



Mensajes secretos.

María Jesús Rodríguez Gallo





1. Shhhhhhhh...
2. CRIPTOGRAFÍA CLÁSICA.
3. CRIPTOGRAFÍA DE CLAVE PÚBLICA.
4. SABER MÁS.

1. Shhhhhhhh....



La curiosidad, el deseo de descubrir secretos está profundamente arraigado en la naturaleza humana.

Desde que las criaturas pueden comunicarse utilizando un lenguaje, aparecen las comunicaciones confidenciales.



los reyes católicos reciben un mensaje cifrado junto con el libro de claves

Madrid, 1495

Cansados de que sus despachos privados fueran interceptados y leídos, los reyes católicos mandan desarrollar uno de los primeros sistemas de codificación de mensajes.

El código elegido ha sido la conversión de palabras en series de números romanos, pero el sistema se ha complicado tanto que monosílabos como "en" se representan como "DCCCCI.XVIII".

Son frecuentes las contestaciones del tipo "No se entiende", "No tiene sentido", "Mande otro despacho".

Para asegurar su comprensión, el diplomático Rodrigo González de la Puebla ha decidido incluir en su último despacho el libro de claves correspondientes.

Reyes, reinas, generales ... durante miles de años han dependido de estas comunicaciones para gobernar sus países, ordenar a sus ejércitos...

criptografía

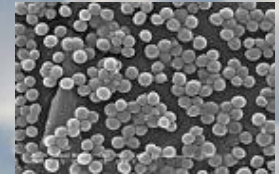
κρυπτός



Las naciones tienen departamentos dedicados a crear sistemas de cifrado y, a la vez, a tratar de descifrar los mensajes ajenos y robar los secretos de otros.



Lucha: cada sistema de cifrado debe enfrentarse a los ataques de los descifradores.



Seguridad de las comunicaciones es vital: Internet, comercio electrónico.

conento

Desde un servidor dedicado para cada proyecto y hasta la máquina del cliente, la seguridad de información a través de Internet queda protegida bajo los **robustos algoritmos de encriptación de 256 bits SSL**.

SSL: protocolo criptográfico de cifrado simétrico.

1. Shhhhhhhh....

En Egipto, la criptografía alcanzó la categoría de ciencia, y los sacerdotes egipcios nos dejaron múltiples ejemplos de escritura cifrada.



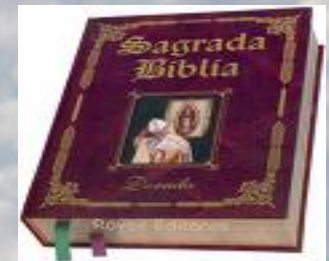
Según Herodoto, el arte de la escritura secreta salvó a Grecia (siglo V a. C). de ser ocupada por Jerjes, el Rey de Reyes, el despótico líder de los persas.

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	
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	

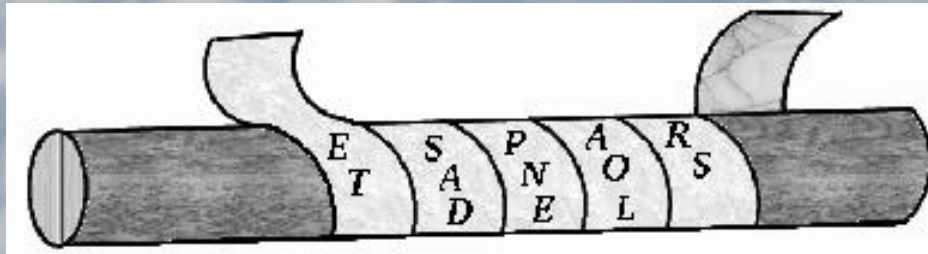
El sistema atbash, aparece en la Biblia, en Jer. 25, 26, que escribe Sesac en lugar de Babel.

XLNVNGL ¿¿¿¿???? **CONENTO**

ABCDEF GH IJK LMNÑOPQRSTUVWXYZ
ZYXWVUTSRQPONML KJ I HGFEDCBA



Hace 2500 años: el gobierno espartano enviaba mensajes a sus generales utilizando el **escítalo**, el primer aparato criptográfico de la historia.



Cifrado: Se escribe el mensaje a lo largo de la longitud del escítalo y luego se desenrosca la tira.

Descifrado: Se enrosca la tira en otro escítalo del mismo diámetro.

