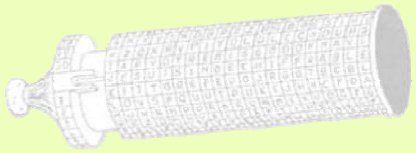
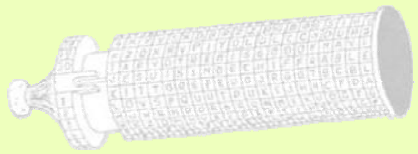
DE CÓMO ALICIA Y BENITO
MANTIENEN SECRETAS SUS CONVERSACIONES

DANIEL SADORNIL
MATESCO - UC

4 Marzo 2009

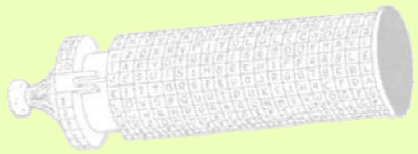


1. INTRODUCCIÓN



Si las matemáticas son la reina de las ciencias, entonces la teoría de números es, a causa de su suprema inutilidad la reina de las matemáticas.

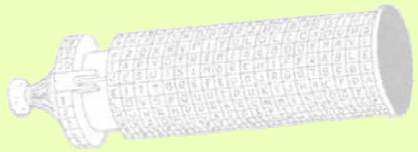
Gauss



…tanto Gauss como otros matemáticos menos importantes tienen mótivo para alegrarse de que haya una ciencia (la teoría de números), y que sea la suya, cuya lejanía de las actividades humanas cotidianas la mantienen apacible y limpia.

La matemática real (pura) no tiene efectos en la guerra. Nadie ha descubierto aún ningún propósito belicoso al que pueda servir la teoría de números. Por el contrario, las matemáticas triviales tienen muchas aplicaciones en la guerra.

G.H. Hardy, Apología de un matemático (1940)



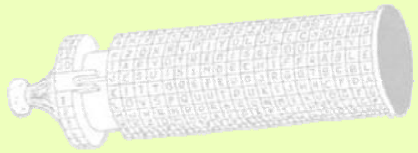
Algunas definiciones

- Criptografia:

  Del griego (kriptos), oculto y (-grafia) escritura. Arte de escribir con clave secreta o de un modo enigmático.

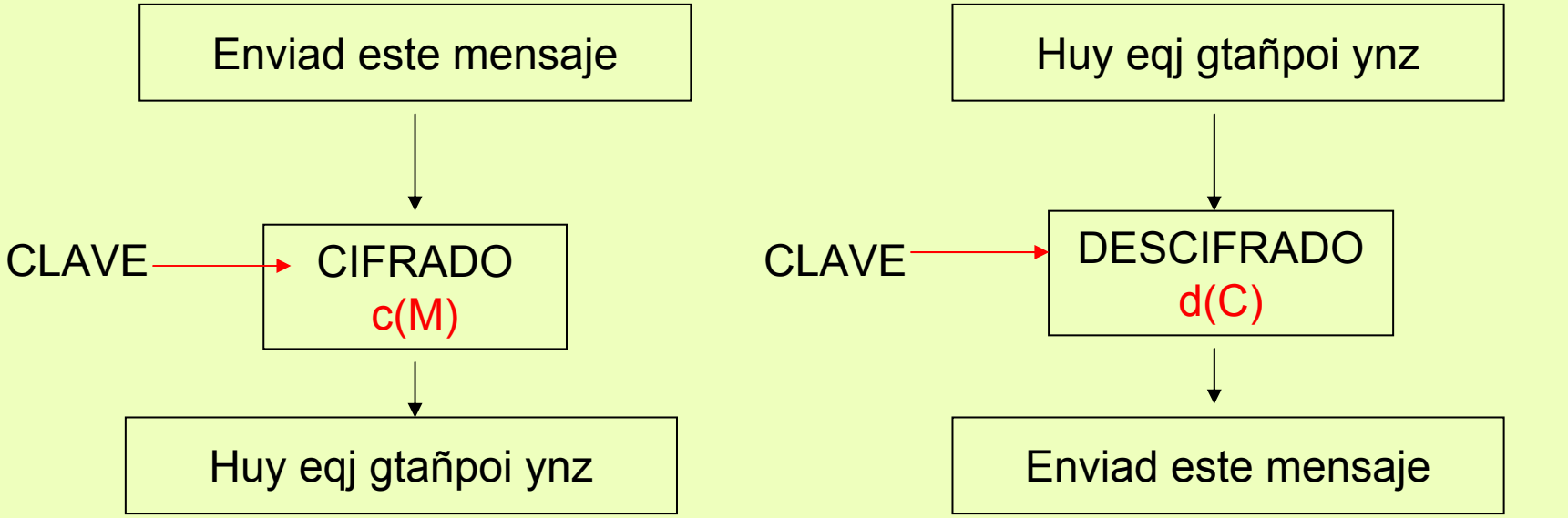
- Estenografía:

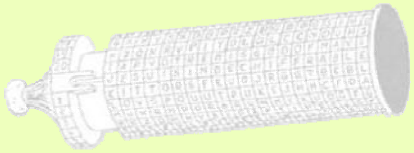
  Del griego (stegos), cubierto y (- grafia), técnicas de transmisión segura de información por medio de la ocultación.



¿Cuál es la diferencia?

Criptografía





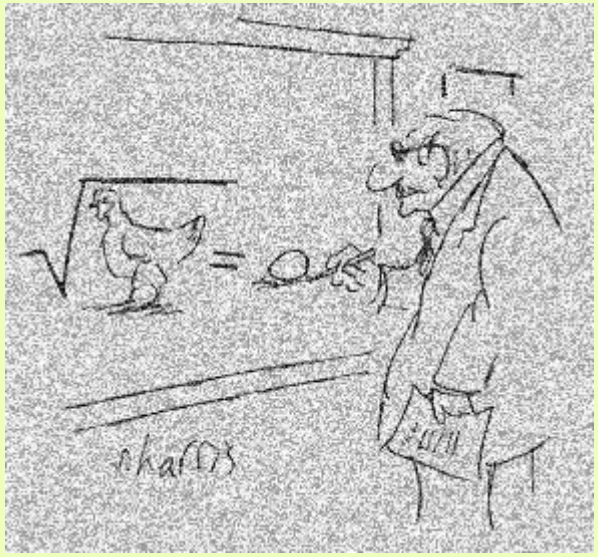
Esteganografía

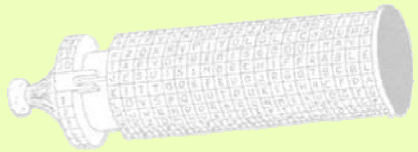
+

EJERCICIOS DE LIMITES

- $\lim_{x\to 1}\frac{\sqrt{x-1}+\sqrt{x+1}}{\sqrt{x-1}-\sqrt{x+1}}=1$
- $\lim_{x\to 3}\frac{\sqrt{x+1}-2}{x-3}\frac{1}{4}$
- $\lim_{x\to 2}\frac{x^2-x-2}{x^2-4x+4}=\frac{3}{0}\lim$
- $\lim_{x\to -1}\frac{x^2+2x+1}{x^3+3x^2+3x+1}=\frac{0}{0}\lim$
- $\lim_{x\to -\infty}\frac{3x^2-4}{2x+3}=-\infty$
- $\lim_{x\to\infty}\frac{5x^2-2x+1}{(2x-1)^2}=\frac{5}{4}$
- $\lim_{x\to\infty}\frac{\sqrt{5x^2+6x}}{2x+1}=\frac{\sqrt{5}}{2}$
- $\lim_{x\to\infty}\left(\frac{x^2-5x}{x+1}-\frac{3x}{2}\right)=-\infty$
- $\lim_{x\to\infty}\frac{1+\sqrt{x}}{2x-3}=0$
- $\lim_{x\to\infty}\sqrt{\frac{5x^2-7}{x+1}}=\infty$
- $\lim_{x\to\infty}\frac{3x}{\sqrt{x^2+2}}=0$
- $\lim_{x\to 1}\frac{(x-1)^2}{x-5}=0$
- $\lim_{x\to 0}\left(\frac{x^3+3}{x^2}-\frac{1}{x}\right)=\frac{3}{0}\lim$
- $\lim_{x\to 1}\left(\frac{2}{(x-1)^2}-\frac{1}{x(x-1)}\right)=\infty$
- $\lim_{x\to 1}\frac{x^2-7x+6}{x-1}=-5$
- $\lim_{x\to 1}\frac{x^3+x-2}{2x^2-2x}=\frac{3}{2}$
- $\lim_{x\to\infty}\frac{3+2\sqrt{x}}{\sqrt{9x+1}}=\frac{2}{\sqrt{x}}$
- $\lim_{x\to 0}\frac{x^3-3x^2}{x^2-x}=0$
- $\lim_{x\to\infty}\frac{3x^3-5x^2+2x-1}{16x^2-7x+3}=\infty$
- $\lim_{x\to\infty}\left(\frac{x^3-3x^2+5}{x^2-1}-2x\right)=\infty$
- $\lim_{x\to\infty}\left(\frac{3x^2-5x}{x+4}\right)^{x+1}=\infty$
- $\lim_{x\to\infty}\left(\frac{x^2+x+1}{x^2-x+3}\right)^{x}=e^2$
- $\lim_{x\to\infty}\frac{\sqrt{x^2-2x+5}}{2x+5}=\infty$
- $\lim_{x\to\infty}\left(\frac{x-3}{2x}\right)^{\frac{x+5}{x}}=\frac{1}{2}$
- $\lim_{x\to\infty}\frac{10x^4+3x+3}{5(1-x^4)}=-2$
- $\lim_{x\to\infty}\left(\frac{x^3-3x^2+5}{x^2-1}+\frac{3-x^2}{x+1}\right)=-2$
- $\lim_{x\to\infty}\left(\frac{x-3}{2x}\right)^{x^2}=\infty$
- $\lim_{x\to 3}\left(\frac{x^2-3x}{x-3}+\frac{3x-9}{x-3}\right)=6$
- $\lim_{x\to 5}\left(\frac{3}{x-5}-\frac{x}{x-5}\right)=-1$
- $\lim_{x\to 2}\frac{\sqrt{x+2}-3}{x-2}=\frac{1}{4}$
- $\lim_{x\to 2}\frac{x^3-4}{x^4+2x^2+5x+9}=-\frac{4}{9}$
- $\lim_{x\to 0}\frac{x^2+7x}{x}=7$
- $\lim_{x\to 0}(x+1)^{\frac{1}{x}}=e$
- $\lim_{x\to 5}\left(\frac{3x-5}{x^2-4x}\right)^{\frac{1}{x-5}}=\frac{3}{9}\lim$
- $\lim_{x\to 4}\frac{\sqrt{5-x}-1}{x-4}=-\frac{1}{2}$
- $\lim_{x\to 1}\frac{x^2+x-2}{2x^2-6x+4}=-\frac{3}{2}$
- $\lim_{x\to 1}\frac{x-1}{1-\sqrt{9-x}}=2$
- $\lim_{x\to 0}\left(\frac{3x+1}{x^2}-\frac{3}{x}\right)=\infty$
- $\lim_{x\to 2}\left(\frac{3}{x^2-5x+6}-\frac{4}{x-2}\right)=\frac{3}{0}\lim$
- $\lim_{x\to\infty}\frac{\sqrt{x^2+\sqrt{2x}}}{\sqrt{x^2-\sqrt{2x}}}=1$

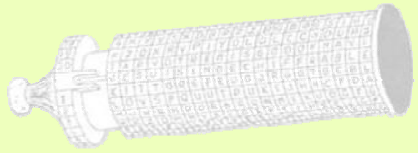
=





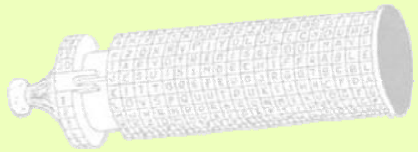
Algunos ejemplos de Esteganografía

- Herodoto : Mensajes escritos en el cuero cabelludo.
- Demerato: Tablillas de cera recubiertas.
- China antigua: Mensajes escritos en cera que se tragaban.
- Plinio: Escritura invisible.
- Giovanni Porta: Escritura en huevo cocido.
- Micropuntos, microfilms.
- Marcas de agua.
- Acrósticos.



¿Para qué lo queremos?

- Privacidad: la información sólo debe ser accesible a aquellos autorizados a obtenerla.
- Integridad: la información sólo debe ser alterada por aquellos autorizados a hacerlo.
- Autentificación: cuando se establece intercambio de información entre dos partes, ambas deben ser capaces de identificarse de manera irrefutable.
- No repudio: nadie debería poder negar acciones o afirmaciones previas.



¿DONDE?


DOCUMENTO NACIONAL DE IDENTIDAD
ESPAÑA
PRIMER APELLIDO
APELLIDO1
SEGUNDO APELLIDO
APELLIDO2
NOMBRE
NOMBRE
SEXO
M-F
NACIONALIDAD
ESP
NUM. PERSONAL
99999999-R
EXPIRACIÓN
DD MM AA
ESPECIMEN
DNI
NUM. DOC.
AAA-000000


08:57
Mensajes


Chip in der Passdecke
Symbol für elektronisches Passbuch
EPASS


Wii


CLASSIC
PLATINUM
VISA

Reglas de Kerckhoffs (s. XIX)

- Debe ser imposible recuperar a partir del texto cifrado el texto original y/o la llave.
- Existen dos tipos de información:
  - Privada (Claves)
  - Pública (Algoritmos)
- La llave debe ser fácil de recordar y modificar.
- La transmisión del texto cifrado debe ser factible con los medios habituales.
- La computación necesaria para descifrar (por el receptor legal) debe corresponderse con el beneficio obtenido.

