad, Autenticidad, No repudio
SSL	Protocolo para transmisiones TCP/IP	RSA, RC2, RC4, MD5, triple DES, SHA	Confidencialidad, Integridad, Autenticidad, No repudio
SET CyberCash	Protocolos para pagos-e	RSA, MD5, RC2	Confidencialidad, Integridad, Autenticidad, No repudio, Anonimato
IPSec	Protocolo de bajo nivel para paquetes IP	Diffie-Hellmann,...	Confidencialidad, Integridad, Autenticidad
Kerberos	Servicio de red para aplicaciones de más alto nivel	DES	Confidencialidad, Autenticidad



Cifrado/Descifrado

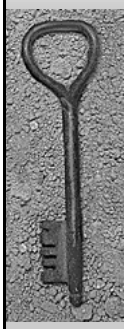






Conceptos básicos

- **Criptografía:** (Ocultar + escritura) Ciencia que estudia cómo **proteger** la información mediante el cifrado.
- **Criptoanálisis:** Ciencia que estudia cómo romper el cifrado y acceder a la información protegida con él.
- **Criptología:** Criptografía + Criptoanálisis.
- **Criptosistema:** Sistema de cifrado.



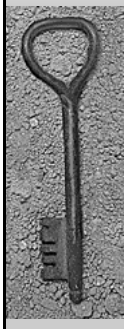
Conceptos básicos

- **Elementos de un criptosistema:**
  - El espacio de mensajes originales (M)
  - El espacio de mensajes cifrados (C)
  - El espacio de claves (K)
  - El conjunto de posibles cifrados E
  - El conjunto de correspondiente descifrados D

- **Requisitos de un criptosistema:**

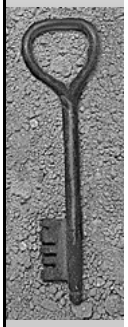
–Los cifrados y descifrados deben ser computacionalmente eficientes.

–La seguridad debe depender sólo del secreto de las claves, y no del secreto de E y D.



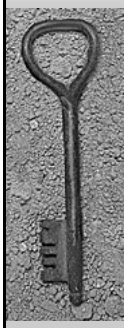
Reglas de Kerchoffs (s.XIX)

1. No debe existir ninguna forma de recuperar el texto en claro a partir del texto cifrado.
2. Todo sistema criptográfico debe estar compuesto por información pública (familia de algoritmos que lo definen) e información secreta (clave).
3. La elección de la clave debe ser fácil de recordar y de modificar.
4. El texto cifrado debe poderse enviar con los medios habituales de comunicación.
5. La complejidad del proceso de recuperación del texto original debe ser proporcional a la importancia de la información protegida.

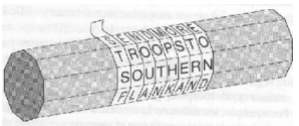


Ataques y Secretos

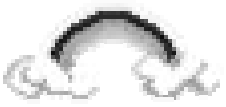
- **Tipos de Ataque:**
  - Ataque sólo con texto cifrado.
  - Ataque con texto original conocido.
  - Ataque con texto original escogido.
  - Ataque con texto cifrado escogido.
- **Tipos de Secreto:**
  - **Secreto teórico o incondicional:** Seguro frente a recursos ilimitados.
  - **Secreto práctico o computacional:** Seguro frente a recursos acotados.



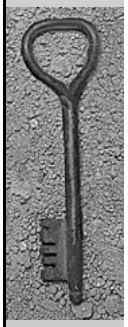
Pasado, Presente y Futuro.



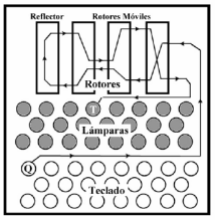
- La Información es Poder
- Pasado:
  - s. V a.C., escítala en Grecia
  - s I d.C, cifrado de César
  - s. XX:
    - Telegrama Zimmermann (I Guerra Mundial)
    - Máquina Enigma (II Guerra Mundial)
    - Clave Pública (1976, Diffie y Hellman)
- Presente: Cambio en el estándar de cifrado en EEUU. (DES → Rijndael)



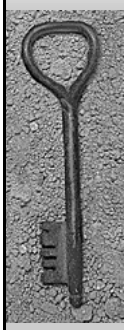
- Futuro: ????