ET_SADPNEAOLRS_ ¿¿¿¿????

ESPARTANOS DEL_

NO_E
S_TA
N_FA
CIL

NSNCO__I_TFLEAA ¿¿¿¿????

NO_ES_TAN_FACIL

Criptosistema de TRANSPOSICIÓN

Formación Conento: febrero 2008

Julio César ya utilizaba un criptosistema para enviar mensajes secretos a Cicerón en el siglo I a.C.



CONENTO → FRPHPWR
 HOLA → KRÑD

Cifrado: sustituir cada letra del mensaje por la que se encuentra tres posiciones más allá en el alfabeto.

Descifrado: sustituir cada letra del mensaje por la que se encuentra tres posiciones a la izquierda en el alfabeto.

Criptosistema de SUSTITUCIÓN



ABCDEF GHIJK LMNÑOPQRSTUVWXYZ
 D F H K Ñ P W

ABCDEF GHIJK LMNÑOPQRSTUVWXYZ
 DEF GHIJK LMNÑOPQRS TUVWXYZABC

Matemáticamente:

ABCD E F G H I J K L M N Ñ O P Q R S T U V W X Y Z
01 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

Cifrado: $* \rightarrow * + 3.$

Descifrado: $* \rightarrow * - 3.$

¿Y si nos pasamos de 26? $Y=25 \rightarrow 25+3=28$ ¿letra? B

¡¡¡¡¡porque $28 = 1!!!!!!$

En general: cifrado de César con clave k

Cifrado: $* \rightarrow * + k.$

Descifrado: $* \rightarrow * - k.$

Cifra AVE CESAR con clave $k=5$

FAJ HJXFW

Descifra KDV GHVFXELHUWR HÑ VHFUHW R

HAS DESCUBIERTO EL SECRETO clave $k=3$

ARITMÉTICA DEL RELOJ: $10 + 6 = 4$



$16 = 4$ porque su diferencia es 12;
 $19 = 7$ porque su diferencia es 12;
 $26 = 2$ porque su diferencia es 24, etc.

ARITMÉTICA MODULAR: reloj \rightarrow módulo 12

Dos números enteros son iguales si se diferencian en un múltiplo del módulo.

Módulo 2: 0, 1, 0, 1, 0, 1,... un par es 0 y un impar es 1

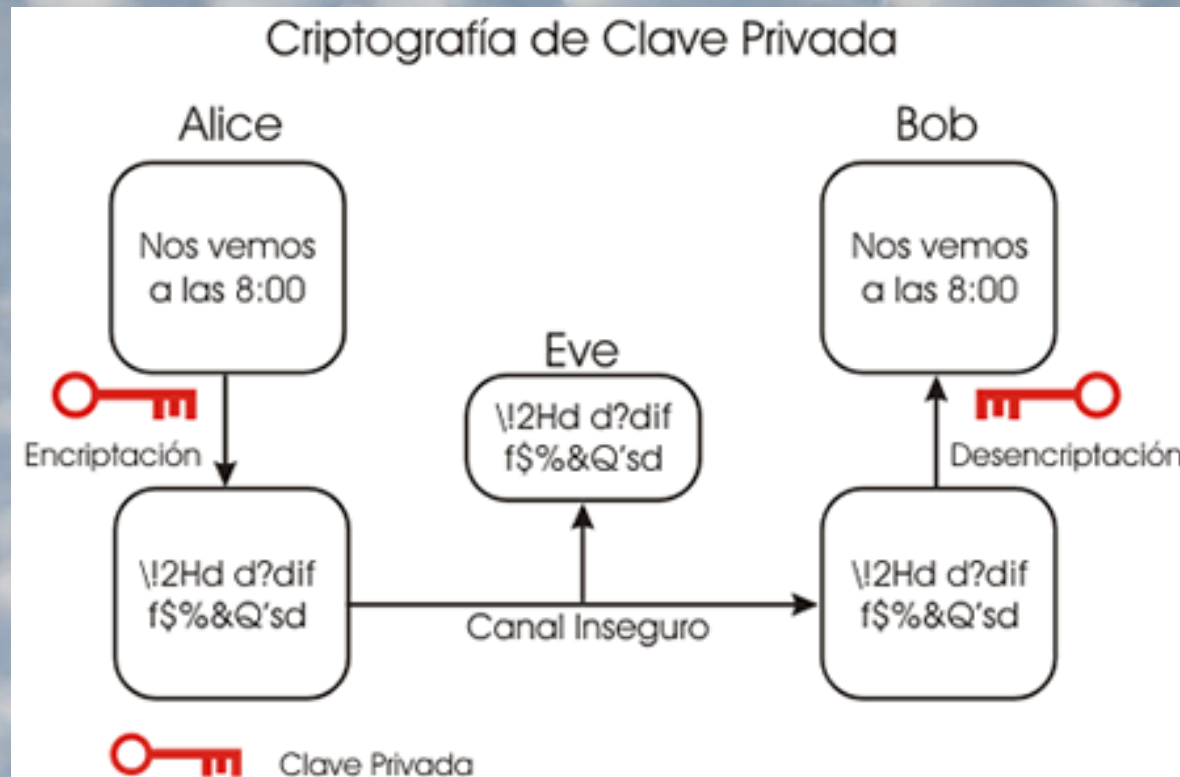
Módulo 3: 0, 1, 2, 0, 1, 2,... $6 = 0 \pmod{3}$, $7 = 1 \pmod{3}$, $8 = 2 \pmod{3}$,
 $9 = 0 \pmod{3}$, etc...