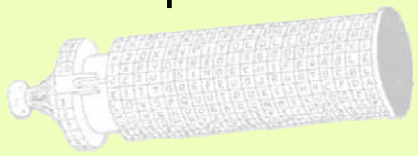
Seguridad

1. Seguridad perfecta: Si es irrompible cuando al criptoanalista se le suponen tiempo y recursos ilimitados.

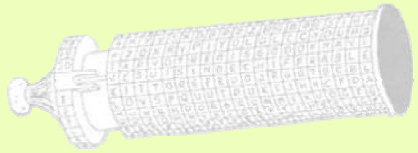
2. Condicional: Seguro hasta que se desarrollen nuevos o mejores métodos de criptoanálisis.

3. Probable: Sistemas que no han sido rotos, pero de los que no se puede demostrar su seguridad matemáticamente.

4. Computacional: Basado en la complejidad computacional (matemáticamente probada) del sistema.

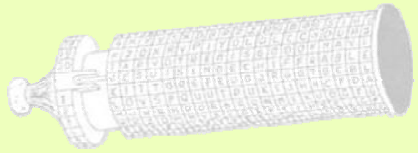


2. CRIPTOGRAFIA DE CLAVE SECRETA



CONSIDERACIONES

- Los usuarios del sistema acuerdan y guardan en secreto las dos funciones (o la clave del que dependen) c y d de cifrado y descifrado, inversas entre sí.
- Cualquier usuario que sepa cifrar sabe descifrar.
- Conocer la clave de cifrado implica conocer la de descifrado y recíprocamente.
- El algoritmo de cifrado/descifrado determina unívocamente el algoritmo de descifrado/cifrado.



Los orígenes

Cifrados de TRASPOSICIÓN

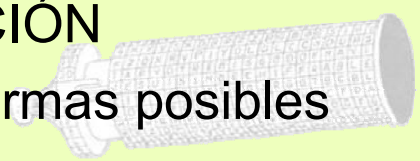
Consiste en remover el mensaje, es decir, desordenarlo mediante una regla determinada para obtener el texto cifrado.

En una trasposición realizada al azar, el desciframiento del mensaje es tan difícil para el receptor del mensaje a quien va dirigido como para un interceptor enemigo.

Si tomamos el mensaje:

ESTE ES UN CIFRADO DE TRASPOSICIÓN

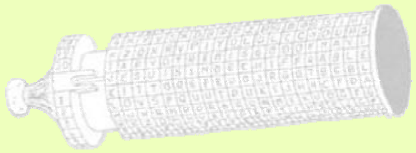
existen 34!=295232799039604140847618609643520000000 formas posibles (más de 10^{39}).



Un pequeño ejemplo

ESTE_ES_UN_CIFRADO_DE_TRASPOSICION

TESEE_US_CN_RIFOADE_DR_TPASIOSOCIN



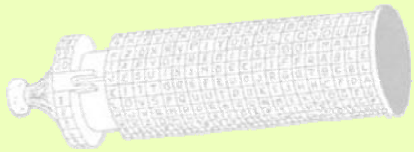
Hablando matemáticamente

Supongamos que estamos trabajando en un texto de tamaño cualquiera troceamos el mensaje en partes de tamaño k.

La clave es una permutación σ de k elementos; en el ejemplo anterior la permutación es: $\begin{pmatrix} 1 & 2 & 3 \\ 2 & 3 & 1 \end{pmatrix}$

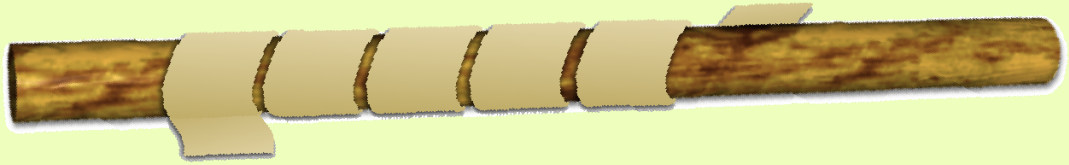
La primera letra ocupa la posición 2, la segunda la posición 3 y la tercera la posición 1. → EST->TES

Para descifrar, solo se necesita la permutación inversa, σ^{-1} , en nuestro caso $\begin{pmatrix} 1 & 2 & 3 \\ 3 & 1 & 2 \end{pmatrix}$



Escitala espartana (s. V a.c.)

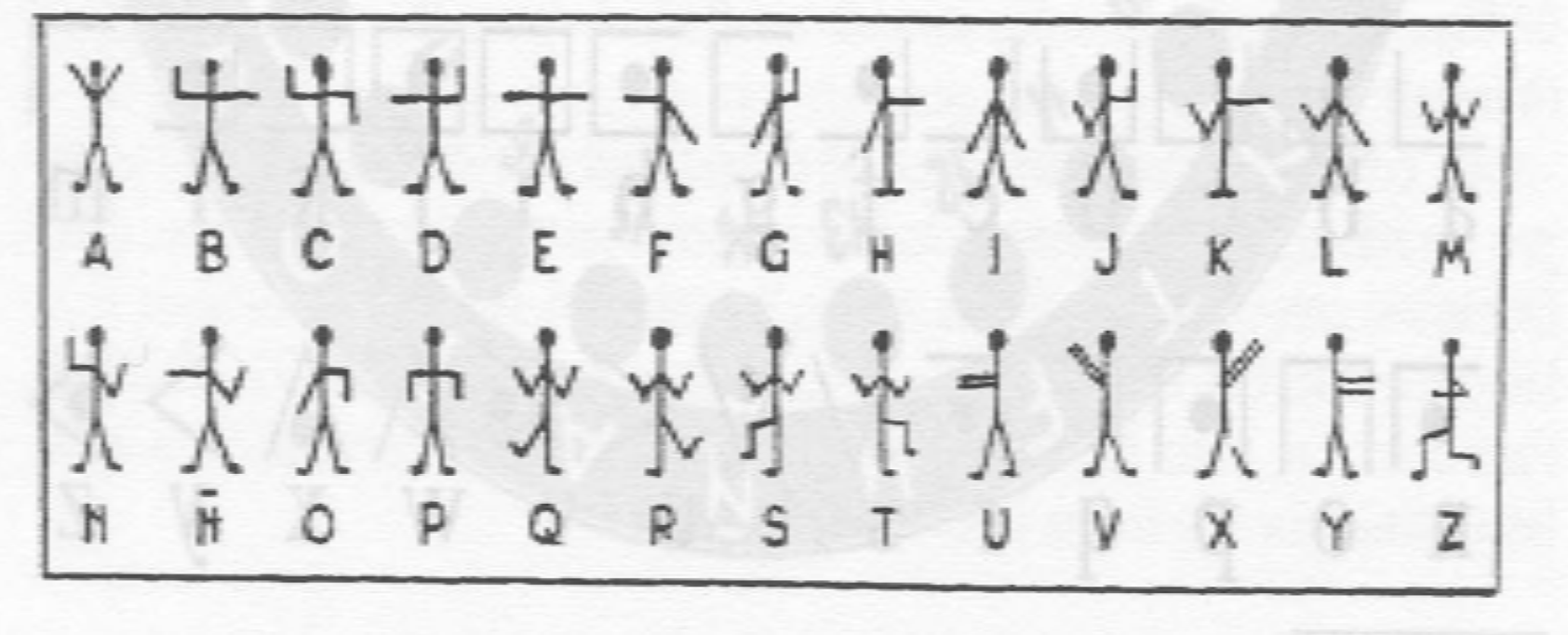
Se trata de una vara de madera sobre la que se enrosca una tira de cuero o pergamino. El emisor escribe el mensaje a lo largo de la tira enroscada y luego la desenrosca. De esta forma, el texto parece una lista de letras sin sentido. Para descifrarlo, se necesita una misma vara de igual diametro.



Cifrados de SUSTITUCIÓN

Se trata de sustituir el alfabeto en el que se escribe por otro de forma que en este segundo alfabeto, el texto no tenga sentido conocido.

Por ejemplo:



o incluso:

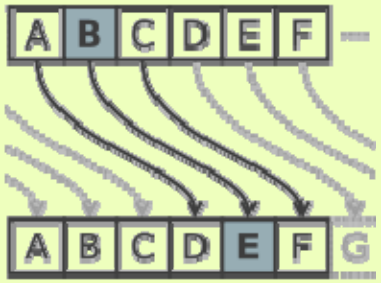
A ·–	B –···	C –·–·	D –··	E ·	F ··–·	G ––·
H ····	I ··	J ·–––	K –·–	L ·–··	M ––	N –·
O –––	P ·––·	Q ––·–	R ·–·	S ···	T –	U ··–
V ···–	W ·––	X –··–	Y –·––	Z ––··		
1 ·––––	2 ··–––	3 ···––	4 ····–	5 ·····	6 –····	7 ––···
8 –––··	9 ––––·	0 –––––				

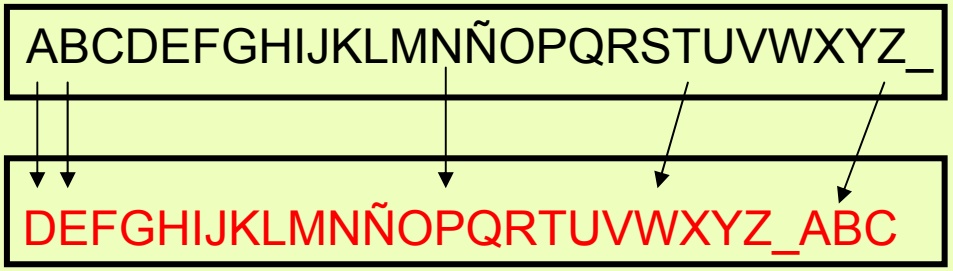
Sin embargo, ya desde la antigüedad, lo que se ha hecho es permutar el alfabeto. Es decir, una letra es cambiada por otra de forma única.

Si se conoce dicha asignación se puede cifrar y descifrar mensajes fácilmente

Cifrado de Cesar o Augusto:

Consiste en trasladar 3 posiciones cada letra del alfabeto. Así la A se cifra como D, la B como E y así sucesivamente.



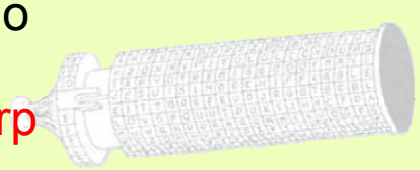


Por ejemplo, si ciframos la palabra TRABAJAR con la clave n = 3 se tiene:

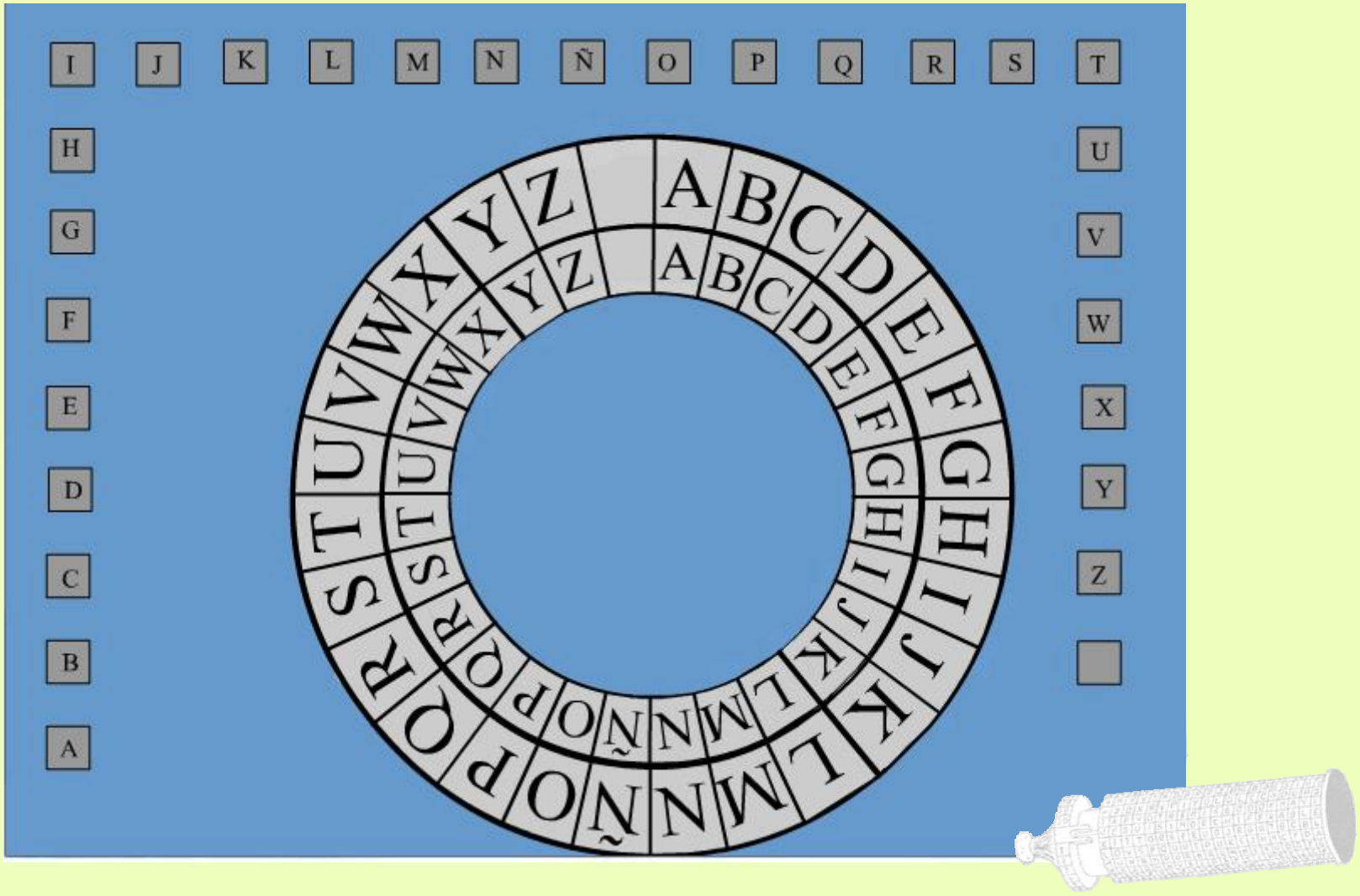
T R A B A J A R
D D D D D D D D
W U D E D M D U

