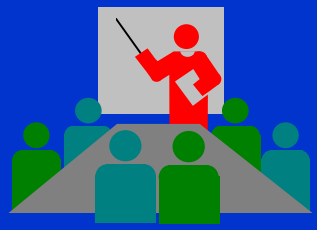
Capítulo 9
Sistemas de Cifra Clásicos

Seguridad Informática y Criptografía



Material Docente de
Libre Distribución

Ultima actualización del archivo: 01/03/06
Este archivo tiene: 41 diapositivas

Dr. Jorge Ramió Aguirre
Universidad Politécnica de Madrid

¿Le interesa la historia?

Si le interesa el tema de la historia de la criptología así como aquellas máquinas que se usaban desde tiempos remotos hasta mediados del siglo XX, un tema verdaderamente apasionante, anexo a este libro electrónico encontrará el documento de libre distribución “Criptografía Clásica” en formato Word y PDF, con más de 100 páginas y 70 ejemplos resueltos.

http://www.criptored.upm.es/guiateoria/gt_m001a.htm

Aunque su interés actual es mínimo, en estas diapositivas se ha incluido, a modo de resumen, lo más interesante de este tipo de cifra, lo que podrá servirle al menos como cultura general.

Encontrará más información y algunos sencillos ejemplos de cifra básica en el software que puede descargar desde la página Web:

http://www.abcdatos.com/tutoriales/tutorial/l10448.html

Cifradores e información en Web

- ✓ Existe una gran cantidad de sistemas y cifradores de los denominados clásicos.
- ✓ En este capítulo sólo se presentan la Escítala, Polybios, César, Afín, Vigenère, Playfair, Hill y Vernam, así como los ataques según métodos de Kasiski y Gauss Jordan.

Puede ampliar información y ver una interesante galería de fotografías sobre estas máquinas y pioneros de la criptografía en la página Web de la NSA, National Security Agency

http://www.nsa.gov/public/publi00007.cfm

Y la descripción de varios algoritmos en el siguiente enlace:

http://library.thinkquest.org/27158/concept1_1.html

Clasificación histórica de criptosistemas

La clasificación actual de los sistemas de cifra se basa en el tratamiento de la información (cifrado en bloque vs cifrado en flujo) o bien en el tipo de clave utilizada en la cifra (sistemas de clave secreta v/s sistemas de clave pública), pero según su relación con la historia de la criptografía podríamos clasificarlos como:

Sistemas de Cifra Clásicos versus Sistemas de Cifra Modernos

Esta no es ni mucho menos la mejor clasificación desde el punto de vista de la ingeniería y la informática ... pero permitirá comprobar el desarrollo de estas técnicas de cifra, hoy en día rudimentarias y simples, desde una perspectiva histórica y culturalmente interesante para un ingeniero. Además, nos permitirá criptoanalizar con cierta facilidad prácticamente todos estos sistemas y comprobar también las teorías de Shannon sobre las estadísticas del lenguaje.