Módulo p: 0, 1, 2, ..., p-1, 0, 1, 2, ...

Criptografía clásica: de clave privada (simétrica).

Escívalo → diámetro

César → $k=3$



Idea fundamental: fácil de hacer, difícil de deshacer –sin clave–.

Criptografía clásica: de clave privada (simétrica).

Clave: 128 bits de longitud son suficientes.

Problemas

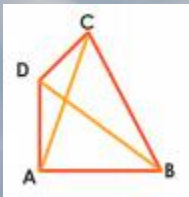
- la clave secreta sólo deben conocerla emisor y receptor → hace falta un **intercambio seguro de claves**.
- cada pareja de usuarios necesita una clave secreta → **hacen falta muchas claves...**

Si son dos, una;

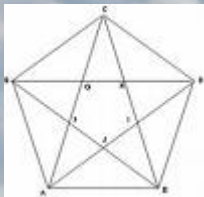
Si son tres, tres;

Si son cuatro, seis;

Si son N usuarios $N(N-1)/2$

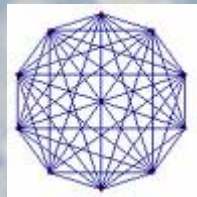


N=4



N=5

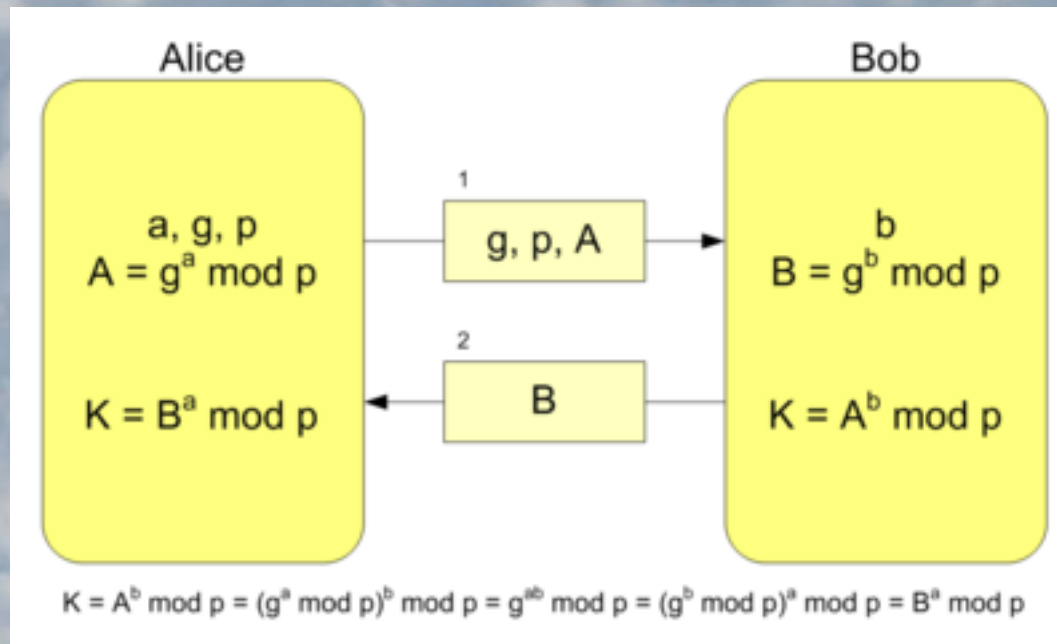
....