Y el mensaje: Este es un cifrado por sustitucion se cifra como

hvwhchvcxpcfliudgrcsrucvxvwlwxflrp



Disco de cifra



ruleta

En términos matemáticos

Supongamos que estamos trabajando en un alfabeto castellano. Identificamos cada letra con la posición que ocupa en el alfabeto. De esta forma:

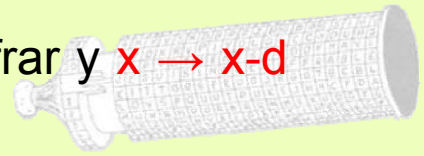
A	B	C	D	E	F	G	H	I	J	K	L	M	N	Ñ	O	P	Q	R	S	T	U	V	W	X	Y	Z	-
1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26	27	28

Y el cifrado/descifrado de César se puede ver como la aplicación:

$$\mathbb{Z}_{28} \longrightarrow \mathbb{Z}_{28} \qquad \mathbb{Z}_{28} \longrightarrow \mathbb{Z}_{28}$$

$$X \rightarrow X+3 \qquad X \rightarrow X-3$$

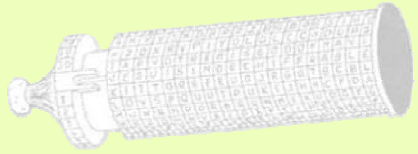
En general, se puede tomar la aplicación $x \rightarrow x+d$ para cifrar y $x \rightarrow x-d$ para descifrar. El entero d es la clave de cifrado.



¿Es posible descifrar el siguiente mensaje

"lz lglzgatg ld vgjomyhkvgslkoht lgatgjomyhkvgklgjlzhyglrgjahrghgwhy oygklrghthrozozgklgmyljaltjohzgzlgwalklgkl lysothy"

sabiendo que se ha usado un cifrado de César?

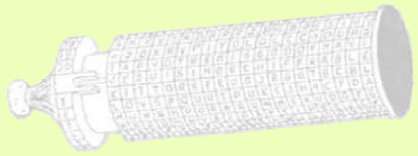


UN POCO DE CRIPTOANÁLISIS

ANÁLISIS DE FRECUENCIAS

Si escribimos cualquier texto (suficientemente largo) , nos daremos cuenta de que hay letras que se repiten con más frecuencia que otras. En castellano (obviando el espacio) la letra que más se repite es ….. e,a,o….

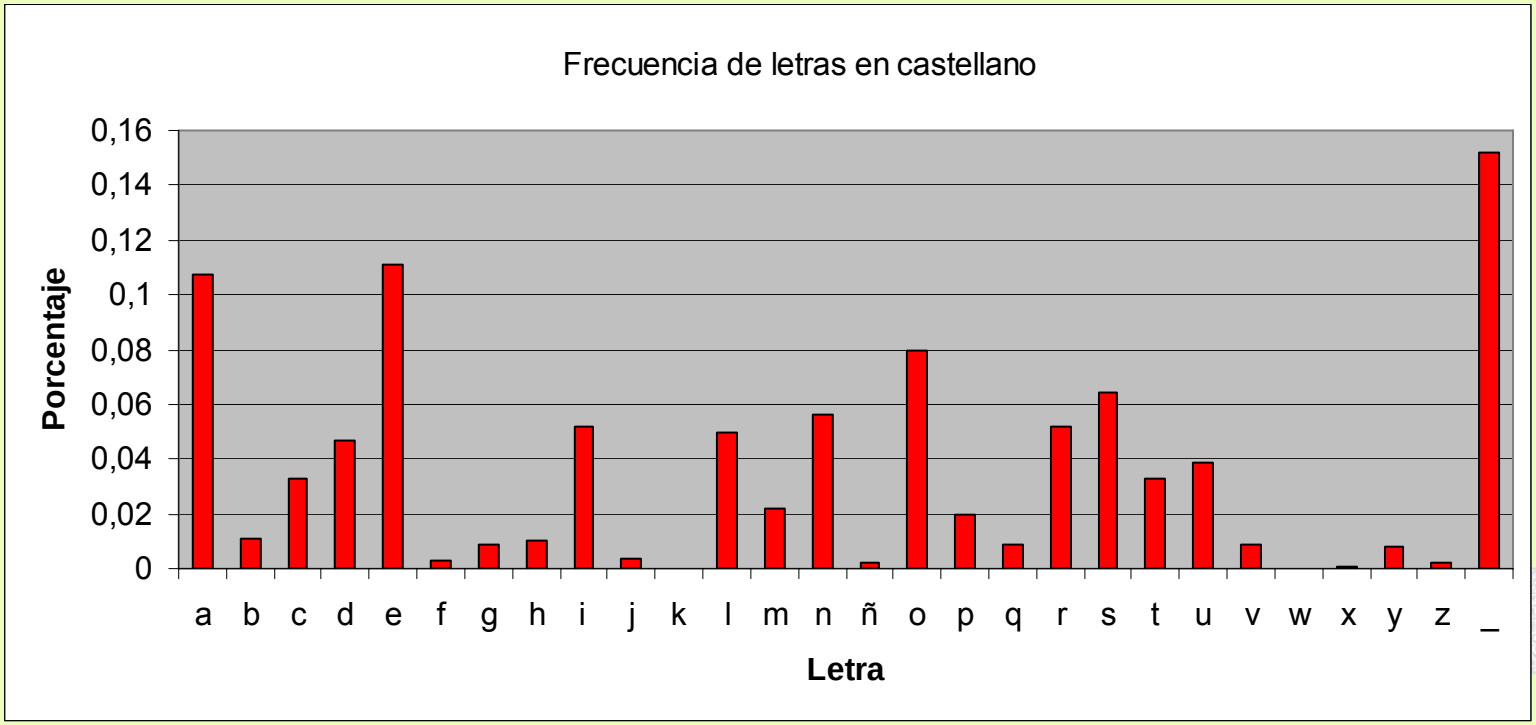
e,a,o,l,s,n,d,r,u,i,t,c,p,m,y,q,b,h,g,f,v,j,ñ,z,x,k,w



En porcentajes:

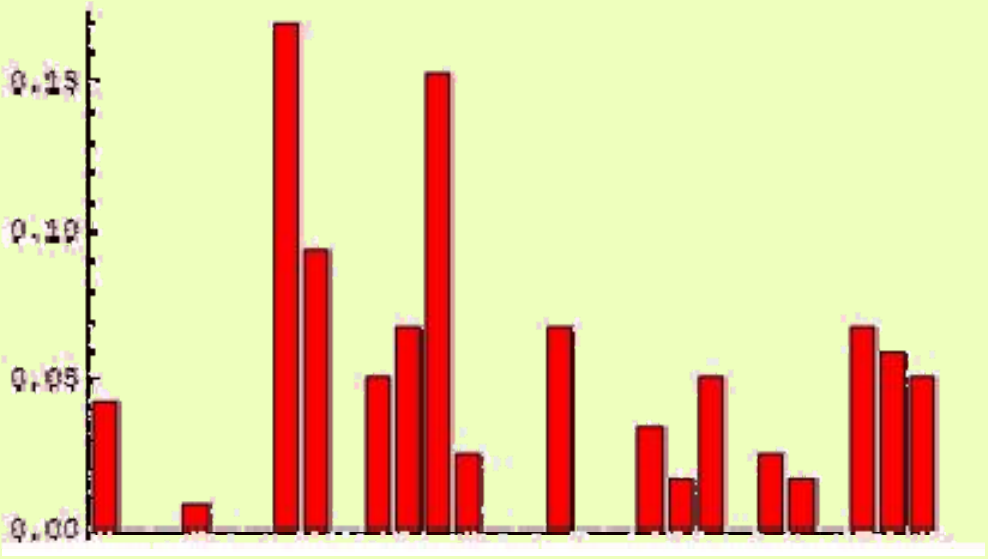
a	b	c	d	e	f	g	h	i	j	k	l	m	n
0,1076	0,011	0,033	0,047	0,111	0,003	0,009	0,01	0,052	0,004	0,00016	0,05	0,022	0,056

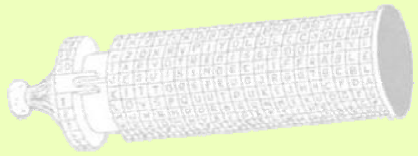
ñ	o	p	q	r	s	t	u	v	w	x	y	z	_
0,002	0,08	0,02	0,009	0,052	0,064	0,033	0,039	0,009	0,00008	0,001	0,008	0,002	0,152



Si estamos utilizando un cifrado César, donde cada letra se sustituye por otra, trasladada una serie de posiciones; las frecuencias relativas no serán iguales pero serán desplazadas.

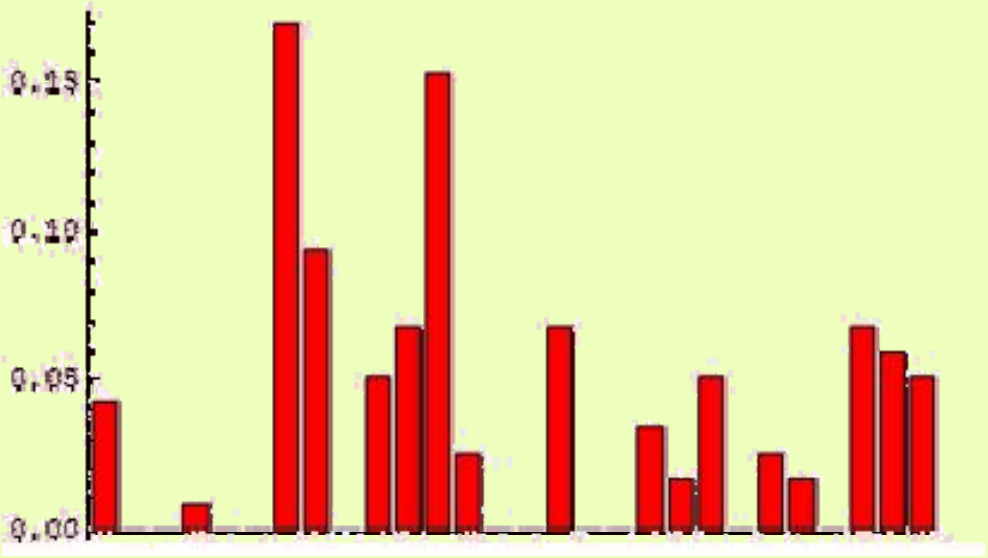
Es decir, supongamos que estamos cifrando la letra e (=4) por la letra k (=10), entonces las frecuencias serán trasladadas d=6 posiciones

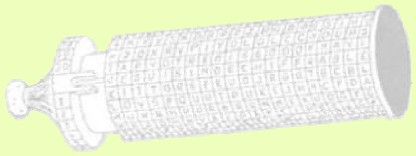




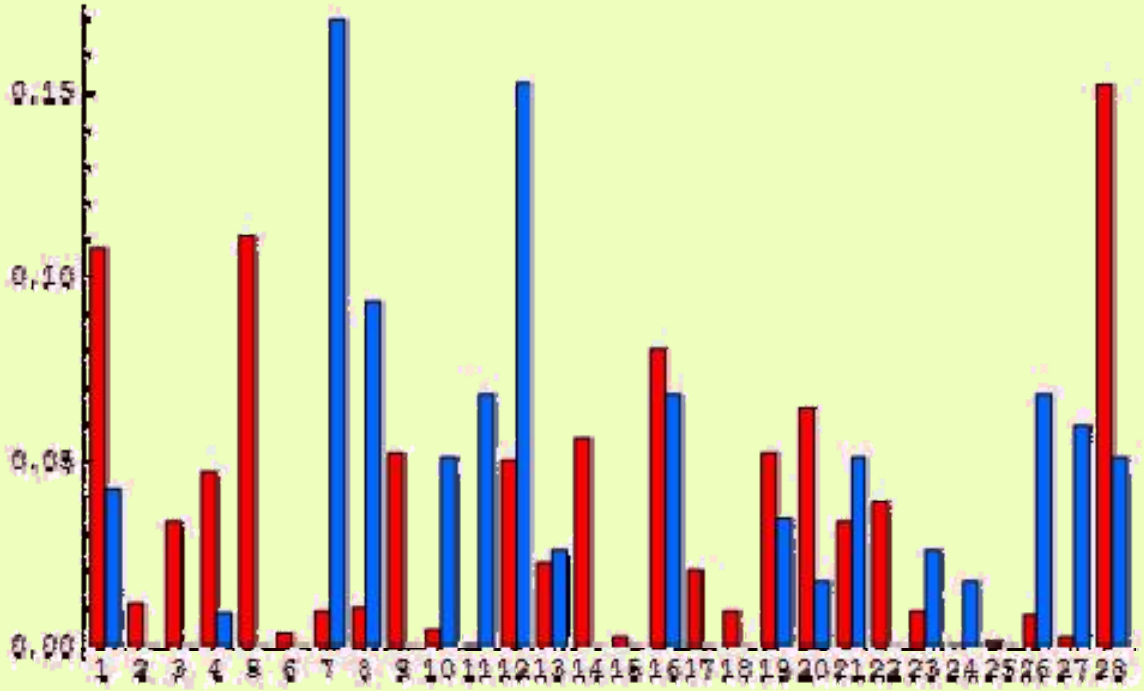
Si estamos utilizando un cifrado César, donde cada letra se sustituye por otra, trasladada una serie de posiciones; las frecuencias relativas no serán iguales pero serán desplazadas.