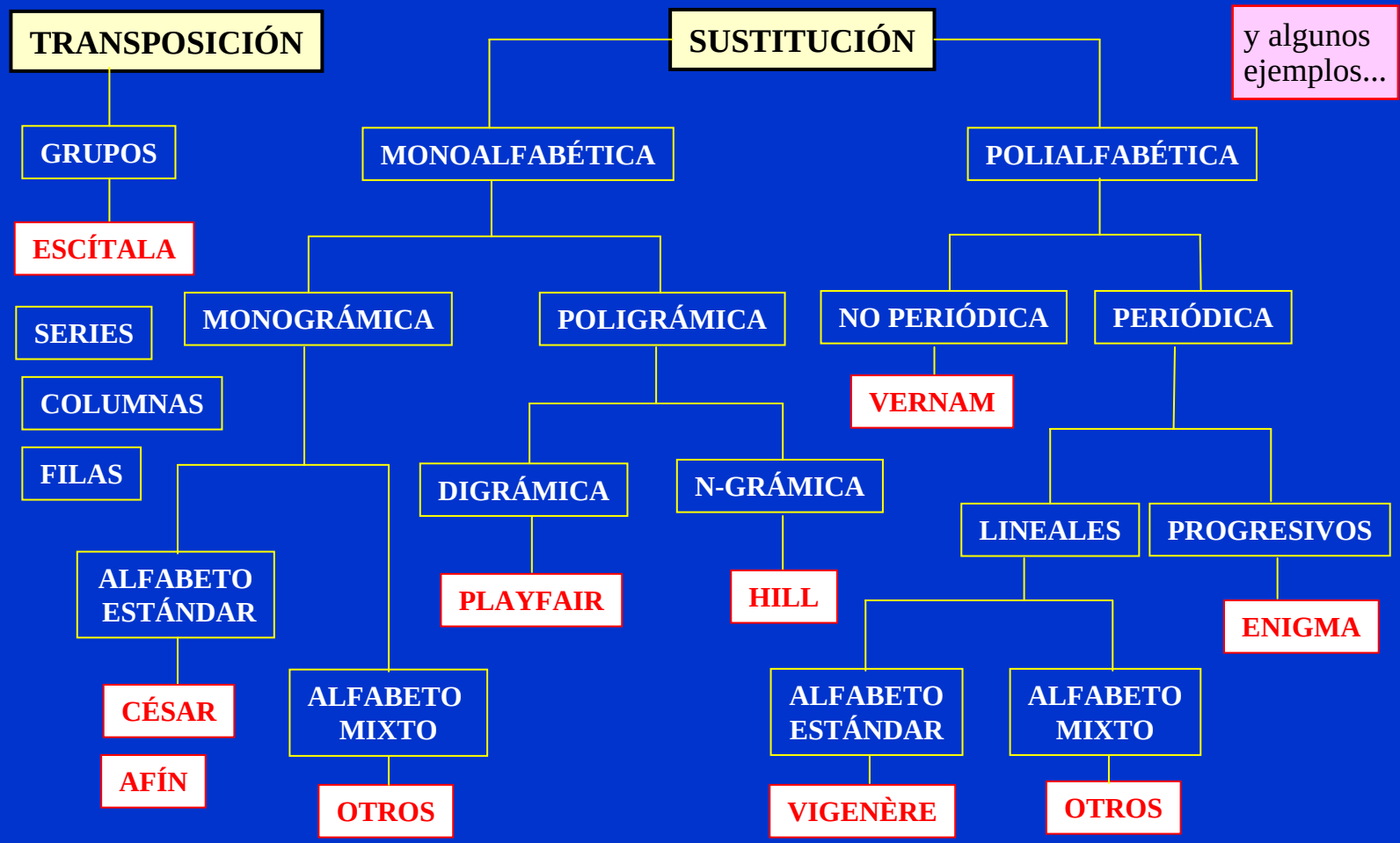
Una primera aproximación histórica

- El uso de técnicas criptográficas es casi tan antiguo como las culturas de los primeros pueblos de nuestro planeta.
- Ya en el siglo V antes de J.C. un pueblo griego usaba técnicas elementales de cifra para proteger su información.
- Se pretendía garantizar en aquellos días sólo la confidencialidad y la autenticidad de los mensajes. A finales del siglo XX se han añadido la disponibilidad y, últimamente, el no repudio.
- Los mayores avances se logran en la Primera y Segunda Guerra Mundiales, especialmente durante y después de esta última. Los países en conflicto poseían verdaderas empresas con un gran número de matemáticos, cuya función era romper los mensajes cifrados de los teletipos intercambiados por sus enemigos.

Herramientas de la criptografía clásica

- Tanto máquinas, artilugios de cifra, como los algoritmos que trabajaban matemáticamente dentro de un cuerpo finito n, hacen uso de dos técnicas básicas orientadas a caracteres y que, muchos siglos después, las propondrá Shannon como herramientas para fortalecer la cifra:
  - Técnicas de sustitución: Los caracteres o letras del mensaje en claro se modifican o sustituyen por otros elementos o letras en la cifra. El criptograma tendrá entonces caracteres distintos a los que tenía el mensaje en claro.
  - Técnicas de transposición o permutación: los caracteres o letras del mensaje en claro se redistribuyen sin modificarlos y según unas reglas, dentro del criptograma. El criptograma tendrá entonces los mismos caracteres del mensaje en claro pero con una distribución o localización diferente.

Clasificación de los criptosistemas clásicos



Hitos históricos en la criptografía

- La criptografía clásica abarca desde tiempos inmemoriales hasta la mitad del siglo XX.
- El punto de inflexión en esta clasificación la marcan tres hechos relevantes:
  - En el año 1948 se publica el estudio de Claude Shannon sobre la Teoría de la Información.
  - En 1974 aparece el estándar de cifra DES.
  - Y en el año 1976 se publica el estudio realizado por Whitfield Diffie y Martin Hellman sobre la aplicación de funciones matemáticas de un solo sentido a un modelo de cifra, denominado cifrado con clave pública.

CIFRADO DIGITAL

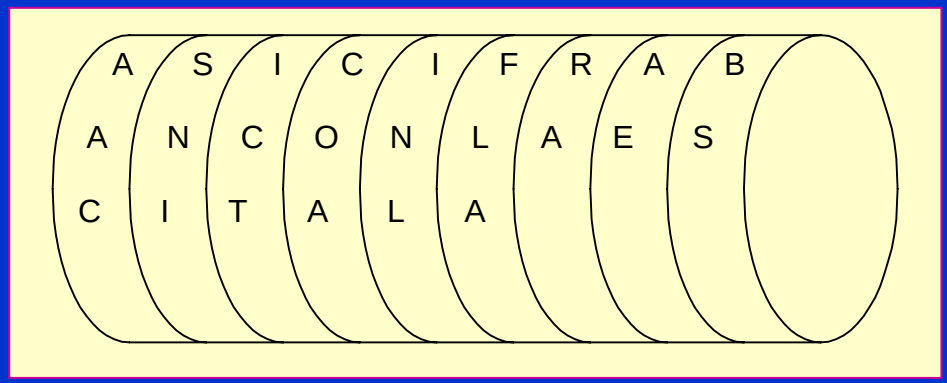
http://www.cs.jhu.edu/~rubin/courses/sp03/papers/diffie.hellman.pdf

Primer cifrador por transposición: escítala

- La escítala era usada en el siglo V a.d.C. por el pueblo griego de los lacedemonios. Consistía en un bastón en el que se enrollaba una cinta de cuero y luego se escribía en ella el mensaje de forma longitudinal.
- Al desenrollar la cinta, las letras aparecerán desordenadas.
- Para descifrar el criptograma y recuperar el mensaje en claro habrá que enrollar dicha cinta en un bastón con el mismo diámetro que el usado en el extremo emisor y leer el mensaje de forma longitudinal. La clave del sistema se encuentra en el diámetro del bastón. Se trata de una cifra por transposición pues los caracteres del criptograma son los mismos que en el texto en claro pero están distribuidos de otra forma dentro del criptograma.

Método de cifra de la escítala

Bastón y cinta para cifrar



En ese bastón residía la fortaleza de un pueblo.

Por ello, y como símbolo de poder, el bastón de mando que se le entrega al alcalde de una ciudad en la ceremonia de su nombramiento, proviene de estos tiempos tan remotos.

El texto en claro es:

M = ASI CIFRABAN CON LA ESCITALA

El texto cifrado o criptograma será:

C = AAC SNI ICT COA INL FLA RA AE BS

Primer cifrador por sustitución: Polybios

Es el cifrador por sustitución de caracteres más antiguo que se conoce (siglo II a.d.C.) pero como duplica el tamaño del texto en claro, con letras o números, ... no fue tan buena la idea.

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

	1	2	3	4	5
1	*A*	*B*	*C*	*D*	*E*
2	*F*	*G*	*H*	*IJ*	*K*
3	*L*	*M*	*N*	*O*	*P*
4	*Q*	*R*	*S*	*T*	*U*
5	*V*	*W*	*X*	*Y*	*Z*

M_1 = QUÉ BUENA IDEA

C_1 = DA DE AE AB DE AE

CC AA BD AD AE EA

M_2 = LA DEL GRIEGO

C_2 = 31 11 14 15 31 22

42 24 15 22 34

El cifrador del César

En el siglo I a.d.C., Julio César usaba este cifrador. El algoritmo consiste en el desplazamiento de tres espacios hacia la derecha de los caracteres del texto en claro. Es un cifrador por sustitución monoalfabético en el que las operaciones se realizan módulo n, siendo n el número de elementos del alfabeto (en aquel entonces el latín).