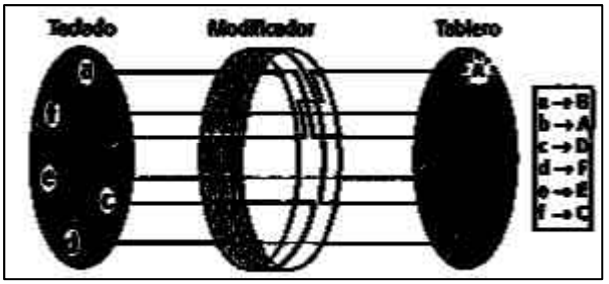
Criptografía Clásica

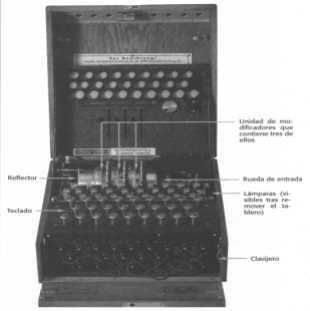


- Rotores
  - Cada rotor es una permutación arbitraria del alfabeto. La salida de un rotor se encuentra conectada a la entrada del rotor siguiente.
  - Por ejemplo en una máquina de 4 rotores; la A -> F, luego la F -> Y, luego Y -> E y finalmente la E-> C.
- La máquina Enigma:
  - Inventada por un ingeniero alemán durante la I guerra mundial, utilizada posteriormente en la II GM por los alemanes.
  - Las llaves se definían mediante 3 rotores. Una vez posicionados los rotores se ingresaba el carácter a cifrar y se obtenía como resultado el carácter cifrado. Se cifraba así, sucesivamente todo el texto. A cada cifrado el rotor se desplazaba permitiendo romper el esquema estadístico del idioma.
  - Para descifrar el mensaje era necesario tener la misma máquina y conocer el posicionamiento inicial de los rotores.
  - Un equipo de criptógrafos polacos logró descifrar la máquina enigma informando a los ingleses.



La Máquina ENIGMA



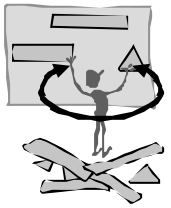


Al pulsar la b en el teclado, una corriente pasa al modificador, sigue el sendero del cableado interno y finalmente sale iluminando la lámpara A en el tablero, de forma que la b es codificada como A

Cada vez que se pulsa una letra en el teclado y se codifica, el modificador gira una posición, cambiando así la forma de codificar la siguiente.

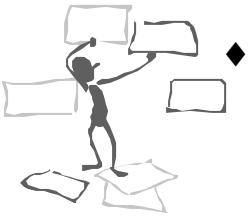
La "clave" en este caso seria el número de modificadores utilizados y su posición inicial.

Criptografía Clásica



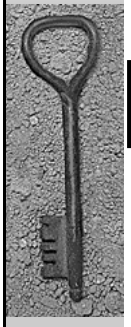
- Transposición: Permuta los símbolos del texto original (desorden).

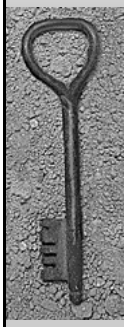
$$\begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ \downarrow & & & & & \\ 2 & 4 & 3 & 1 & 6 & 5 \end{pmatrix}$$



- Sustitución: Cambia las unidades del texto original por otras (correspondencia).

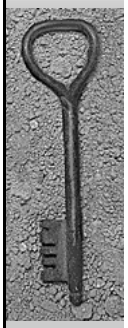
Criptografía Clásica





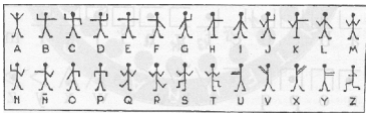
Pasado, Presente y Futuro.