Es decir, supongamos que estamos cifrando la letra e (=4) por la letra k (=10), entonces las frecuencias serán trasladadas d=6 posiciones





que comparándola con la tabla de frecuencias en castellano queda (la roja representa un texto en castellano y la azul nuestro texto cifrado).

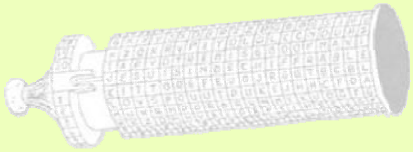


Es fácil ver que no concuerdan exactamente, pero fijémonos en los picos. En la azul, los picos (grandes) están en las letras 7,8 y 12, mientras que en la roja los picos altos están en la 28,1 y 5. Por tanto podríamos suponer que la clave de cifrado es 7.

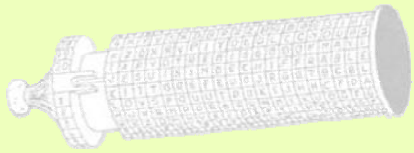
Si sustituimos cada letra del texto cifrado por la que ocupa 7 posiciones antes, nos queda;

“lz lglzgatg ld vgjomyhkvgslkoht lgatgjomyhkvgklgjlzhyglrgjahrghgwhy oygklrghthrozozgklgmyljaltjohzgzlgwalklgkl lysothy”

“este es un texto cifrado mediante un cifrado de cesar el cual a partir del analisis de frecuencias se puede determinar“.



- Número posible de claves: 27 (la clave A no transforma el mensaje).
- El criptoanalista puede, con poco esfuerzo, ensayar todas las claves hasta acertar con la verdadera.
- Letras iguales se cifran siempre de la misma forma.
- Las frecuencias de los caracteres de un texto cifrado suficientemente largo se corresponden con la frecuencia de un texto claro pero trasladada una serie de posiciones.
- Conociendo ÚNICAMENTE como se cifra un carácter, se puede descifrar el texto.



Cifrados afines

Un cifrado de César viene caracterizado por aplicaciones del tipo

$$\mathbb{Z}_{28} \longrightarrow \mathbb{Z}_{28}$$
$$X \rightarrow X+d$$

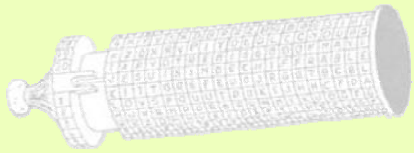
Si cambiamos de aplicación (mientras sea biyectiva), podremos obtener otro tipo de cifrado. De esta forma, la aplicación

$$\mathbb{Z}_{28} \rightarrow \mathbb{Z}_{28}$$
$$X \rightarrow aX+b$$

define un cifrado de sustitución que denominamos afín, cuando sea biyectiva; es decir si MCD(a,28)=1 (¿Por qué?).

En este caso, su función de descifrado es:

$$\mathbb{Z}_{28} \rightarrow \mathbb{Z}_{28}$$
$$Y \rightarrow (Y-b)a^{-1}$$



Por ejemplo si a=13 y b=25, la palabra TRABAJAR se cifra como:

T=13*21+25 mod 28=298 mod 28=18=Q.

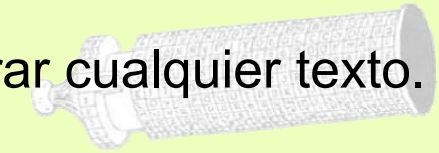
…..

QSJVJÑJS

Al igual que en los cifrados de César

- Letras iguales se cifran siempre de la misma forma.
- Las frecuencias de los caracteres de un texto cifrado suficientemente largo se corresponden con la frecuencia de otro carácter.
- Conociendo como se cifran dos caracteres, se puede descifrar el texto (un sistema de dos ecuaciones con dos incógnitas).

Se puede aplicar un análisis de frecuencias para descifrar cualquier texto.



UN ÚLTIMO EJEMPLO DE SUSTITUCIÓN MONOALFABÉTICA

Consideremos el alfabeto A. Entonces un cifrado de sustitución es simplemente fijar una biyección del alfabeto A.
Por ejemplo, si fijamos como tabla de sustitución la siguiente:

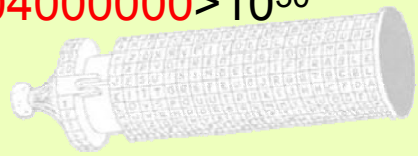
ABCDEFGHIJKLMNÑOPQRSTUVWXYZ-

QWERTYUIO-PASDFGHJKLÑZXCVBNM

quiere decir que para cifrar el texto se sustituye la A por Q, la B por W, la C por E, y así sucesivamente.

Número de claves posibles: $28! = 304888344611713860501504000000 > 10^{30}$

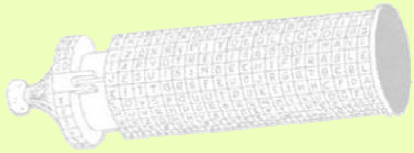
También es vulnerable a un análisis de frecuencias.



POLISUSTITUCIONES: r-GRAFOS

En vez de sustituir un único carácter, se trata de agruparlos en parejas, trios, . . ., conjuntos de *r* letras y considerarlos en un alfabeto de longitud 28^r .

- BLOQUES de r letras iguales se cifran siempre de la misma forma.
- Las frecuencias de los caracteres de un texto cifrado no se corresponden a las de un texto claro. PERO, las frecuencias de los r-grafos SI.
- Basta con conocer la correspondencia de *r* (ó *r* + 1 si es afín) caracteres para descifrar el mensaje.

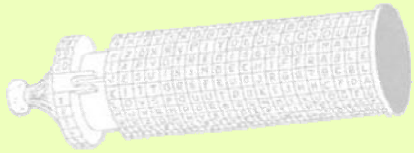


CIFRADO DE VIGENÈRE

En lugar de cifrar siempre con la misma regla (alfabeto de llegada) se utilizan diferentes alfabetos dependiendo de la posición en que se encuentre el carácter a cifrar.

Consiste en utilizar varias permutaciones del alfabeto (es decir varios alfabetos alternativos, que tradicionalmente son permutaciones del original) con arreglo a alguna pauta.

La misma letra no se cifra siempre de la misma forma, de esta forma se evita un ataque por análisis de frecuencias.



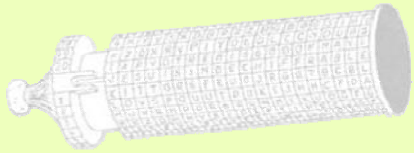
Construcción:

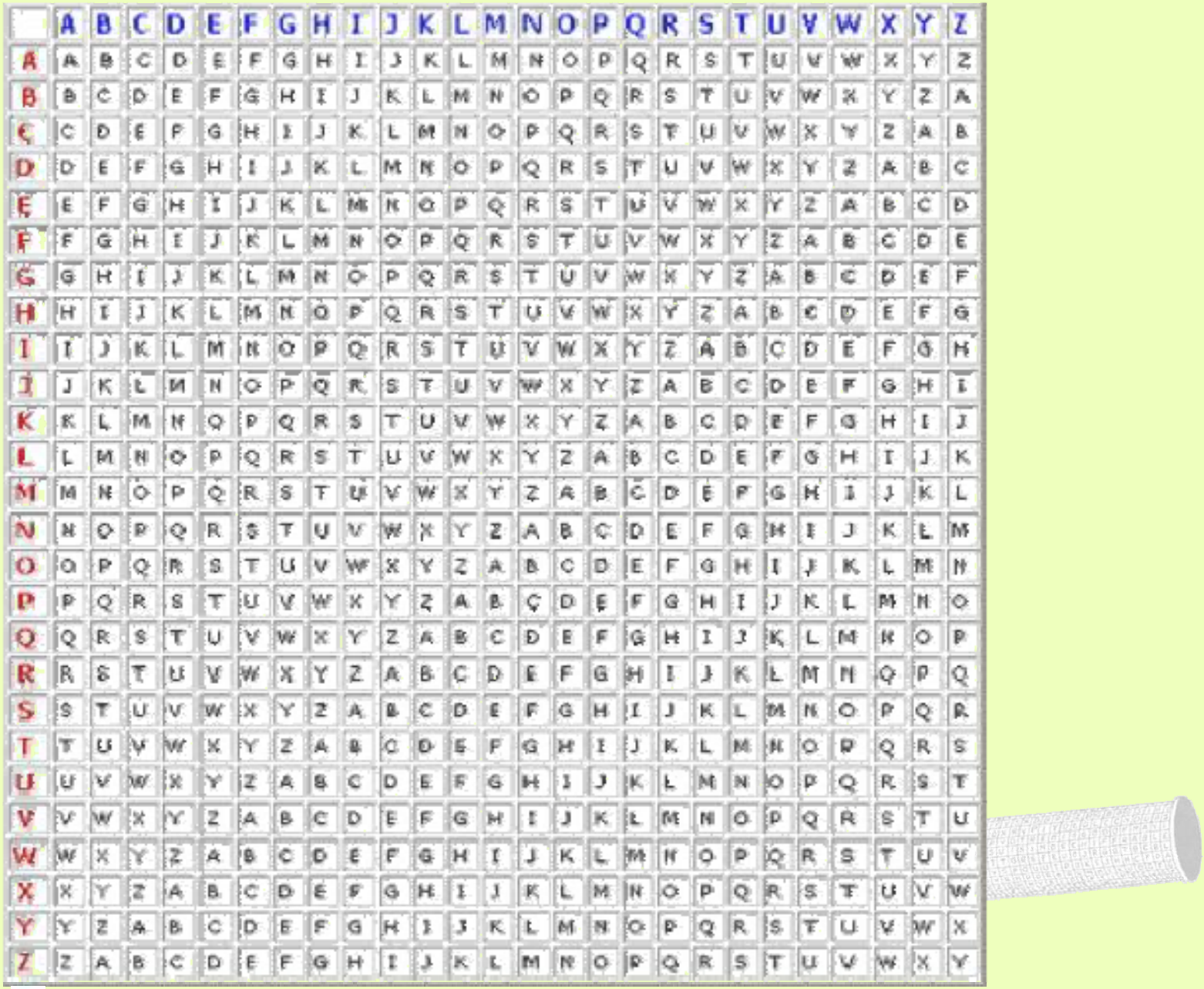
Se fija una palabra clave: $k = k_1 k_2 \ldots k_s$.

El mensaje original en claro es $m = m_0 m_1 m_2 \ldots . m_n$.

se reparte en bloques de longitud *s* y el carácter i de cada bloque se cifra con la cifra de César de clave k_i, es decir:

$$m_{st+i} \rightarrow m_{st+i} + k_i$$





Ejemplo:

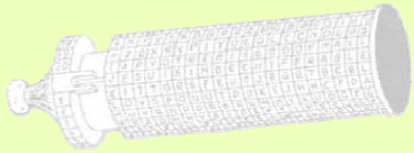
C O M O S I L L E G A R A A B U E N P U E R T O

R O S A R O S A R O S A R O S A R O S A R O S A

T C D O J W C L V U S R R O T U V A H U V F L O

Sin embargo, no es perfecto, si el texto cifrado es suficientemente largo, se puede descifrar sin conocer la clave.

Su debilidad está en la repetición de la clave.



Solución al problema de repetición de la palabra clave:

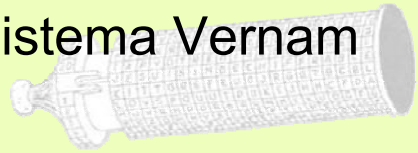
utilizar una llave tan larga como el mensaje

Código de secreto perfecto

Si se utiliza como llave:

1. Una sucesión aleatoria.
2. De longitud mayor o igual que la del mensaje.
3. Tal llave se emplea una sola vez (llave de un solo uso)

El código anterior es absolutamente indescifrable (sistema propuesto en 1917 por Vernam).
Shannon en 1949 demuestra matemáticamente que el sistema Vernam es de secreto perfecto.

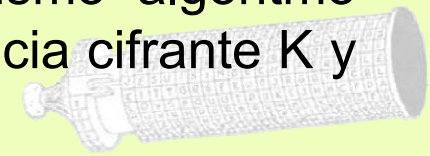


Problemas prácticos del sistema Vernam:

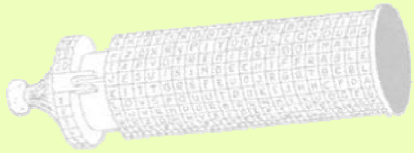
- La dificultad de generar una secuencia realmente aleatoria.
- La transmisión de la clave requiere el mismo esfuerzo que la del mensaje.

Habitualmente se utilizan simplificaciones del método anterior que se conocen con el nombre genérico de ***técnicas de cifrado en flujo*** y que consisten en:

El emisor A, mediante una ***clave corta (secreta)*** y un ***método determinista (público)*** genera una secuencia binaria K (***secuencia cifrante o secuencia pseudoaleatoria***) mediante la que cifra el mensaje.
El receptor B, dispone de la ***misma clave*** y el mismo algoritmo determinista, por tanto puede generar la misma secuencia cifrante K y recupera el mensaje.