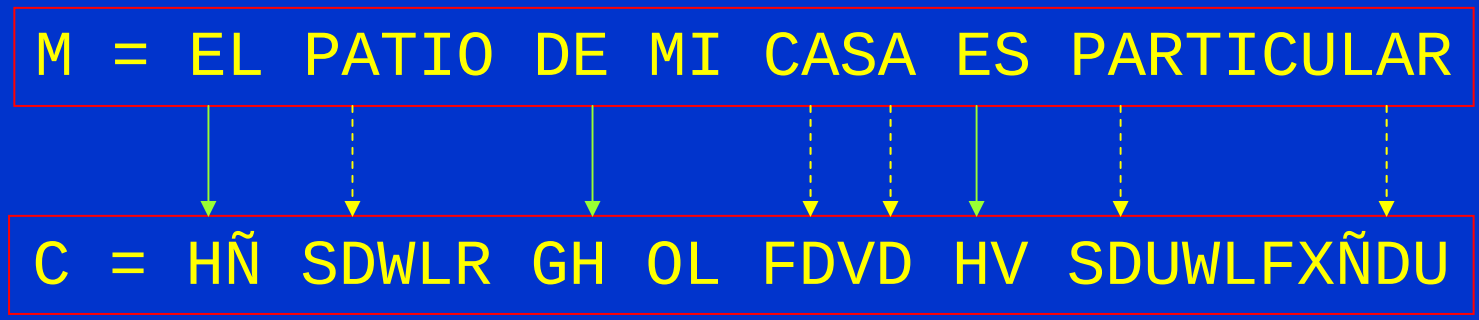
	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26
M_i	A	B	C	D	E	F	G	H	I	J	K	L	M	N	Ñ	O	P	Q	R	S	T	U	V	W	X	Y	Z
C_i	D	E	F	G	H	I	J	K	L	M	N	Ñ	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C

Alfabeto de cifrado del César para castellano mod 27

Ejemplo de cifra del César en mod 27

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

Cifrado: $C_i = M_i + 3 \bmod 27$ Descifrado: $M_i = C_i - 3 \bmod 27$



Cada letra se cifrará siempre igual. Es una gran debilidad y hace que este sistema sea muy vulnerable y fácil de atacar, simplemente usando las estadísticas del lenguaje. Puede ver la tabla de frecuencias típicas del lenguaje castellano en el capítulo 21 de este libro.

Criptoanálisis del cifrador por sustitución

A	B	C	D	E	F	G	H	I	J	K	L	M	N	Ñ	O	P	Q	R	S	T	U	V	W	X	Y	Z
00	01	02	03	04	05	06	07	08	09	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26

Cifrado: $C_i = (M_i + b) \bmod 27$ Descifrado: $M_i = (C_i - b) \bmod 27$

La letra más frecuente del criptograma la hacemos coincidir con la más frecuente del lenguaje, la letra E, y encontramos así b.

C = LZAHL ZBTHW YBLIH XBLKL ILYOH ZLYCH ROKH

Frecuencias observadas en el criptograma: L (7); H (6); Z (3); B (3); Y (3); I (2); K (2); O (2); A (1); T (1); W (1); X (1); C (1); R (1).

Es posible que la letra E del lenguaje se cifre como L. Comprobamos además si la letra A (segunda más frecuente) se cifra como H:

$E + b \bmod 27 = L \Rightarrow b = L - E \bmod 27 = 11 - 4 \bmod 27 = 7$ 

$A + b \bmod 27 = H \Rightarrow b = H - A \bmod 27 = 7 - 0 \bmod 27 = 7$ 

M = ESTA ES UNA PRUEBA QUE DEBERIA SER VALIDA

Cifrador por sustitución afín mod 27

Cifrado: $C_i = a*M_i + b \bmod 27$

Descifrado: $M_i = (C_i - b) * a^{-1} \bmod 27$ donde $a^{-1} = \text{inv}(a, 27)$

- El factor de multiplicación a deberá ser primo relativo con el cuerpo n (en este caso 27) para que exista el inverso a^{-1}.
- El factor de desplazamiento puede ser cualquiera: $0 \leq b \leq 26$.

El ataque a este sistema es también muy elemental. Se relaciona el elemento más frecuente del criptograma a la letra E y el segundo a la letra A, planteando un sistema de 2 ecuaciones. Si el texto tiene varias decenas de caracteres este ataque prospera; caso contrario, podría haber ligeros cambios en esta distribución de frecuencias.

Criptoanálisis a la cifra afín mod 27

C: NAQÑF EKNDP NCIVU FPUAN EJUIP FCNER NFRÑF UNPLN
AFPFQ TFPEI JRTÑE FPKÑI KTAPF LIKIÑ AIPÑU RCUJI
PCIVU CUNER IRLNP TJIAF NEOIÑ CFLNC NLUFA TEF

Caracteres más frecuentes en el criptograma: F = 14; N = 13; I = 12

Con E y A las más frecuentes, el ataque falla. En un segundo intento suponemos la letra A más frecuente que la E, luego:
F = (a∗A + b) mod 27 ⇒ (a∗0 + b) mod 27 = 5 ⇒ b = 5
N = (a∗E + b) mod 27 ⇒ (a∗4 + 5) mod 27 = 13
Entonces a = (13-5) ∗ inv (4, 27) mod 27 = 8 ∗ 7 mod 27 = 2

$C_i = (2*M_i + 5) \bmod 27 \Rightarrow M_i = (C_i - 5)*\text{inv}(2, 27) = (C_i - 5)*14 \bmod 27$