N=10

Intercambio seguro de claves (Diffie & Hellman)

Protocolo que permite el intercambio secreto de una clave entre dos partes que no han tenido contacto previo, utilizando un canal inseguro.



p es un número primo, $g < p$ y ambos pueden ser públicos.

Alice escoge $a < p$. Bob escoge $b < p$. La clave es K

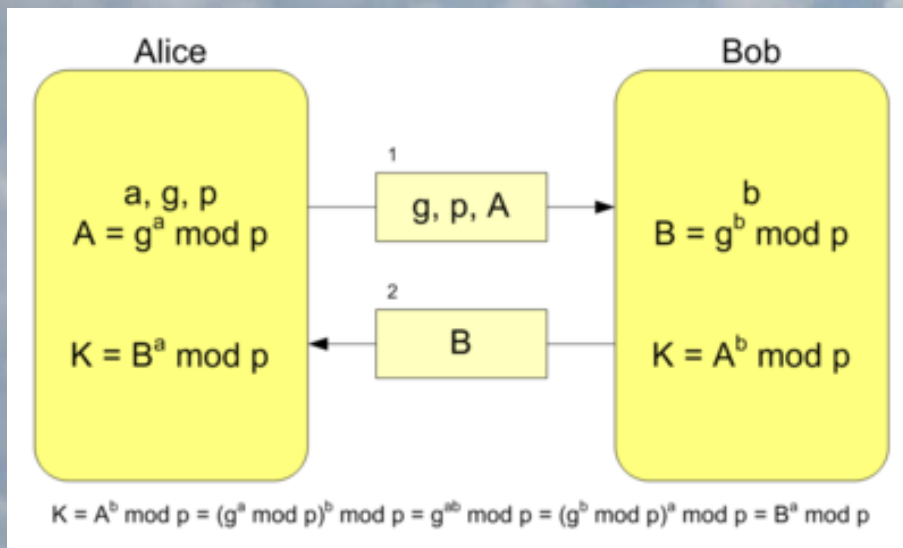
Intercambio seguro de claves (Diffie & Hellman)

¿Y si alguien intercepta A ó B?

Si logran obtener a ó b, podrían calcular la clave.