- 600 a 500 a.C. Libro de Jeremias (sustitución simple)
- 300 a.C. Euclides (Teoria de Números y Números Primos)
- 276 a 194 a.C. Criba de Erastótenes (Números Primos)
- 204 a 122 a.C. Código de Políbio (sustitución poligrámica)
- 50 a.C. Código de César
- 79 d.C. Cuadrado Latino (transposición)
- 400 Cifrado Kama-Sutra
- 801 a 873 Criptanálisis al-Kindi
- 1466 Leon Battista Alberti (sustitución polialfabética)
- 1518 Johannes Trithemius (esteganografia)
- 1550 Girolamo Cardano (esteganografia y sustitución autoclave)
- 1563 Giambattista Della Porta (sustitución polialfabética)
- 1586 Blaise de Vigenère (sustitución polialfabética)
- 1948 Claude Elwood Shannon



Criptografía Clásica

Sustitución



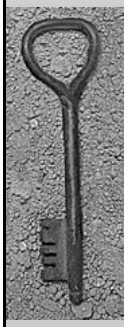
El código de Cesar : ***VENI VIDI VICI (k+3)***

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

YHQL YLGL YLFL

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

CIFRADO DE CESAR: CIFRADO AFÍN
j= at+b (mod m)



Criptografía Clásica

•César: Cada letra se sustituye por otra que ocupa k posiciones mas allá en el alfabeto.

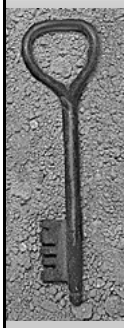
A>Z, B>A, C>B,...,Z>Y

IBM > HAL

•Vigenere: La primera letra se sustituye por otra que ocupa k1 posiciones mas allá en el alfabeto, la segunda por la que ocupa k2 posiciones mas allá,...

A>Z, B>A, C>B,...,Z>Y

A>B, B>C, C>D,...,Z>A



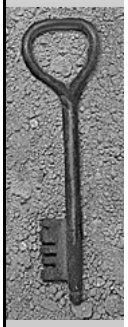
Criptografía Clásica

Sustitución

Disco de Alberti

Cifrado de Vigenere

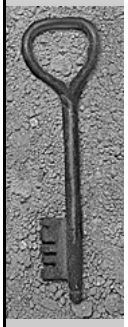
	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z
0	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z
1	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A
2	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B
3	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C
4	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D
5	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E
6	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F
7	H	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
8	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
9	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	I
10	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J
11	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K
12	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L
13	N	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
14	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
15	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	O
16	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P
17	R	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
18	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
19	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	S
20	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T
21	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U
22	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V
23	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W
24	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X
25	Z	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



Cifrado de Playfair

- Inventado por Charles Wheatstone para comunicaciones telegráficas en 1854. Utilizado por el Reino Unido en la 1ª Guerra Mundial
- Consiste en separar el texto en claro en digramas y cifrar de acuerdo a una matriz alfabética de dimensiones 5 X 5 en la cual se encuentran representadas las 26 letras del alfabeto ingles. La clave se coloca al comienzo de la matriz quitando las repeticiones y a continuación el resto de las letras del alfabeto.
- Matriz de Playfair

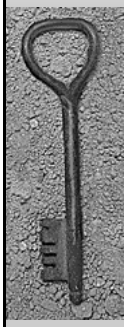
A	B	C	D	E
F	G	H	I/J	K
L	M	N	O	P
Q	R	S	T	U
V	W	X	Y	Z