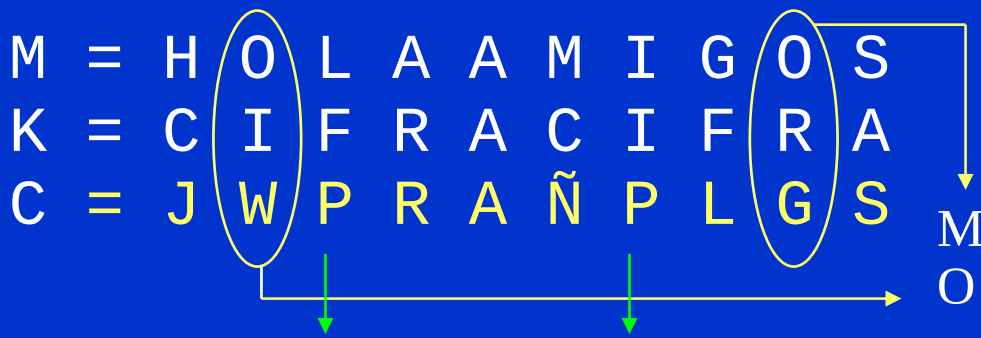
M: EL GRAN PEZ SE MOVÍA SILENCIOSAMENTE A TRAVÉS DE LAS AGUAS NOCTURNAS, PROPULSADO POR LOS RÍTMICOS MOVIMIENTOS DE SU COLA EN FORMA DE MEDIA LUNA.
(Comienzo de la novela Tiburón de Peter Benchley)

El cifrador de Vigenère

Este cifrador polialfabético soluciona la debilidad del cifrado del César en que una letra se cifra siempre igual. Se usa una clave K de longitud L y se cifra carácter a carácter sumando módulo n el texto en claro con los elementos de esta clave.

$$C_i = M_i + K_i \bmod 27$$

Sea K = CIFRA y el mensaje M = HOLA AMIGOS



sumando mod 27...

Más de un alfabeto: la letra O se cifra de forma distinta.

Observe que el criptograma P se obtiene de un texto L y de un texto I.

¿Es Vigenère un algoritmo seguro?

Si la clave de Vigenère tiene mas de 6 caracteres distintos, se logra una distribución de frecuencias en el criptograma del tipo normal, es decir más o menos plana, por lo que se logra difuminar la redundancia del lenguaje.

Aunque pudiera parecer que usando una clave larga y de muchos caracteres distintos, y por tanto varios alfabetos de cifrado, Vigenère es un sistema de cifra seguro, esto es falso.

La redundancia del lenguaje unido a técnicas de criptoanálisis muy sencillas, como los métodos de Kasiski y del Índice de Coincidencia, permiten romper la cifra y la clave de una manera muy fácil y con mínimos recursos. En la siguiente diapositiva veremos un ataque por el método de Kasiski.

Ataque por el método de Kasiski

- El método de Kasiski consiste en buscar repeticiones de cadenas de caracteres en el criptograma. Si estas cadenas son mayores o iguales a tres caracteres y se repiten más de una vez, lo más probable es que esto se deba a cadenas típicas del texto en claro (trigramas, tetragramas, etc., muy comunes) que se han cifrado con una misma porción de la clave.
- Si se detectan estas cadenas, la distancia entre las mismas será múltiplo de la longitud de la clave. Luego, el máximo común divisor entre esas cadenas es un candidato a ser la longitud de la clave, digamos L.
- Dividimos el criptograma en L subcriptogramas que entonces han sido cifrados por una misma letra de la clave y en cada subcriptograma hacemos un ataque simple ahora de tipo estadístico monoalfabético.
- La idea es buscar ahora a través de los tres caracteres más frecuentes en cada subcriptograma las posiciones relativas de las letras A, E y O que en castellano están separadas por 4 y 11 espacios. La letra de la posición que ocupe la letra A (A = 0) será entonces la letra clave correspondiente.

Cadenas repetidas en ataque de Kasiski

Sea el criptograma C de 404 caracteres que vamos a criptoanalizar el siguiente:

```
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 VAEEP 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.
```

Entre otras, se observan las siguientes cadenas (subrayadas) en el criptograma:

- 3 cadenas GGMP, separadas por 256 y 104 posiciones.
- 2 cadenas YEDS, separadas por 72 espacios.
- 2 cadenas HASE, separadas por 156 espacios.
- 2 cadenas VSUE, separadas por 32 espacios.

Luego el período de la clave puede ser mcd (256, 104, 72, 156, 32) = 4. La clave tendrá cuatro caracteres, por lo tanto tomaremos del criptograma el carácter 1º, el 5º, el 9º, etc. para formar el primer subcriptograma C_A; luego el 2º, el 6º, el 10º, etc. para formar el subcriptograma C_B, y lo mismo para subcriptogramas C_C y C_D.

Paso a cifrado monoalfabético en Kasiski

Tenemos ahora 4 subcriptogramas de sólo 101 letras c/u (muy importante tenerlo en cuenta en las estadísticas) que han sido cifrados con la misma letra de la clave:

C_A = PQAAEPDMRÑEEDCNUSRIECNIONSAAETLUOLAUIEULMNIIEAAOOLU
MNARSOMRSISERNAISIRTMDTOORLIORRENENOAVSNIAEOFAMTEI

C_B = BVDÑTSBPPPDÑPPPBFDPQBUFNUEZCDFBÑMBEÑSFNPBBÑBÑNMKDPF
QFSJFTBPUNJMBNGDUNUFPFSSÑRPFTPJTBTETTJFUBSUTFTPBÑE

C_C = VISSSIGSWWSDCQWZNMWVOEQMVIYESPHEEXEEEWMQRPMVISTMSWO
MOEWQWJWEQEGDISSETEGOOSETYWWGQSXLGMXOHHECEEIGGIWEE

C_D = RCKDJEGLRYDRRMKVVTUVVDLWRKEYEHGSHVPLVHCPRVTVDJJDEIZ
VHSRCVGVXRUGGLJVEGEGRGTQGVJXGRKRZGUJRRVJHHUEYGKUNU

La frecuencia relativa observada en cada uno de los subcriptogramas es:

	A	B	C	D	E	F	G	H	I	J	K	L	M	N	Ñ	O	P	Q	R	S	T	U	V	W	X	Y	Z
C_A	12	0	2	3	12	1	0	0	11	0	0	5	6	9	1	10	2	1	9	7	4	5	1	0	0	0	0
C_B	0	14	1	6	4	12	1	0	0	4	1	0	3	6	8	0	14	2	1	6	9	7	1	0	0	0	1
C_C	0	0	2	2	18	0	7	3	7	1	0	1	7	1	0	6	2	6	1	12	3	0	4	12	3	2	1
C_D	0	0	3	5	7	0	12	6	1	7	5	4	1	1	0	0	2	1	13	2	3	6	14	1	2	3	2

Luego, la letra más frecuente del subcriptograma debería corresponder a la letra E del texto en claro, la segunda a la letra A y la tercera a la letra O. ⟶

La regla AEO en el ataque de Kasiski

- Si la posición relativa de la letra A es el valor 0, entonces la letra E está cuatro espacios a la derecha de la A (m+4 mod 27) y la letra O está 15 espacios a la derecha de la letra A (m+15 mod 27) y a 11 de la letra E.
- Buscaremos en cada subcriptograma C_i las tres letras más frecuentes y que cumplan además con esa distribución: $0 \rightarrow +4 \rightarrow +11 \bmod 27$.
- Es suficiente contar con estas tres letras para que el ataque prospere. No obstante, podemos afinar un poco más el ataque si tomamos en cuenta la siguiente letra frecuente en castellano S, en la posición (m+19) mod 27.