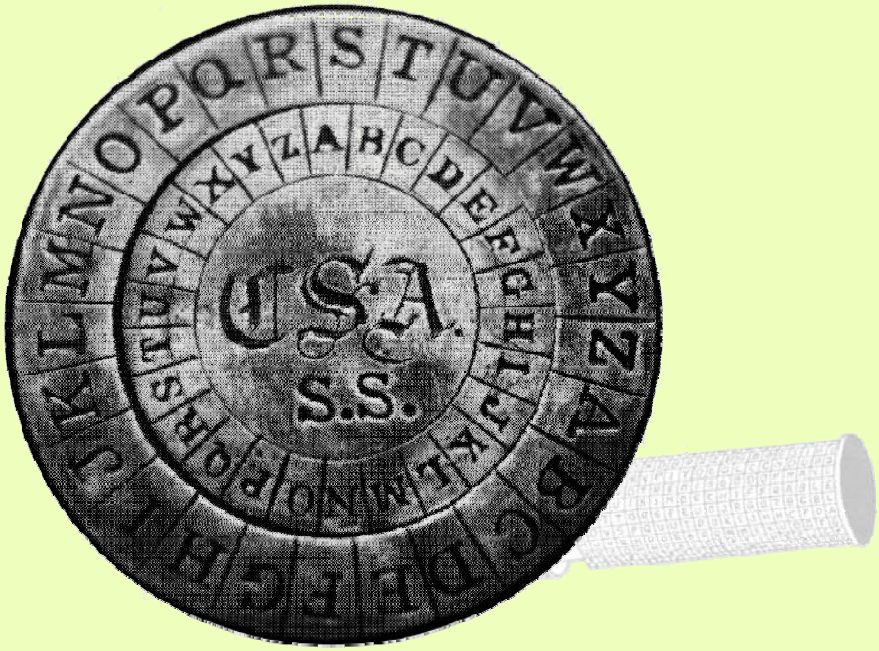
3. Y LLEGARON LAS MÁQUINAS



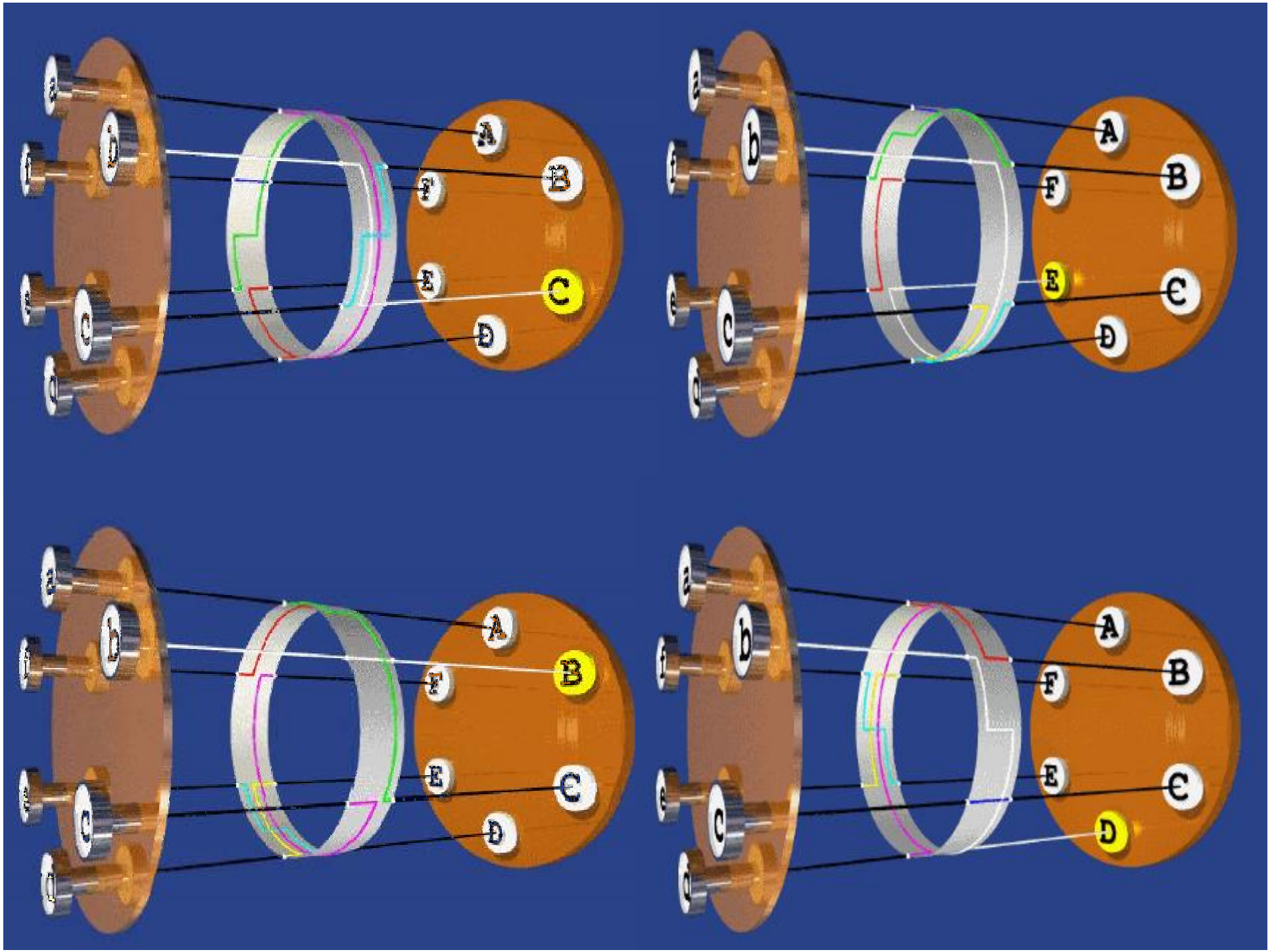
LA MAQUINA ENIGMA

Primera versión creada por Arthur Scherbius en Alemania (sobre 1920)

Idea básica: utilizar un disco de cifra, donde el alfabeto de cifrado no es correlativo. Además cada vez que se cifra un carácter, este disco gira.



Si el usuario pulsa una tecla en el teclado, se ilumina un carácter en un tablero expositor que corresponde con el cifrado.


a
b
c
A
B
C
D
E
F

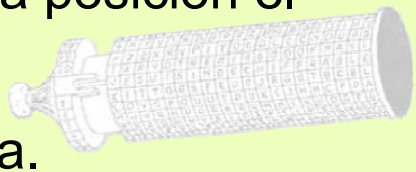
El alfabeto cifrado cambia tras cada cifrado de un carácter. El modificador define esencialmente (en el dibujo anterior) 6 cifrados de sustitución. Cuando se da una vuelta completa, se vuelve a realizar el primer cifrado.

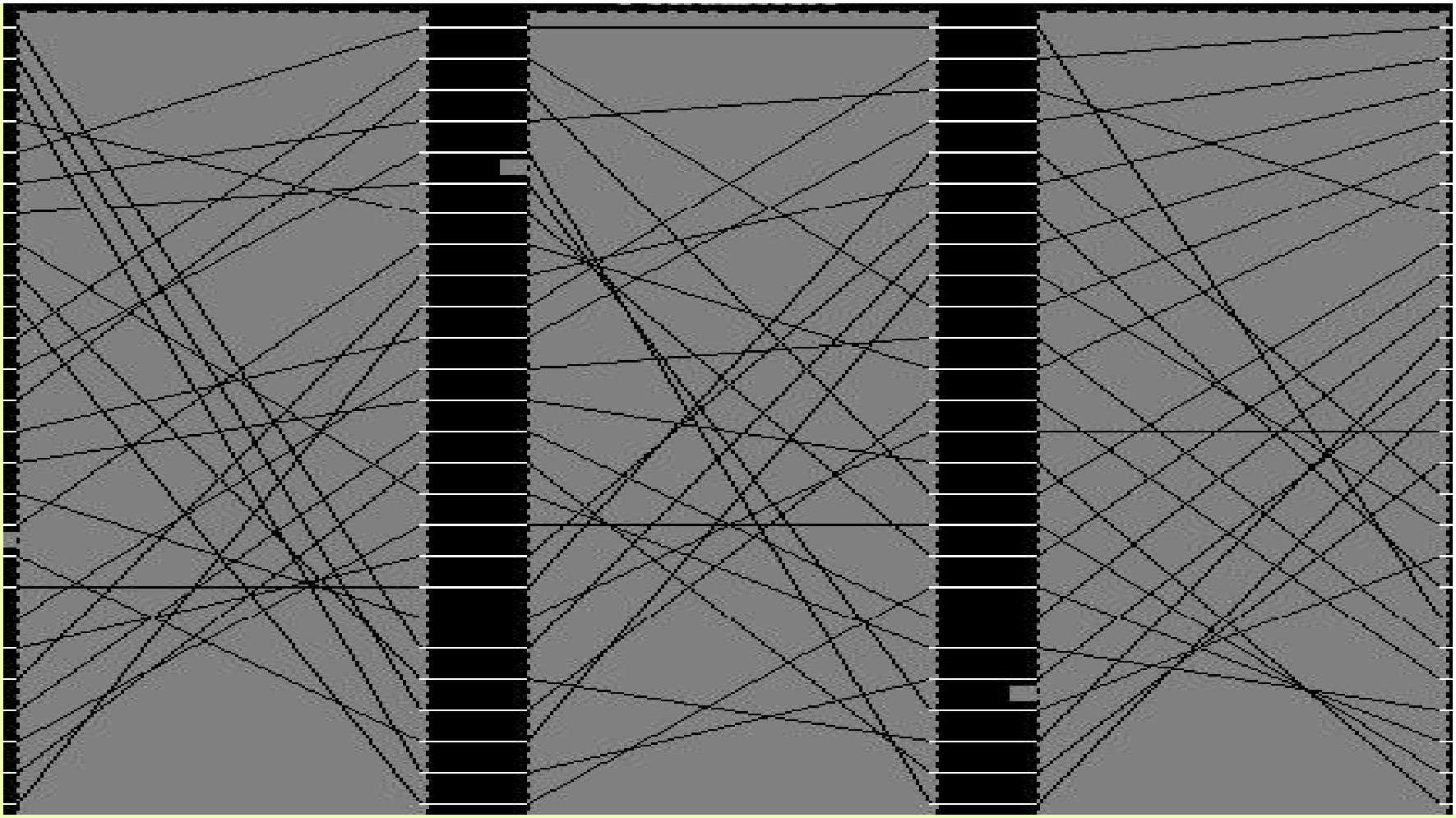
Teclear repetidas veces (6 en el dibujo) un mismo carácter hace que el modificador vuelva a su posición inicial y teclear el mismo carácter una y otra vez repetirá el mismo patrón de cifrado.

Añadir más modificadores.

Cada vez que se cifra un carácter, gira el primer modificador, hasta que este no ha realizado una vuelta completa, no gira una posición el segundo modificador.

Como si fueran las agujas del segundero, minutero y hora.





Con un teclado de 26 letras y tres modificadores hay

$$26^3 = 17576$$

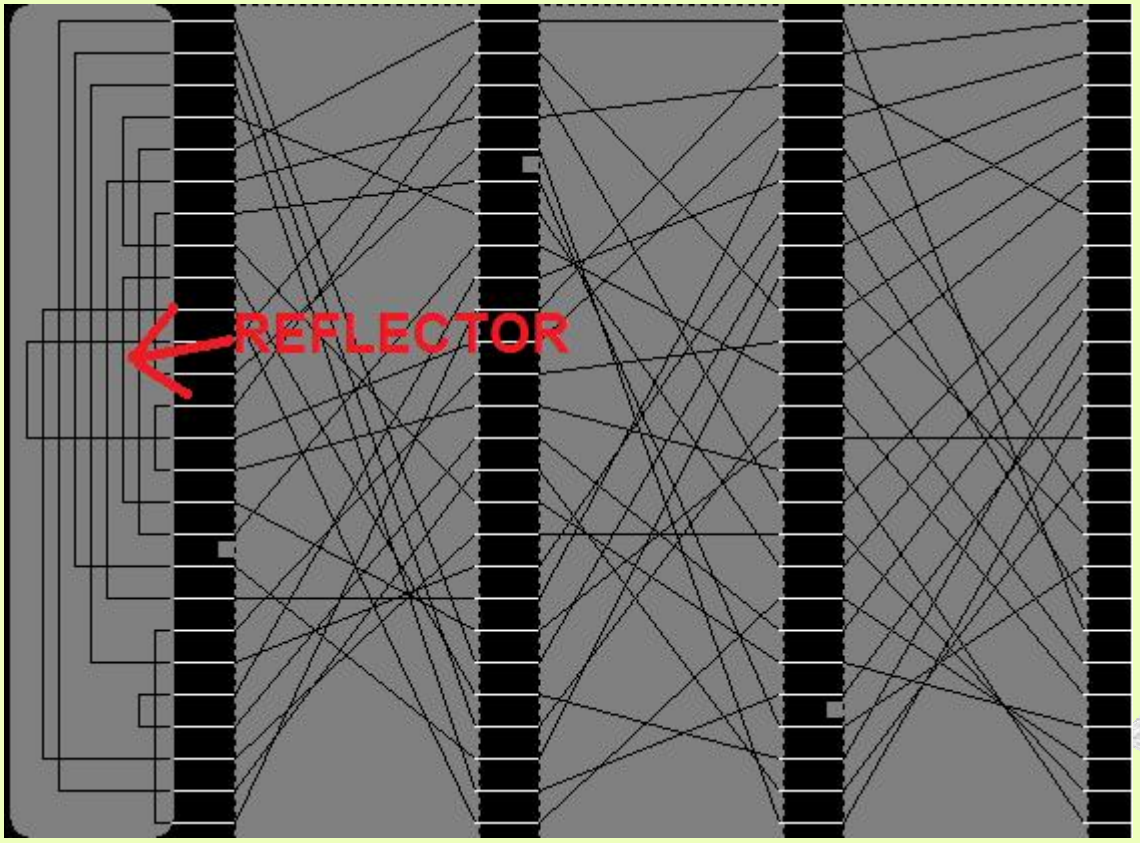
Posiciones de los modificadores, es decir, alfabetos de cifrado diferentes.