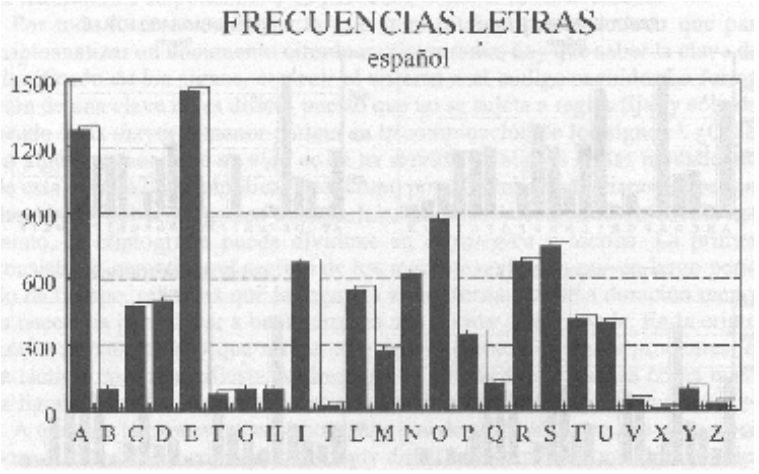
Cifrado de Playfair

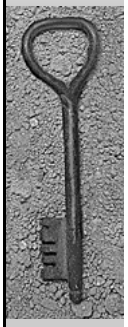
- Para cifrar es necesario seguir las siguientes reglas:
  - Si los símbolos están en la misma fila y diferente columna, se desplaza una columna a la derecha.
  - $(a_{ij}; a_{ik}) \longrightarrow (a_{ij+1}; a_{ik+1})$
  - Si los símbolos están en la misma columna y diferente fila, se desplaza una columna hacia abajo.
  - $(a_{ik}; a_{jk}) \longrightarrow (a_{(i+1)k}; a_{(j+1)k})$
  - Si estan en filas y columnas diferentes.
  - $(a_{ki}; b_{js}) \longrightarrow (a_{ks}; b_{ji})$
  - Si hay dos símbolos iguales consecutivos, se inserta un símbolo acordado con anterioridad (por lo general es "X").
- Ejemplo:
  - Palabra Clave: VERANO AZUL
  - Letra Nula: X
  - Texto Claro: COMPRUEBALO TU
  - Con la Letra Nula: CO MP RU EB AL OT UX
  - Texto Cifrado: IC PQ UF NZ LG ZS LW

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



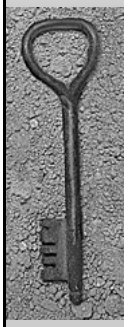
Criptoanálisis Estadístico





Criptoanálisis Estadístico

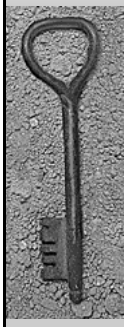
- Las letras, ordenadas por porcentaje de utilización de mayor a menor, son: E A O S R I N L D C T U P M Y Q G V H F B J Z K W X
- Las combinaciones de dos letras más usuales, ordenadas de mayor a menor frecuencia de aparición, son: ES EN EL DE LA OS UE AR RA RE ON ER AS ST AL AD TA CO OR
- Las combinaciones de tres letras más usuales, ordenadas de mayor a menor frecuencia de utilización, son: QUE EST ARA ADO AQU CIO DEL NTE EDE OSA PER NEI IST SDE
- La letra más utilizada es la "E", con un porcentaje de utilización del 13%
- El porcentaje de aparición de las vocales es del 47%



Criptoanálisis Estadístico

Método Kasiski

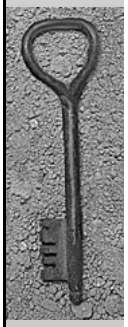
- Ideado por un oficial polaco en 1863 para romper el cifrado de Vigenere, considerado irrompible durante 300 años.
- Se basa en la suposición de que la repetición de una cadena de dos o más caracteres a lo largo del criptograma se corresponderán con la misma cadena en el texto plano, por lo que la longitud entre las cadenas será un múltiplo de la longitud de la llave K.
- Una vez encontrada la longitud n de la llave K, se divide el texto cifrado en bloques de tamaño n y se realiza un análisis de frecuencias por cada bloque, lo cual es más sencillo que realizarlo a todo el criptograma completo.



Criptoanálisis Estadístico

Método Kasiski

- Ejemplo: Texto cifrado: KSMEHZBBLKSMEMPOGAJXSEJCSFLZSY
  - Se buscan los poligramas más repetidos y las distancias medias para cada uno.
  - Se calculan los factores en cada caso y se descubren los factores más repetidos (candidatos a longitud de clave).
  - Se divide el criptograma según cada longitud (empezando por la mayor) y se compara la distribución de frecuencias con la del idioma usado.
- KS SM ME. Factores: 3,9
- Texto: TO BE OR NOT TO BE THAT IS THE QUESTION