En el ejemplo para C_A se observa que la única solución que cumple con esto es la que coincide la AEO (12, 12, 10) luego la letra clave sería la A. Para C_B elegimos BFP (14, 12, 14) por lo que la letra clave sería B. Para C_C elegimos EIS (18, 7, 12) por lo que la letra clave sería E. Para C_D elegimos RVG (13, 14, 12) por lo que la letra clave sería R.

Con la clave K = ABER obtenemos “Para que la cosa no me sorprenda...”. Al ser éste un texto largo y con sentido, hemos encontrado la clave ✌. (artículo del periodista Andrés Aberasturi sobre la Navidad, España, año 1995)

El índice de coincidencia IC

El estudio del índice IC queda fuera del contexto de estos apuntes. Si bien tiene relación con el número de alfabetos, no es efectivo como Kasiski.

$$IC = \sum_{i=0}^{26} p_i^{\,2}$$ para castellano mod 27: $IC = p_A^{\,2} + p_B^{\,2} + ... + p_Z^{\,2} = 0{,}072$

Si el IC es menor que 0,5 es muy probable que no se trate de un cifrador monoalfabético sino polialfabético con un periodo 2 o mayor.

Así, cuando encontramos una longitud L de la clave por el método de Kasiski y rompemos el criptograma en L subcriptogramas, aplicando el concepto del índice de coincidencia IC podemos comprobar que cada uno de ellos se trata efectivamente de un cifrado monoalfabético cuando para cada subcriptograma este valor se acerca a 0,072 o lo supera.

En el ejemplo anterior, una vez roto el criptograma en cuatro tenemos: $IC_{CA} = 0{,}080$; $IC_{CB} = 0{,}091$; $IC_{CC} = 0{,}083$; $IC_{CD} = 0{,}082$ ... perfecto

Cifrador poligrámico de Playfair

Los cifrados anteriores se hacían carácter a carácter, es decir eran monográmicos. Para aumentar la seguridad de la cifra y romper las estadísticas, podemos cifrar por poligramas, bloques de caracteres.

Un cifrador inventado a finales del siglo XIX es el de Playfair que trabaja con una matriz de 5x5 letras, cifrando por digramas. Si el texto en claro tiene un número impar de elementos, se rellena con una letra preestablecida, por ejemplo la letra X.

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

- Si M_1M_2 están en la misma fila, C_1C_2 son los dos caracteres de la derecha.
- Si M_1M_2 están en la misma columna, C_1C_2 son los dos caracteres de abajo.
- Si M_1M_2 están en filas y columnas distintas, C_1C_2 son los dos caracteres de la diagonal, desde la fila de M_1.

Ejemplo de cifra con Playfair

Si la clave K = BEATLES y eliminamos la letra Ñ (inglés), cifre el mensaje M = WITH A LITTLE HELP FROM MY FRIENDS.

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

Se rompe la doble MM agregando una X y se rellena al final también con X

M = WI TH AL IT TL EH EL PF RO MX MY FR IE ND SX
C = EP BM TB ME LB BI AB RC UP KY RT MY PC KG DV

Estos sistemas también son criptoanalizables pues en el criptograma C persisten algunas propiedades del lenguaje; en este caso la distribución de digramas típicos; por ejemplo en el castellano en, de, mb, etc.

El cifrador de matrices de Hill

En 1929 el matemático Lester Hill propone un sistema de cifra usando una matriz como clave, cifrando Ngramas de forma que:

$$\begin{pmatrix} C_1 \\ C_2 \\ C_3 \\ .. \\ C_N \end{pmatrix} = \begin{pmatrix} k_{11} & k_{12} & k_{13} & \dots & k_{1N} \\ k_{21} & k_{22} & k_{23} & \dots & k_{2N} \\ k_{31} & k_{32} & k_{33} & \dots & k_{3N} \\ .. & .. & .. & & .. \\ k_{N1} & k_{N2} & k_{N3} & \dots & k_{NN} \end{pmatrix} X \begin{pmatrix} M_1 \\ M_2 \\ M_3 \\ .. \\ M_N \end{pmatrix} \quad \text{mod n}$$

La matriz clave K debe tener inversa K^{-1} en el cuerpo de cifra n. Luego, como $K^{-1} = T_{ADJ(K)}/|K|$ mod n, en donde ADJ(K) es la matriz adjunta, T es la traspuesta y |K| el determinante, este último valor |K| no podrá ser cero ni tener factores en común con n puesto que está en el denominador (concepto de inverso ya visto).
Si el texto en claro no es múltiplo del bloque N, se rellena con caracteres predeterminados, por ejemplo la letra X o la Z.

Ejemplo de cifrado de Hill

Sea M = AMIGO CONDUCTOR y la clave K la que se muestra:

$$\begin{pmatrix} C_1 \\ C_2 \\ C_3 \end{pmatrix} = \begin{pmatrix} 16 & 4 & 11 \\ 8 & 6 & 18 \\ 15 & 19 & 15 \end{pmatrix} \times \begin{pmatrix} 0 \\ 12 \\ 8 \end{pmatrix} \text{ mod } 27$$

K = PELIGROSO será la clave simbólica. Se cifrará el primer trigrama: AMI = 0, 12, 8.