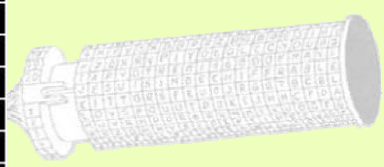
Un cifrado modificado de Vigenere de longitud de clave 17576

Más ingredientes de la Enigma

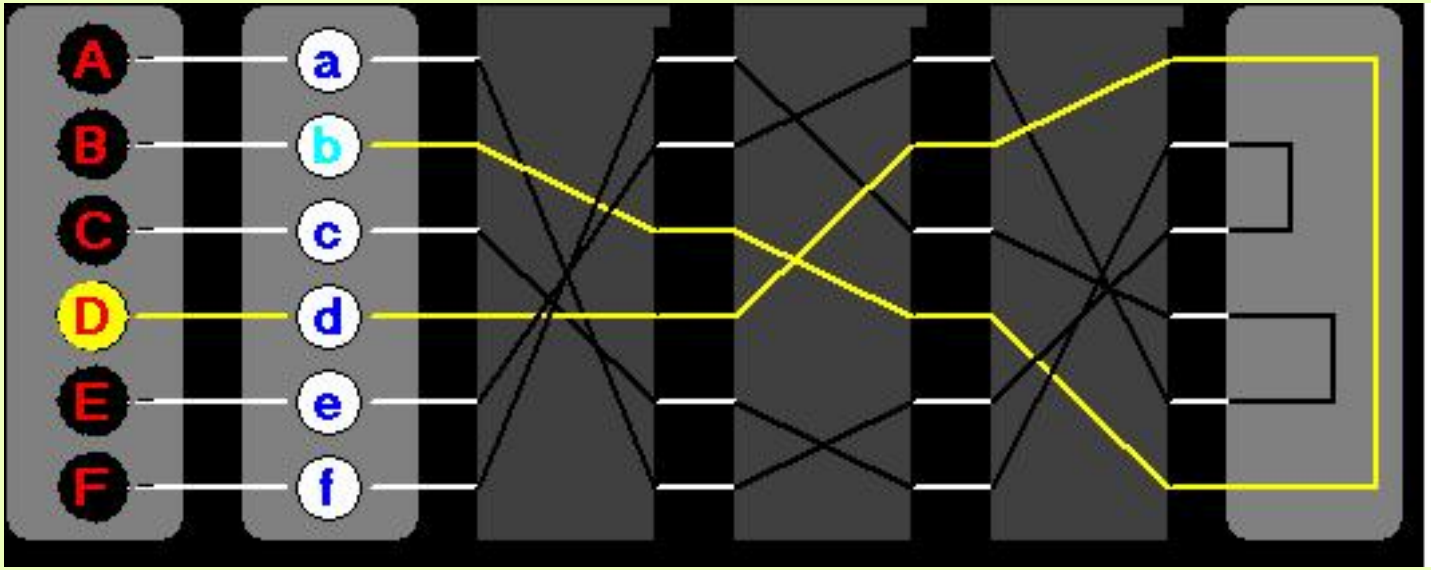
Un reflector:

Cuando se teclea un carácter, se pasa por los modificadores y llega al reflector, que “refleja” enviando otra vez la señal a los modificadores pero por otra ruta diferente.



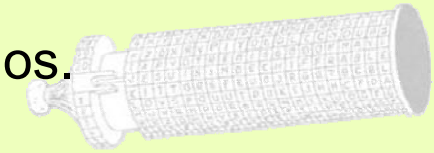


A primera vista, el reflector no añade seguridad al sistema, su beneficio se ve al cifrar y descifrar.



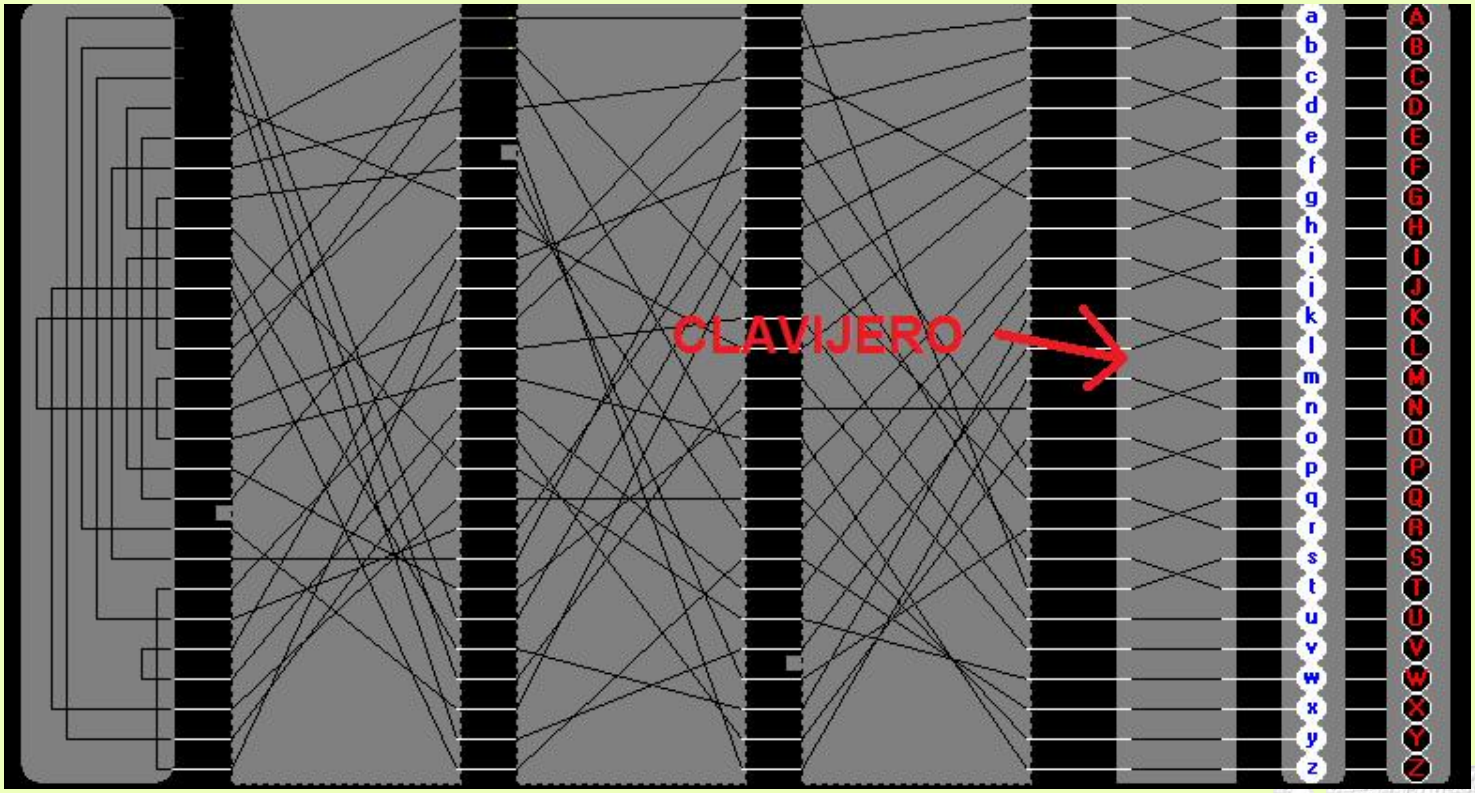
El cifrado y descifrado parte de la misma posición inicial de los modificadores. Si se cifra la b con estas posiciones se obtiene la letra D. Y si se descifra la d, se obtiene la letra B. Esta es la labor del reflector, la “simetría”.

Los modificadores son extraíbles y había 5 tipos de ellos.



El clavijero:

Permite que el emisor inserte cables entre el teclado y el primer modificador para intercambiar algunas letras antes de que se modifiquen.



Existían 10 cables para alterar 20 caracteres.

Hace las veces de un cifrado de sustitución fijo.

Número de claves posibles (posiciones):

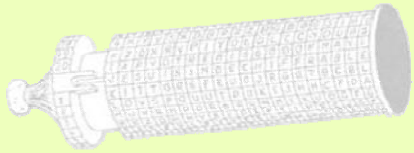
$5*4*3*26^3*150738274937250=158962555217826360000>10^{21}$

¿Por qué añadir modificadores si el número de claves proviene, en mayor medida, del clavijero?

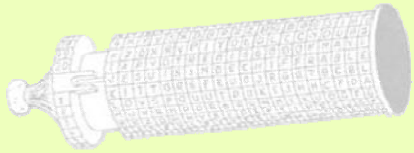
El clavijero sólo realiza un cifrado de sustitución monoalfabética. Los modificadores hacen que, al estar cambiando continuamente, no sea posible realizar un análisis de frecuencia.

A pesar de todo…..

Los británicos lograron encontrar debilidades y romper los cifrados alemanes. Entre los que lo consiguieron estaba Alan Turing.



4. LA ESTANDARIZACIÓN DEL CIFRADO

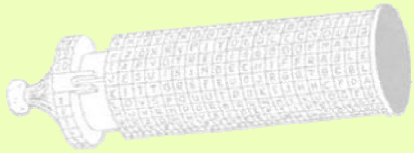


LOS ORIGENES

Los códigos de sustitución y trasposición son muy vulnerables ante ciertos tipos de ataques. Sin embargo, la aplicación sucesiva de un numero suficientemente alto de cifrados como los anteriores puede dar lugar a un cifrado producto bastante seguro (ENIGMA).

En 1973 el National Bureau of Standards (NBS) de los Estados Unidos, convocó un concurso para la adopción de un estándar de cifrado (de clave privada) para el Registro Federal.

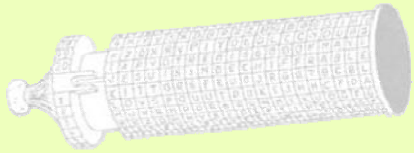
Desde 1977, este sistema se convirtió en el método estándar de cifrado (DES) en los Estados Unidos.



CARACTERÍSTICAS

DES es un sistema criptográfico de clave privada para cifrado en bloque. Esto significa que el texto en claro es troceado en bloques de longitud fija que se cifran (y posteriormente se descifran) independientemente.

Concretamente, DES cifra textos en claro de 64 bits utilizando una clave de 56 bits. El cifrado de cada bloque de 64 bits, es de nuevo un bloque de 64 bits.

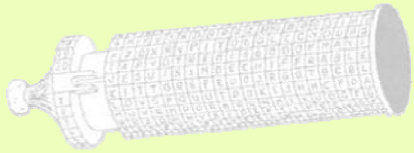


DESCRIPCIÓN GENERAL DEL ALGORITMO

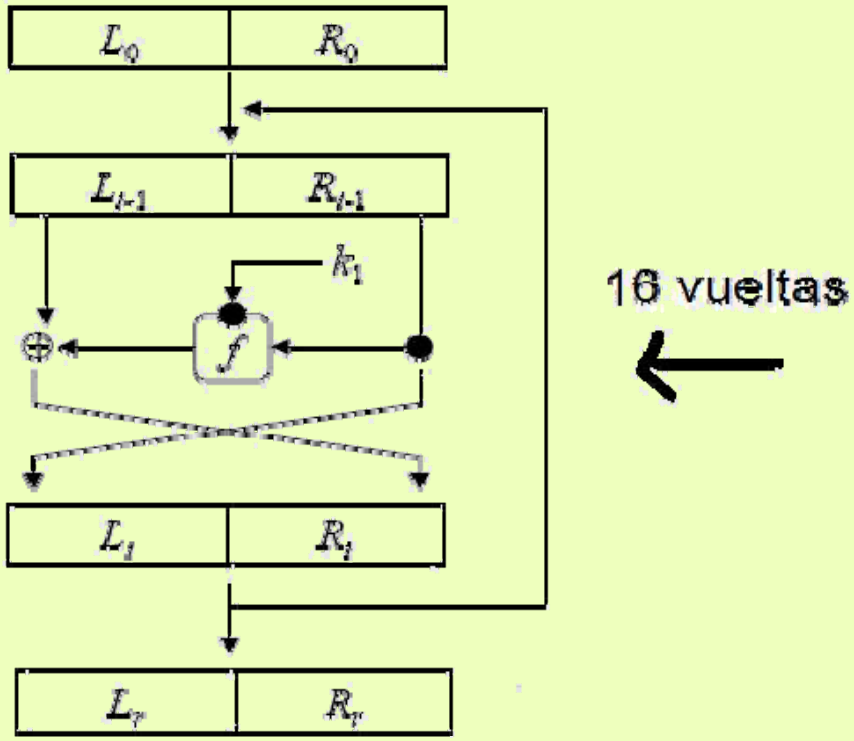
El cifrado de un texto en claro m comprende tres etapas principales:

1. Una permutación inicial, IP, de los bits de m;
2. 16 iteraciones (o vueltas) de un proceso de cifrado realizado con ayuda de la clave K;
3. Una permutación final, IP^{-1}, que es la inversa de la inicial.

La permutación inicial 'revuelve' los bits del texto en claro, mientras que la final compensa su efecto. Por supuesto, ninguna de las dos tienen influencia en la seguridad del sistema.