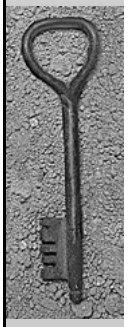


Método Kasiski

AN**YVG YS**TYN RPLWH RDTKX RNYPV QTGHP HZKFE YUMUS AYWVK
ZYEZM E**ZUDL JK**TUL JLKQB JUQVU ECKBN RCTHP KESXM AZOEN SXGOL
PGN**LE EBMMT GCSSV MRSEZ M**XHLP KJEJH TUPZU EDWKN NNRWA GEEXS
LK**ZUD LJK**FI XHTKP IAZMX FACWC TQIDU WBRRL TTKVN AJWVB
REAWT N**SEZM** OE**CSS VM**RSL JM**LEE BMMTG** AYVIY GHPEM YFARW AOAEL
UPIUA YYMGE EMJQK SFCGU GYBPJ BPZYP JASNN FSTUS ST**YVG YS**

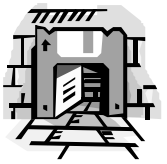
Repetición		*Primera*	*Segunda*	*Intervalo*	*Factores*
YVGYS	3	283	280	2 x 2 x 2 x 5 x 7	
ZUDLJK	52	148	96	2 x 2 x 2 x 2 x 2 x 2 x 3	
LEEBMMTG	99	213	114	2 x 3 x 19	
CSSVMRS		107	203	96	2 x 2 x 2 x 2 x 2x 3
SEZM	113	197	84	2 x 2 x 3 x 7	

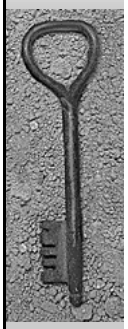
*If **signals** are to be displayed in the presence ofan enemy, they must be guarded by ciprés. The **ciphers** must be capable of **frequent changes**. The rules by which these **changes** are made must be simple. **Ciphers** are undiscoverable in proportion as their **changes** are **frequent** and as the messages in each **change** are brief.*
From Albert J. Myer's Manual of Signals.



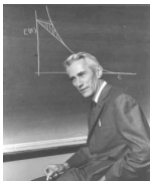
Bases Teóricas

1. Teoría de la Información.
2. Teoría de la Complejidad Computacional.
3. Teoría de Números.





Teoría de la Información

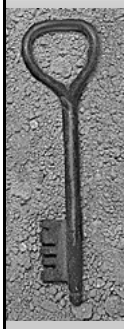


- Claude E. Shannon (1948)
- Seguridad teórica de los cifrados.

- **Información: disminución de incertidumbre** sobre un suceso: Mínimo número de bits necesarios para codificar todos los posibles significados de un mensaje.

$$I(E) = \log \frac{1}{P(E)}$$

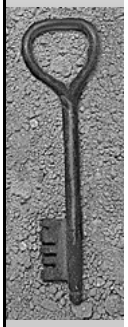
- Ejemplos:
  - –Campo Día tiene 3 bits de información ya que 000=Lunes,..., 110=Domingo.
  - –Campo Sexo contiene 1 bit de información ya que 0=Hombre, 1=Mujer



Teoría de la Información

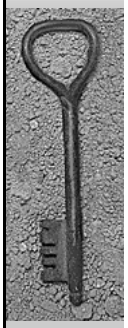
$$H(S) = \sum_{S} P(s_i) \log_2 \frac{1}{P(s_i)}$$

- **Entropía** de una fuente de información: Cantidad media de información por símbolo emitido.
  - $H(S)=\log_2(n)$, si n es el nº de valores equiprobables de S
- **Incertidumbre**: Nº de bits de texto original que hay que descifrar para recuperar el mensaje original
- **Redundancia** de un lenguaje: Diferencia entre el máximo nº de bits que puede codificarse en cada letra (supuesta equiprobable) y el nº de bits por letra del lenguaje



Teoría de la Información

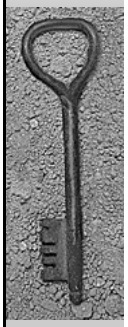
- Los lenguaje "naturales" poseen gran redundancia (información innecesaria y repetida).
- Maneras de ocultar la redundancia:
  - **Confusión:** Oculta la relación entre texto claro, criptograma y clave (sustitución).
  - **Difusión:** Dispersa la influencia de cada bit del texto claro a lo largo de todo el texto cifrado (transposición).