M = AMI GOC OND UCT ORZ

$C_1 = (16*0 + 4*12 + 11*8) \text{ mod } 27 = 136 \text{ mod } 27 = 1 = B$

$C_2 = (8*0 + 6*12 + 18*8) \text{ mod } 27 = 216 \text{ mod } 27 = 0 = A$

$C_3 = (15*0 + 19*12 + 15*8) \text{ mod } 27 = 348 \text{ mod } 27 = 24 = X$

C = BAX PMA BJE XAF EUM (compruebe Ud. los demás trigramas)

Para descifrar encontramos $K^{-1} = \text{inv}(K, 27) = K^{-1} = T_{ADJ(K)}/|K| \text{ mod } n$

$|K| = 16(6*15 - 19*18) - 4(8*15 - 15*18) + 11(8*19 - 15*6) \text{ mod } 27 = 4$

Encontramos luego la matriz adjunta de K, la trasponemos cambiando filas por columnas y la multiplicamos por inv (|K|, 27) = inv (4, 27) = 7 con lo que se obtiene la matriz que se indica (hágalo Ud.)

Ejemplo de descifrado de Hill

$$\begin{pmatrix} M \end{pmatrix} = \begin{pmatrix} K^{-1} \end{pmatrix} \text{ x } \begin{pmatrix} C \end{pmatrix} \text{ mod n} \quad \text{y} \quad K^{-1} = \begin{pmatrix} 18 & 26 & 15 \\ 24 & 6 & 13 \\ 11 & 24 & 10 \end{pmatrix}$$

C = BAX PMA BJE XAF EUM y la clave K^{-1} es la que se muestra:

$$\begin{pmatrix} M_1 \\ M_2 \\ M_3 \end{pmatrix} = \begin{pmatrix} 18 & 26 & 15 \\ 24 & 6 & 13 \\ 11 & 24 & 10 \end{pmatrix} \text{ x } \begin{pmatrix} 1 \\ 0 \\ 24 \end{pmatrix} \text{ mod } 27$$

Descifrado del primer trigrama del criptograma: BAX = 1, 0, 24.

C = BAX PMA BJE XAF EUM

$M_1 = (18*1 + 26*0 + 15*24) \text{ mod } 27 = 378 \text{ mod } 27 = 0 = A$

$M_2 = (24*1 + 6*0 + 13*24) \text{ mod } 27 = 336 \text{ mod } 27 = 12 = M$

$M_3 = (11*1 + 24*0 + 10*24) \text{ mod } 27 = 251 \text{ mod } 27 = 8 = I$

M = AMI GOC OND UCT ORZ (compruebe Ud. los demás trigramas)

¿Es seguro el cifrador de Hill?

Si con el sistema de Hill se cifran bloques de 8 caracteres, incluso en un cuerpo tan pequeño como n = 27 el espacio de claves aumenta de forma espectacular, comparable con DES.

Si el módulo de cifra es un primo p, entonces el número de claves válidas es cercano al máximo posible: p^x donde $x = d^2$, con d el tamaño de N-grama o de la matriz clave.

No obstante, el sistema no es seguro. Debido a su linealidad será muy fácil hacer un ataque con texto claro conocido según el método de Gauss Jordan y encontrar así la matriz clave K.

Esto es debido a que aparecen los llamados vectores unitarios en el criptograma o en el texto en claro, o bien los obtenemos aplicando este método.

Ataque al cifrado de Hill por Gauss Jordan

El método consiste en escribir una matriz 2N-grámica con los elementos del texto en claro y los elementos del criptograma. En esta matriz realizamos operaciones lineales (multiplicar filas por un número y restar filas entre sí) con el objeto de obtener los vectores unitarios.

Por ejemplo podemos romper la matriz clave K teniendo:

M = ENU NLU GAR DEL AMA NCH ADE CUY ONO ...
C = WVX IDQ DDO ITQ JGO GJI YMG FVC UÑT ...

$$\left(\begin{array}{ccc|ccc} E & N & U & W & V & X \\ N & L & U & I & D & Q \\ G & A & R & D & D & O \\ D & E & L & I & T & Q \\ A & M & A & J & G & O \\ N & C & H & G & J & I \\ A & D & E & Y & M & G \\ C & U & Y & F & V & C \\ O & N & O & U & Ñ & T \end{array}\right) = \left(\begin{array}{ccc|ccc} 4 & 13 & 21 & 23 & 22 & 24 \\ 13 & 11 & 21 & 8 & 3 & 17 \\ 6 & 0 & 18 & 3 & 3 & 15 \\ 3 & 4 & 11 & 8 & 20 & 17 \\ 0 & 12 & 0 & 9 & 6 & 15 \\ 13 & 2 & 7 & 6 & 9 & 8 \\ 0 & 3 & 4 & 25 & 12 & 6 \\ 2 & 21 & 25 & 5 & 22 & 2 \\ 15 & 13 & 15 & 21 & 14 & 20 \end{array}\right)$$

Operaciones en la matriz de Gauss Jordan

Vamos a dejar en la primera columna un número uno en la fila primera y todas las demás filas un cero. Luego multiplicamos el vector (4 13 21 | 23 22 24) por el inv (4, 27) = 7. Así obtenemos 7(4 13 21 | 23 22 24) mod 27 = (1 10 12 | 26 19 6). Si esto no se puede hacer con la primera fila movemos los vectores. Hecho esto vamos restando las filas respecto de esta primera como se indica:

$$\left(\begin{array}{ccc|ccc} 4 & 13 & 21 & 23 & 22 & 24 \\ 13 & 11 & 21 & 8 & 3 & 17 \\ 6 & 0 & 18 & 3 & 3 & 15 \\ 3 & 4 & 11 & 8 & 20 & 17 \\ 0 & 12 & 0 & 9 & 6 & 15 \\ 13 & 2 & 7 & 6 & 9 & 8 \\ 0 & 3 & 4 & 25 & 12 & 6 \\ 2 & 21 & 25 & 5 & 22 & 2 \\ 15 & 13 & 15 & 21 & 14 & 20 \end{array}\right)$$

a) 2^a fila = 2^a fila – 13∗1^a fila mod 27
b) 3^a fila = 3^a fila – 6∗1^a fila mod 27
c) 4^a fila = 4^a fila – 3∗1^a fila mod 27
d) 5^a fila ya tiene un 0
e) 6^a fila = 6^a fila – 13∗1^a fila mod 27
f) 7^a fila ya tiene un 0
g) 8^a fila = 8^a fila – 2∗1^a fila mod 27
h) 9^a fila = 9^a fila – 15∗1^a fila mod 27

Matriz clave de Hill criptoanalizada

Repetimos este procedimiento ahora para algún vector en cuya segunda columna tenga un número con inverso en 27 y lo mismo para la tercera columna, moviendo si es preciso los vectores.