El conjunto de las 16 vueltas puede verse como



$$f(R_{i-1},k_i)=P(S(E(R_{i-1}) \oplus k_i))$$

E una permutación fija expansiva de 32 a 48 bits, *P* una permutación fija de 32 bits y *S* la aplicación de las *S*-cajas.

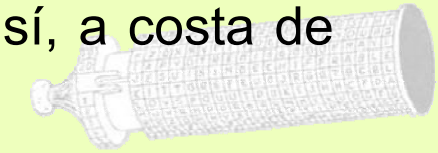
Cada caja (hay 8) es un cifrado de sustitución fijo de 6 bits en 4 bits.

LA CONTROVERSIA DEL DES

1. Desde el momento en que fue adoptado como estandar, DES ha sido objeto de considerable controversia.

2. Inicialmente, la causa fue la propia fortaleza de DES. Todas las operaciones que realiza son lineales, con excepción de las sustituciones basadas en las cajas S, (que por tanto, son vitales para su seguridad). Sin embargo, los criterios de diseño de estas cajas no han sido conocidos nunca.

3. Por otro lado, han ido desarrollándose herramientas de criptoanálisis especialmente destinadas a DES, como los conocidos diferencial y lineal. Recientemente, incluso ha sido posible descifrar mensajes cifrados con DES (eso sí, a costa de considerables recursos de calculo).

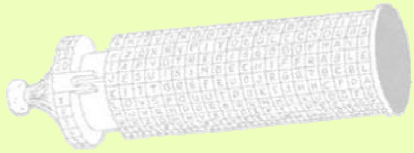


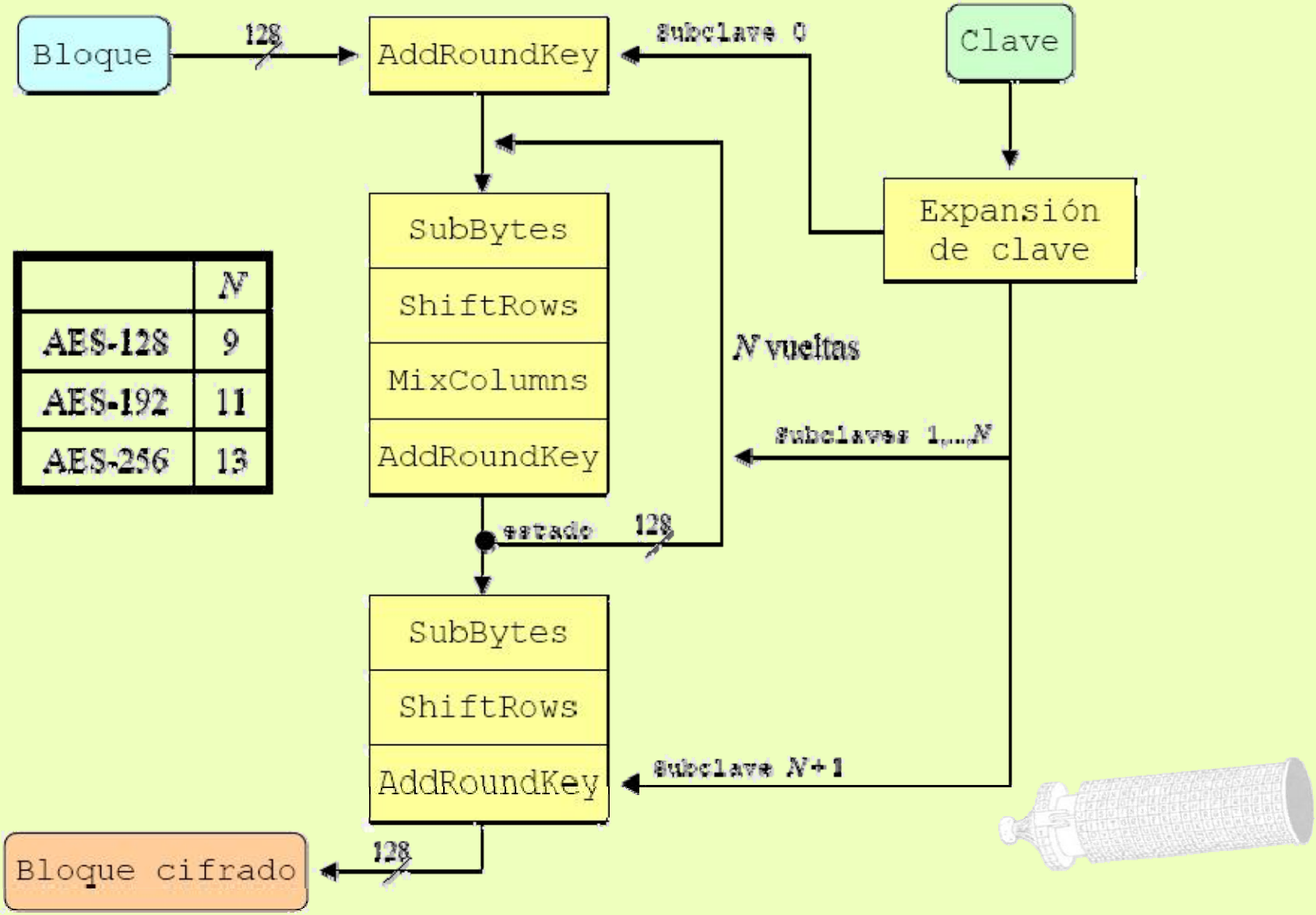
EL CAMBIO

A finales del ano 2000 fue adoptado un nuevo estándar de cifrado (AES), con lo que (al menos oficialmente) acaba la historia de DES.

1. Ser un algoritmo de cifrado en bloque simétrico.
2. Ser público (disponible gratuitamente).
3. Con posibilidad de aumentar la longitud de la clave según las necesidades del momento. En particular debe soportar (al menos) longitudes de bloque de 128 bits, y longitudes de clave de 128, 192 y 256 bits.
4. Debe ser fácilmente implementable en hardware y software.

RIJNDAEL



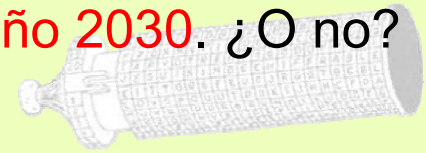

Bloque
128
AddRoundKey
Subclave 0
Clave
Expansión de clave
SubBytes
ShiftRows
MixColumns
AddRoundKey
N vueltas
Subclaves 1,...N
estado
128
SubBytes
ShiftRows
AddRoundKey
Subclave N+1
Bloque cifrado
128
N
AES-128 9
AES-192 11
AES-256 13

La característica mas llamativa de Rijndael se refiere a su forma de manejar la información (texto a cifrar y clave). A lo largo de todos los procesos que involucra, la información se trata como una secuencia de bytes (es decir, se sustituyen bits por bytes como elementos básicos).

En el proceso de cifrado los bytes son sometidos a diversas transformaciones matemáticas, que involucran operaciones aritméticas. Para llevar a cabo estas operaciones, los bytes se manejan como elementos del cuerpo:

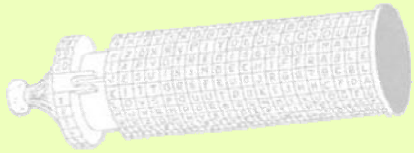
$$F_2^8 = F_{256} = F_2[X]/(X^8 + X^4 + X^3 + X + 1)$$

Usar claves de 128 bits con AES será seguro hasta el año 2030. ¿O no?



5. Y LA CLAVE SE HIZO PÚBLICA ¿O NO?

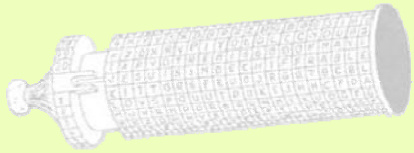
(CRIPTOGRAFÍA DE CLAVE PÚBLICA)



Problemas con la clave secreta

1. Intercambio de claves.
2. Modificación de las claves.
3. Almacenamiento de claves (n(n-1)/2 para n usuarios).
4. Autentificación e Integridad.

En 1976, Walter Diffie y Martin Hellman (*New Directions in Cryptography*) sientan las bases de la criptografía de clave pública. Hasta ahora, en la criptografía de clave secreta, el proceso de cifrado y descifrado es *similar* y la llave de cifrado y descifrado es la misma (o equivalente).

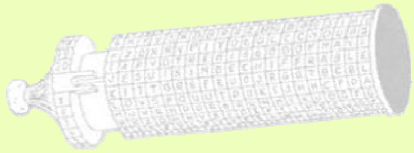


Características del nuevo paradigma

Cada usuario i posee dos claves (c_i, d_i).

- c_i pública, es la que emplea otro usuario j para transmitir un mensaje M a i (y que cifrará como $C = c_i(M)$).

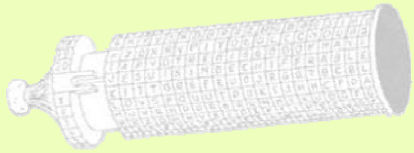
- d_i privada, conocida solo por i, le sirve para leer los mensajes que le llegan (pues $M = d_i(C) = d_i c_i(M)$).



Condiciones Diffie-Hellman de clave pública

En su articulo, Diffie y Hellman establecen los principios teóricos que debería satisfacer un sistema de clave pública:

1. El cálculo de las llaves, pública y privada, debe ser computacionalmente sencillo.
2. El proceso de cifrado debe ser computacionalmente sencillo.
3. El proceso de descifrado, conociendo la clave secreta, debe ser también computacionalmente sencillo.
4. La obtención de la clave secreta, a partir de la pública, debe ser un problema computacionalmente imposible.
5. La obtención del mensaje en claro, conociendo el mensaje cifrado y la clave pública, debe asimismo ser computacionalmente imposible.

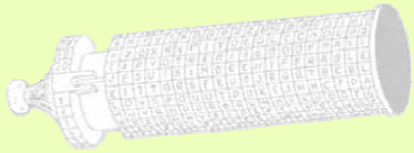


Para el cumplimiento de las condiciones de Diffie y Hellman, es necesario lo que se denomina Función Trampa.

Definición: $f : A \rightarrow B$ se denomina función de una vía si

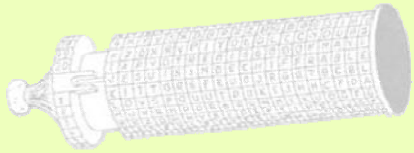
- para $x \in A$ es computacionalmente sencillo calcular $f(x)$.
- dado $y \in Im(f)$, es computacionalmente imposible, en general, determinar un elemento $x \in A$ tal que $f(x) = y$.

Una Función Trampa es una función de una vía f, tal que existe una información complementaria secreta (la trampa), que permite calcular eficientemente el inverso de f.



Posibilidades

1. Logaritmo discreto
2. Multiplicación/Factorización
3. Mochilas
4. Raíces cuadradas mod N
5. Curvas elípticas/Curvas algebraicas
6. Códigos correctores
7. Grupos
8. Etc…



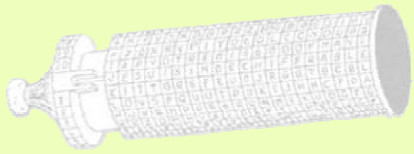
CAMBIO DE CLAVE DE DIFFIE-HELLMAN

A y *B* seleccionan públicamente un grupo cíclico finito *G*, $|G| = n$, y un generador g.

1. *A* genera un número aleatorio *a*, calcula g^a y lo envía a *B*.
2. *B* genera un número aleatorio *b*, calcula g^b y lo envía a *A*.

3. *A* recibe g^b y calcula $(g^b)^a = g^{ba}$.
4. *A* recibe g^b y calcula $(g^b)^a = g^{ba}$.

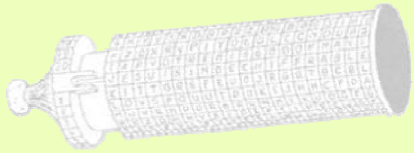
A y *B* comparten el mismo elemento secreto del grupo: g^{ab}.



RSA

La primera construcción explícita de cifrado de clave pública fue propuesta en 1978 por Rivest, Shamir y Adleman.

El candidato utilizado como función de una vía es la dificultad de factorizar un número natural.



Generación de claves

1. Cada usuario i elige una pareja de números primos p_i, q_i, suficientemente grandes (en la actualidad se cree que cada primo debe tener 100-200 cifras decimales).

2. Se considera el grupo $(Z/n_i)^*$, cuyo orden es

$$\phi(n_i) = (p_i - 1)(q_i - 1)$$

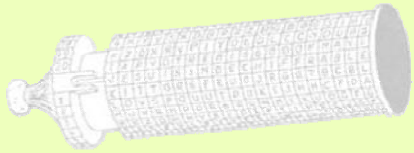
3. El usuario elige (arbitrariamente) e_i, $0 < e_i < n_i$, tal que

$$mcd(e_i, n_i) = 1$$

y su inverso modular $d_i = e^{-1} \mod \phi(n_i)$.

Clave pública: n_i, e_i

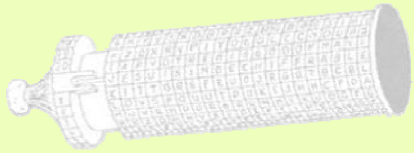
Clave privada: d_i



La *trampa* radica en el hecho de que $\phi(n_i)$ es fácil de calcular conociendo la factorización de n_i ($\phi(n_i) = (p_i - 1)(q_i - 1)$) pero difícil si tal factorización no se conoce (su dificultad computacional se considera equivalente a la de factorizar n_i).

De la misma forma, la clave secreta d_i no puede conocerse a partir de e_i sin el conocimiento de $\phi(ni)$.

Tanto los mensajes en claro como los cifrados deben previamente identificarse con elementos del conjunto Z/n_i (o si se prefiere enteros menores que n_i).