Teoría de la Información

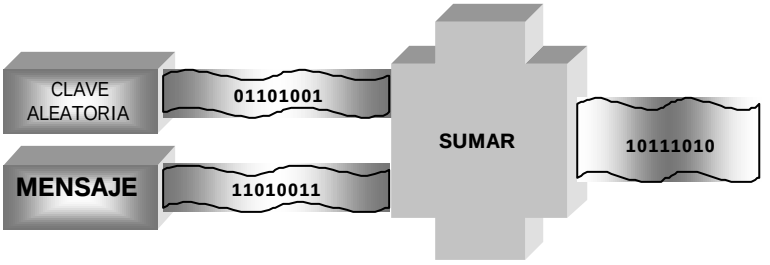
- Un cifrado tiene **secreto perfecto** si el texto cifrado no proporciona ninguna información sobre el texto original, es decir, si el texto claro es estadísticamente independiente del criptograma.

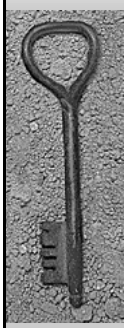
✓**Conclusión: La clave debe usarse una única vez y debe ser al menos de igual longitud que el texto claro**



Teoría de la Información

Secreto Perfecto: Cifrado de Vernam

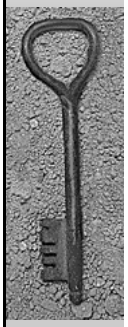




Teoría de la Complejidad

- La Tª de la información dice que todos los cifrados pueden romperse.
- La Tª de la complejidad dice si pueden romperse en la práctica.
- Todo cifrado está basado en un problema tal que el usuario que posee la clave puede resolverlo de forma eficiente mientras que un posible atacante no puede. (**Funciones unidireccionales**).
- La fortaleza de un cifrado viene dada por la potencia computacional necesaria para romperlo.
- *No basta con resolver un problema, la solución (algoritmo) ha de ser óptima.* ¿Qué algoritmo es mejor? Los compararemos usando sus tiempos de ejecución en el

Caso mejor Caso peor Caso promedio

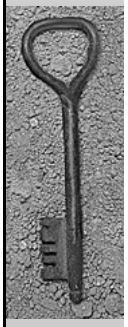


Teoría de la Complejidad

- La complejidad de un algoritmo se expresa en función de n, tamaño de la entrada, usando la notación O(), con el término que crece más rápido cuando n crece, ignorando todos los demás términos de orden inferior y constantes.

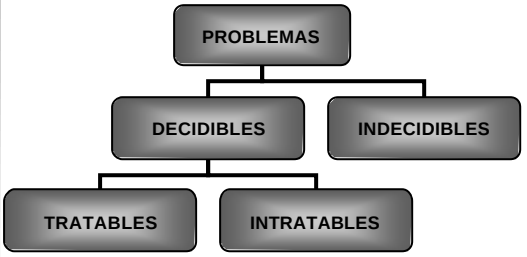
  Ej: Si la función complejidad es $4n^2+7n+12$, entonces se dice que la complejidad es $O(n^2)$

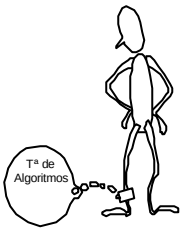
- Algoritmo **polinomial**: Su peor caso de ejecución es $O(n^k)$
- Algoritmo **exponencial**: Imposible de acotar por una función polinomial.
- Lo ideal para el diseñador de un cifrado es que los algoritmos para romperlo sean todos exponenciales



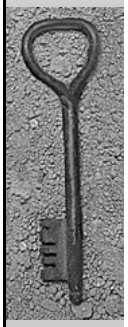
Teoría de la Complejidad

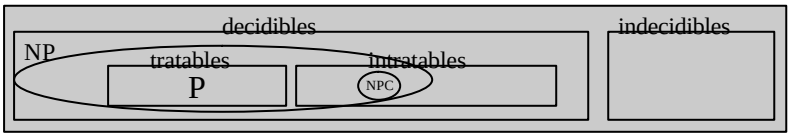
La Complejidad de un problema es la complejidad del mejor algoritmo que para la peor de las entradas resuelve dicho problema.