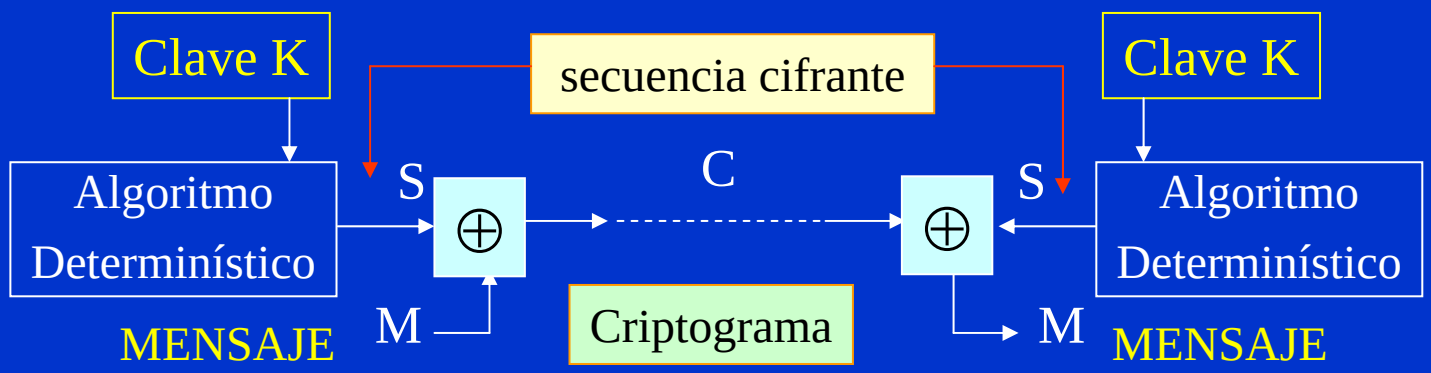
Como la mitad izquierda de la matriz 2N era el texto el claro, la parte derecha de la matriz con vectores unitarios corresponderá a la traspuesta de la clave.

$$\left(\begin{array}{ccc|ccc} 1 & 0 & 0 & 2 & 5 & 7 \\ 0 & 1 & 0 & 3 & 5 & 8 \\ 0 & 0 & 1 & 4 & 6 & 9 \\ 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 \end{array}\right) \Rightarrow \quad K = \begin{pmatrix} 2 & 3 & 4 \\ 5 & 5 & 6 \\ 7 & 8 & 9 \end{pmatrix}$$

Compruebe que la clave es la utilizada en este cifrado.

El cifrador de Vernam

- En 1917 Gilbert Vernam propone un cifrador por sustitución binaria con clave de un solo uso (one-time pad) basado en el código Baudot de 5 bits:
  - La operación de cifra es la función XOR.
  - Usa una secuencia cifrante binaria y aleatoria S que se obtiene a partir de una clave secreta K compartida por emisor y receptor.
  - El algoritmo de descifrado es igual al de cifrado por la involución de la función XOR.
  - La clave será tan larga o más que el mensaje y se usará una sola vez.



Ejemplo de cifrado de Vernam

Usando el código Baudot (vea los códigos en la tabla de Baudot que encontrará en el Capítulo 21) se pide cifrar:

M = BYTES
K = VERNAM

Solución:

B⊕V = 11001⊕11110 = 00111 = U
Y⊕E = 10101⊕00001 = 10100 = H
T⊕R = 10000⊕01010 = 11010 = G
E⊕N = 00001⊕01100 = 01101 = F
S⊕A = 00101⊕00011 = 00110 = I
C = UHGFI

El esquema de Vernam es el único cifrador matemáticamente seguro y, por tanto, imposible de criptoanalizar pues la clave K se usa una sola vez (one-time pad), es aleatoria y tanto o más larga que el propio mensaje. En este caso, no cabe ningún ataque por estadísticas del lenguaje o por correlación de bits.

http://www.pro-technix.com/information/crypto/pages/vernam_base.html

Fin del capítulo

Cuestiones y ejercicios (1 de 3)

LAS SIGUIENTES PREGUNTAS ESTÁN RELACIONADAS CON ESTOS APUNTES, EL LIBRO ELECTRÓNICO DE CRIPTOGRAFÍA CLÁSICA Y EL SOFTWARE DE PRÁCTICAS CRIPTOCLÁSICOS QUE SE HA COMENTADO.

1. ¿Qué significa cifrar por sustitución y qué por transposición?
2. ¿Por qué que el método escítala es un cifrado por permutación?
3. ¿Cuál es la peor debilidad que tiene el sistema de cifra del César?
4. Ciframos el mensaje M = HOLA QUE TAL con un desplazamiento de 6 caracteres, ¿cuál es el criptograma? ¿Y si desplazamos 27?
5. ¿Por qué no podemos cifrar en el cuerpo n = 27 con la función de cifra C = (12M + 5) mod n? ¿Qué condición deberá cumplirse?
6. ¿Cómo podríamos atacar un sistema de cifra tipo César? ¿Y si la cifra es de tipo afín como el de la pregunta anterior?

Cuestiones y ejercicios (2 de 3)

7. Cifre el mensaje M = VAMOS A VERLO con un sistema afín siendo el valor a = 5 y b = 2, usando sólo operaciones modulares.
8. En un sistema de cifra de Vigenère la clave a usar puede ser CERO o bien COMPADRE, ¿cuál de las dos usaría y por qué?
9. Cifre según Vigenère el mensaje M = UN VINO DE MESA con la clave K = BACO sin usar la tabla, sólo con operaciones modulares.
10. ¿Por qué se dice que Vigenère es un cifrador polialfabético?
11. ¿Cómo podríamos atacar un cifrado polialfabético periódico?
12. Cifre con el método de Vernam binario en mensaje M = VIDA y clave K = TACOS suponiendo texto ASCII. ¿Y si la clave es ahora K = TACO? ¿Cómo se comporta este cifrador si K es aleatoria?
13. ¿Qué significa cifrar por homófonos? ¿Qué es el cifrado de Beale?