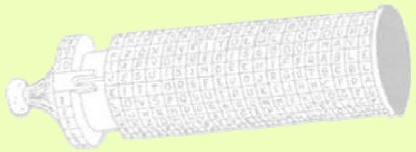
CIFRADO

$$C = M^{e_i} \mod n_i$$

DESCIFRADO

$$M = C^{d_i} \mod n_i$$

$$M^{e_i d_i} = M^{\phi(n_i)} = M \mod n_i$$



Identificación de mensajes

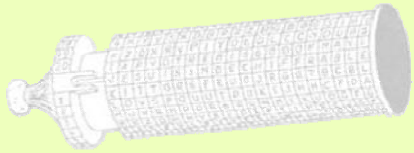
Cada usuario posee un entero n_i de forma que $N^k < n_i < N^l$.

Todo mensaje M se identifica con un elemento de Z/n_i.

$$M = m_1 N^{k-1} + m_2 N^{k-2} + \ldots + m_{k-1} N + m_k$$

E igualmente para los mensajes cifrados

$$C = c_1 N^{l-1} + c_2 N^{l-2} + \ldots + c_{l-1} N + c_l$$



EJEMPLO

Sea N = 26 letras (alfabeto castellano sin el espacio donde se ha identificado A = 0,B = 1, . . . ,Z = 25).

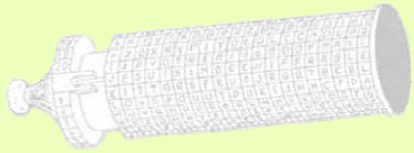
Sean k = 5 y l = 6 (los mensajes en claro serán bloques de tamaño 5 y los mensajes cifrados tendrán longitud 6).

Un usuario i ha elegido $p_i = 3851$ y $q_i = 6607$.

$$11881376 = 26^5 < n_i = 25443557 < 26^6 = 308915776$$

$$\phi(ni) = 3850 \cdot 6606 = 25433100$$

Clave pública: $e_i = 8651341$.
Clave privada: $d_i = e_i^{-1} \bmod \phi(n_i) = 4899061$.



El mensaje M = VENDE se identifica con:

$$21 \cdot 26^4 + 4 \cdot 26^3 + 13 \cdot 26^2 + 3 \cdot 26 + 4 = 9675670$$

Su cifrado es:

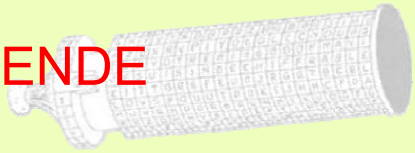
$$C = 9675670^{8651341} \bmod 25443557 = 15989266 =$$

$$1 \cdot 26^5 + 8 \cdot 26^4 + 25 \cdot 26^3 + 18 \cdot 26^2 + 19 \cdot 26 + 20 =$$

BIZSTU

y su descifrado

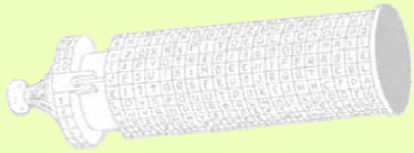
$$15989266^{4899061} = 9675670 \bmod 25443557 = \text{VENDE}$$



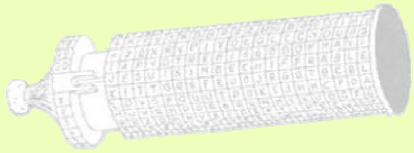
CONSIDERACIONES

- Elección de los primos p y q.
- No todos los exponentes de cifrado ofrecen la misma seguridad

  (por ejemplo existe un valor de e para el que todos los mensajes quedan inalterados al cifrarse).
- Si se utiliza el mismo exponente (pequeño) de cifrado para enviar un mensaje a varios destinatarios, éste puede ser encontrado sin conocer las claves privadas.
- El exponente de descifrado debe ser mayor que $n^{¼}$.
- No se ha demostrado si los procesos de factorizar el módulo RSA y romper el criptosistema son equivalentes.
- Ataques específicos (cíclico, cumpleaños, variaciones lineales, etc…)



6. FIRMA DIGITAL

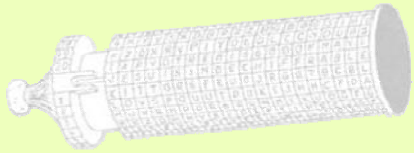


Seguridad

El acceso a las claves públicas es fácil y ello permite conocer las claves de numerosos usuarios. De este modo, ¿cómo saber quien envía el mensaje? , ¿Cómo determinar si un mensaje llega inalterado?

FIRMA DIGITAL

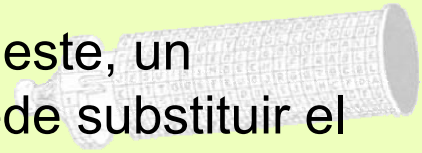
1. Autenticación del remitente: La firma digital asegura que ningún remitente puede ser suplantado por otro usuario.
2. Autenticación del mensaje: La firma digital asegura que ninguna parte del mensaje se ha modificado.



Propiedades

- Personal: Solo el propietario puede producirla.
- Infalsificable: El intento, por parte de un usuario ilegal, de falsificar tal firma debe ser computacionalmente imposible.
- Fácil de Autentificar: El receptor y eventualmente un arbitro o juez, deben ser capaces de atestiguar, la autoría de la firma.
- No repudiación: El autor de la firma no debe tener la posibilidad de rechazarla como falsa.
- Fácil de Generar.

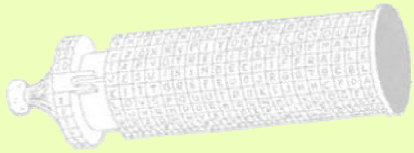
Sin embargo, a diferencia de la firma ordinaria, que es siempre la misma, la firma digital depende generalmente del mensaje.
Si la firma fuese independiente del mensaje y añadida a este, un criptoanalista que intercepte un tal mensaje firmado, puede substituir el mensaje propiamente dicho por otro falso.



LOGARITMO DISCRETO

Sea G un grupo abeliano finito y $g \in G$. Sea $< g >$ el subgrupo de G generado por g. Si $h \in < g >$, el problema del logaritmo discreto (DLP) es encontrar un entero n tal que $g^n = h$.

Conocidos g y n es computacionalmente sencillo calcular h utilizando, por ejemplo, el algoritmo de cuadrados repetidos (exponenciación modular). Sin embargo, dados g y h, se considera intratable (computacionalmente imposible) determinar n. Este hecho no es aplicable para ciertos tipos de grupos G..



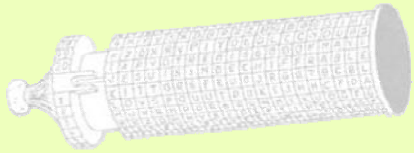
Ejemplo

Sea $p = 97$. $\mathbb{Z}_{97}$ es un subgrupo cíclico de orden $n = 96$ generado por $g = 5$.

Como $5^{32} = 35 \bmod 97$, se tiene que $\log_5 35 = 32 \bmod 97$.

Pero:

¿Quién es $\log_5 31 \bmod 97$?



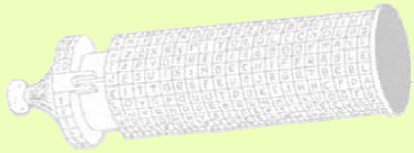
FIRMA DIGITAL ELGAMAL

Basada en el logaritmo discreto.

Se trabaja en un cuerpo finito $\mathbb{Z}/p$ y se dispone de un generador g.

Cada usuario A elige un entero a, $1 \leq a \leq p - 2$.

- Clave pública: $g^a \bmod p$.
- Clave privada: a.



GENERACIÓN DE FIRMA

1. A genera un número aleatorio h, $1 \leq h \leq p - 2$, tal que mcd (h, p−1)= 1.

2. A calcula $r = g^h \bmod p$.

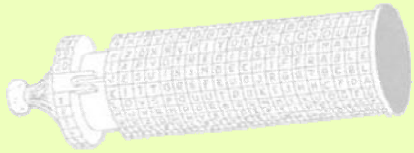
3. Si m es el mensaje a firmar, A resuelve en s la ecuación

$$m = a \cdot r + h \cdot s \bmod (p - 1)$$

(a es la clave privada de A, sólo conocida por él)

calculando $h^{-1} \bmod (p - 1)$ y determinando $s = h^{-1} (m - a \cdot r) \bmod (p - 1)$.

4. A envía a B el mensaje cifrado y su firma digital: (c, (r, s)).



VERIFICACIÓN DE FIRMA

1. Se recibe el mensaje cifrado y su firma:
$$(c, (r, s))$$

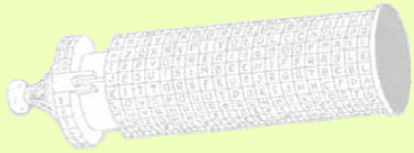
2. B calcula los elementos
$$(g^a)^r \bmod p,$$
$$r^s \bmod p = g^h \, g^{h^{-1}(m - a \cdot r)} \bmod p = g^{(m - a \cdot r)} \bmod p$$

3. B comprueba que
$$r^s \cdot (g^a)^r \bmod p = m \bmod p,$$
donde m es el descifrado del mensaje c.

Si esta última igualdad no se cumple, o bien el mensaje ha sido alterado, o bien no fue A quien envió el mensaje.

6. Y ADEMAS ¿PARA QUÉ?

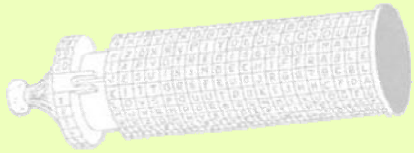
PROTOCOLOS CRIPTOGÁFICOS



Protocolo. Es el conjunto de acciones coordinadas que realizan dos o más partes o entidades con el objeto de llevar a cabo un intercambio de datos o información.

Los Protocolos criptográficos serán aquellos que cumplen esta función usando para ello algoritmos y métodos criptográficos.

Su objetivo es dar una solución a distintos problemas de la vida real, especialmente aquellos en donde puede existir un grado de desconfianza entre las partes.

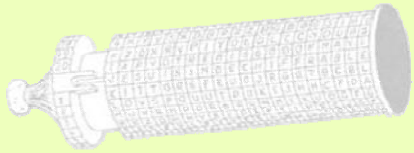


➢ Identificación del usuario

¿Cómo permitir que un usuario se identifique y autentique ante una máquina -y viceversa- con una clave, password y no pueda ser suplantado por un tercero

➢ Lanzamiento de una moneda

¿Cómo permitir que dos usuarios realicen una prueba con probabilidad ½ -como es el lanzamiento de una moneda- si éstos no se encuentran físicamente frente a frente y, a la vez, asegurar que ninguno de los dos hace trampa?

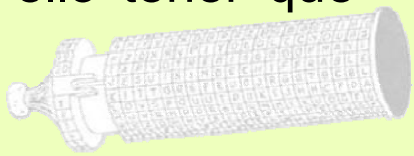


➢ Firma de contratos

¿Cómo permitir que dos o más usuarios que se encuentran físicamente alejados puedan realizar la firma de un contrato, asegurando que ninguno de los firmantes va a modificar las condiciones ni negarse a última hora a dicha firma?

➢ Descubrimiento mínimo de un secreto

¿Cómo poder demostrar y convencer a otra persona o a un sistema que uno está en posesión de un secreto, sin por ello tener que desvelarlo ni a ella ni a un tercero?

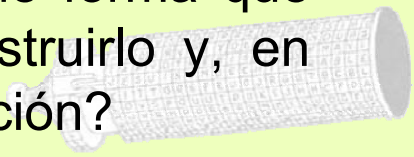


➢ Póquer mental o por teléfono

¿Cómo permitir que dos o más usuarios puedan jugar a través de la red una partida de póquer -o de cualquier otro juego de cartas – si no están físicamente en una misma mesa de juego y asegurando, al mismo tiempo, que ninguno de ellos va a hacer trampa?

➢ División de un secreto

Si tenemos un único secreto, y por tanto muy vulnerable, ¿cómo permitir que ese secreto sea dividido en n partes, de forma que juntando al menos $k < n$ partes sea posible reconstruirlo y, en cambio, con $k - 1$ partes, sea imposible su reconstrucción?

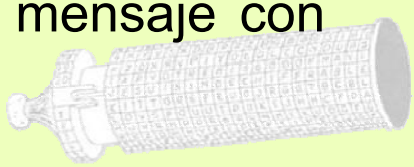


➢ Esquema electoral o voto electrónico

¿Cómo realizar unas elecciones a través de una red, de forma que pueda asegurarse que el voto es único y secreto, que los votantes y mesas estén autenticados, y se pueda comprobar que el voto se contabiliza adecuadamente?

➢ Transmisión por canales subliminales

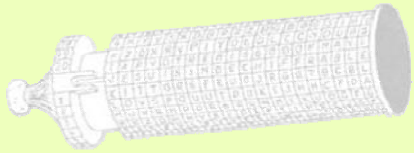
Dos usuarios desean intercambiar información a través de un tercero del cual desconfían. ¿Cómo pueden hacerlo sin cifrar la información de forma que este tercero sólo vea un mensaje con texto en claro aparentemente inocente?



➢ Problema del millonario

Dos usuarios desean conocer cuál de los dos tiene más dinero en su cuenta corriente. ¿Cómo pueden hacerlo de forma que, una vez terminado el protocolo, ambos sepan quién de los dos es más rico sin por ello desvelar el dinero que tiene el otro?

➢ .....



JUDFLDVCSRUCWRGR!!!!

-

DDDDDDDDDDDDDDDDD

=

GRACIAS POR TODO!!!!