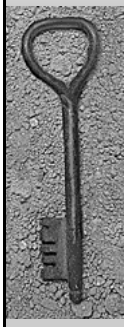
Teoría de la Complejidad





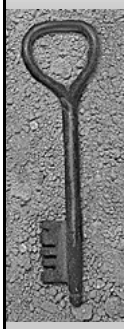
- Clase P: Problemas resolubles en tiempo polinomial.
- Clase NP: Problemas cuya solución puede verificarse en tiempo polinomial, empleando alguna información extra.
- Clase NP-Completa (NPC): Subconjunto de NP en el que todos los problemas son reducibles entre sí.
- Clase NP-dura: Problemas de búsqueda correspondientes a problemas NP-completos.

Teoría de Números



- **Aritmética modular:** Maneja un conjunto finito de enteros donde existen muchos problemas interesantes, se pueden realizar de manera eficiente cálculos muy complejos y existe la inversa de varias operaciones.
- **Relación de congruencia:** Dados dos números enteros a y b, se dice que a es congruente con b módulo n
  (**a ° b (mod n)**) sii existe algún entero k de manera que
  a – b = k* n (b es el resto de de a dividido por n).
- **Algoritmo de Euclides**: Para obtener mcd
  19=1x12+7; 12=1x7+5; 7=1x5+2; 5=2x2+1.

- **Cálculo de inversos** a $^{-1}$(mod n): Encontrar x tal que ax=1(mod n) : ax +kn =1, siendo a y x primos entre sí.
  Ej: Buscando 12^{-1}(mod 19):
  7=19-12; 5=12-(19-12)= 2x12-19; 2=19-12-(2x12-19)=
  3x12+2x19; 1=2x12-19-2x(-3x12+2x19)= **8**x12-5x19



Teoría de Números

- Calcular $a^x \pmod n$ rápidamente expresando x como suma de potencias de 2:

  $25=2^4+2^3+2^0 \Rightarrow a^{25} \pmod n = ((((a^2 x a)^2)^2)^2 a \pmod n$

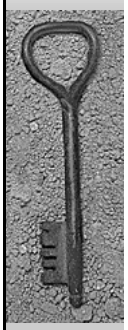
- Función fi de Euler: f (n)=Nº de enteros positivos menores que n y primos con n.

  Ej: Buscando $12^{-1} \pmod{19}$: $f(19)=18 \Rightarrow 12^{17} \pmod{19}$

- Residuos cuadráticos: a<n tal que $x^2=a \pmod n$,

  Si n=pq ⇒ Hay (p-1)(q-1)/4 residuos cuadráticos mod n,

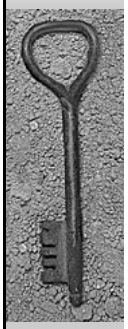
  Ej: residuos cuadráticos mod 35: 1,4,9,11,16,29



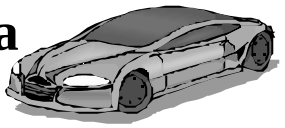
Algoritmo de Euclides

Para el cálculo del mcd(a,b) y/o el inverso de b mod a, siendo a>b:

- Inicializar x_0 (dividendo) y x_1 (divisor) como a y b
- Mientras el resto no dé 0, dividir x_{i-1} por x_i y asignar a x_{i+1} el valor del resto
- El mcd(a,b) es x_i
- Si mcd(a,b)=1, entonces para el cálculo del inverso:
  - Se define la variable $z_i = -\text{div}(x_{i-1}, x_i) \cdot z_{i-1} + z_{i-2}$, con $z_{-1}=0$, $z_0=1$
  - El inverso es z_{i-1}



Exponenciación Rápida



Para hallar $a^m \pmod n$

- Inicializar i=1, a_i y m_i como a y m, y $x_i = 1$
- Mientras $m_i \neq 0$, incrementar i:
  - mientras $m_i \equiv 0 \pmod 2$, asignar a m_i el valor $m_{i-1}/2$, a a_i el valor $a_{i-1}^2 \pmod n$, y mantener $x_i = x_{i-1}$
  - asignar a m_i el valor $m_i - 1$ y a x_i el valor $x_{i-1} \cdot a_{i-1} \pmod n$, y mantener $a_i = a_{i-1}$
- El resultado es x_i