Cuestiones y ejercicios (3 de 3)

14. Nombre dos máquinas de cifrar que se usaron en la Segunda Guerra Mundial y diga de forma sencilla cómo funcionaban.
15. Se cifra por permutaciones usando para ello una distribución en columnas con clave. ¿Qué similitud tendrá luego este sistema de cifra con algunas operaciones hechas en el DES?
16. Cifre con Hill digrámico el mensaje mod 27 M = ADIOS AMIGO. ¿Qué matriz simbólica puede usar: GATO, GOTA, MISA o MESA?
17. Cifre y descifre con la matriz trigrámica simbólica PELIGROSO el mensaje HOY ES UN HERMOSO DIA.
18. Si K puede ser tan grande, ¿por qué no es segura la cifra de Hill?
19. ¿Qué significan los vectores unitarios? ¿Es fácil encontrarlos?
20. ¿Cómo funciona el ataque de Gauss Jordan? Obtenga la matriz clave del ejercicio 17 mediante Gauss Jordan.

Use el portapapeles

Prácticas del tema 9 (1/4)

Software CripClas: http://www.criptored.upm.es/software/sw_m001c.htm

1. Con el algoritmo del César, b = 3, cifre, descifre y criptoanalice el mensaje M = En el cifrado del César el criptoanálisis es muy elemental.
2. Con el algoritmo de cifra por multiplicación (decimación) con a = 5, cifre, descifre y criptoanalice, según estadísticas del lenguaje, el mensaje M = El cifrado por multiplicación exige la existencia del inverso en el cuerpo.
3. Con el algoritmo de cifra afín (a = 7, b = 10) cifre, descifre y criptoanalice, según estadísticas del lenguaje, el mensaje M = Si tenemos un texto de unos cuantos caracteres, el ataque al criptograma es muy sencillo.
4. Con el algoritmo de Vigenère cuya clave es K = GOL, cifre, descifre y criptoanalice el mensaje M = El jugador se adentró al área y de un golpe preciso introdujo el balón en la portería de aquel desgraciado portero. Era el presagio de lo que iba a ser aquella fatídica tarde para Manolo, justo en el día en que debutaba en aquel estadio.

Use el portapapeles

Prácticas del tema 9 (2/4)

5. Cifre y descifre en modo clave continua el mensaje M = Aquí se suma carácter a carácter la cadena de entrada con la clave siendo K = La clave será un texto de longitud igual o mayor que el texto en claro.
6. Cifre con Vernam el mensaje M con la clave numérica K. M = Una cifra muy interesante. K = 0 1 2 0 1 2 0 1 2 0 1 2 0 1 2 0 1 2 0 1 2 0. Al copiar la clave, respete los espacios en blanco.
7. Cifre con Vernam binario el mensaje M de 18 caracteres con la clave K de 26 caracteres. M = una cifra por bits. K = CIFRADOR BINARIO DE VERNAM. Compruebe la cifra del los tres primeros caracteres.
8. Cifre con Playfair el mensaje M usando la clave K. M = Un cifrador digrámico. K = JUEGO LIMPIO. Se eliminan K y W de la matriz. Observe la matriz de cifra. Descifre el criptograma y observe el relleno.
9. Cifre con Hill digrámico mod 27 el mensaje M = UN CIFRADO DE HILL con la clave $k_{11} = 7$; $k_{12} = 4$; $k_{21} = 13$; $k_{22} = 17$. Descifre el criptograma.

Use el portapapeles

Prácticas del tema 9 (3/4)

Software Hill: http://www.criptored.upm.es/software/sw_m001i.htm

1. Calcule el determinante y la inversa para comprobar si las siguientes matrices digrámicas son válidas para cifrar en el cuerpo 27:

   $k_{11} = 7; k_{12} = 10; k_{21} = 12; k_{22} = 19.$

   $k_{11} = 8; k_{12} = 5; k_{21} = 2; k_{22} = 8.$

   $k_{11} = 18; k_{12} = 15; k_{21} = 7; k_{22} = 8.$

2. Calcule el determinante y la inversa para comprobar si las siguientes matrices trigrámicas son válidas para cifrar en el cuerpo 27:

   $k_{11} = 4; k_{12} = 12; k_{13} = 9; k_{21} = 5; k_{22} = 0; k_{23} = 13; k_{31} = 6; k_{32} = 8; k_{33} = 3.$

   $k_{11} = 3; k_{12} = 12; k_{13} = 9; k_{21} = 5; k_{22} = 0; k_{23} = 13; k_{31} = 6; k_{32} = 8; k_{33} = 3.$

3. Calcule la inversa de la siguiente matriz pentagrámica en modulo 27:

   $k_{11} = 3; k_{12} = 2; k_{13} = 1; k_{14} = 0; k_{15} = 2; k_{21} = 5; k_{22} = 5; k_{23} = 3; k_{24} = 7;$
   $k_{25} = 1; k_{31} = 8; k_{32} = 7; k_{33} = 6; k_{34} = 5; k_{35} = 5; k_{41} = 4; k_{42} = 9; k_{43} = 6;$
   $k_{44} = 8; k_{45} = 3; k_{51} = 3; k_{52} = 9; k_{53} = 8; k_{54} = 7; k_{55} = 3.$

Use el portapapeles

Prácticas del tema 9 (4/4)

4. Para la matriz del ejercicio anterior, calcule el determinante y la inversa al trabajar en módulo 37 y en módulo 191.
5. Guarde la matriz clave que se indica con el nombre pract14libro.mtr. Abra ahora el editor del programa y guarde como pract14libro.txt el siguiente texto M = AHORA VAMOS A CIFRAR POR TRIGRAMAS.

   $k_{11} = 1$; $k_{12} = 1$; $k_{13} = 1$; $k_{21} = 3$; $k_{22} = 5$; $k_{23} = 7$; $k_{31} = 2$; $k_{32} = 1$; $k_{33} = 2$.
6. Descifre el criptograma anterior. Observe el relleno introducido.
7. Criptoanalice la matriz de cifra anterior mediante Gauss-Jordan, indicando que desea crear un archivo de seguimiento con nombre pract14libroataque. Una vez que haya encontrado la matriz clave de cifra, abra este archivo y observe las operaciones que el programa ha tenido que hacer para ello.
8. Cree matrices clave y documentos para cifrar, descifrar y criptoanalizar en módulo 191 y observe las opciones que le entrega el programa.