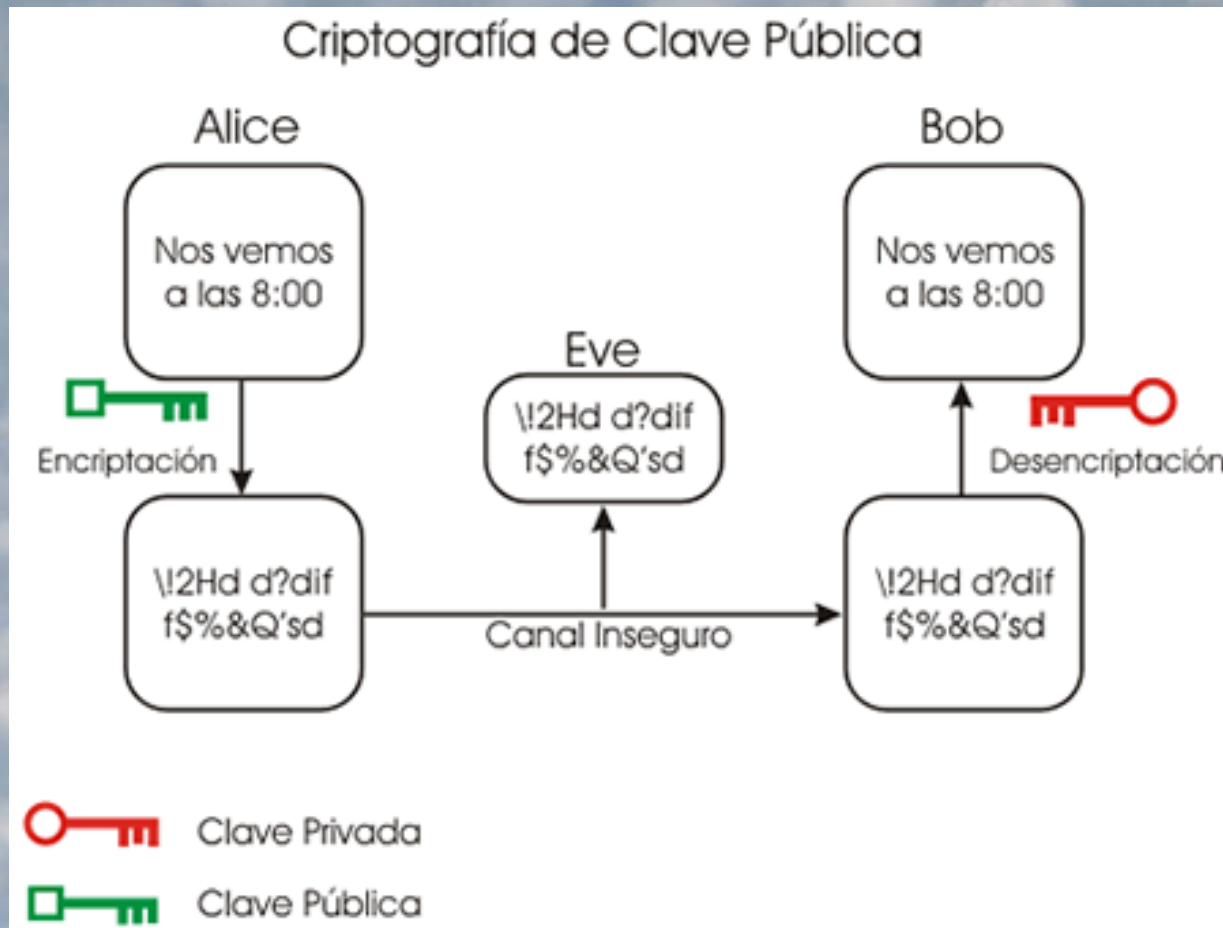
Por ejemplo, deben encontrar un número a tal que:

$$4^a = 5 \pmod{11} \quad g^a = A \pmod{p}$$



Problema del logaritmo discreto:
en aritmética modular es

- fácil: elevar a un exponente.
- difícil: obtener el logaritmo



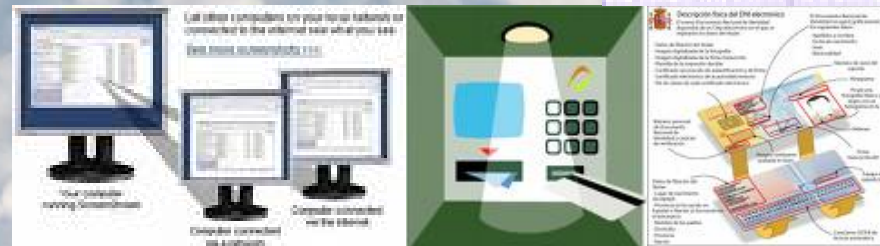
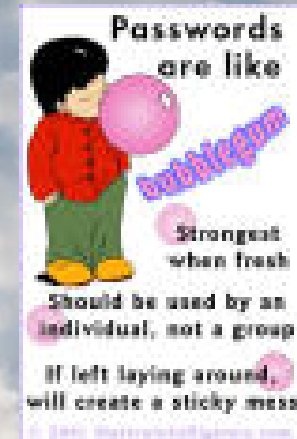
Criptografía de clave pública (asimétrica).

En los años 70, surge un nuevo tipo de criptografía.
Cada usuario dispone de:

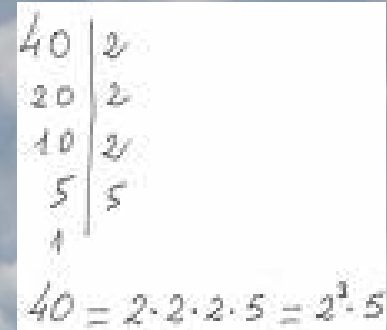
- una clave pública para cifrar.
- una clave privada para descifrar.

Ventajas:

- No hace falta intercambiar claves.
- Si hay N usuarios sólo hacen falta N claves.



RSA: Rivest-Shamir-Adleman (1977)



Fácil: multiplicar

Difícil: factorizar, descomponer en factores primos

¿Por qué es difícil?

$$486 = 2 \times 3^5$$

$$713 = 23 \times 31$$

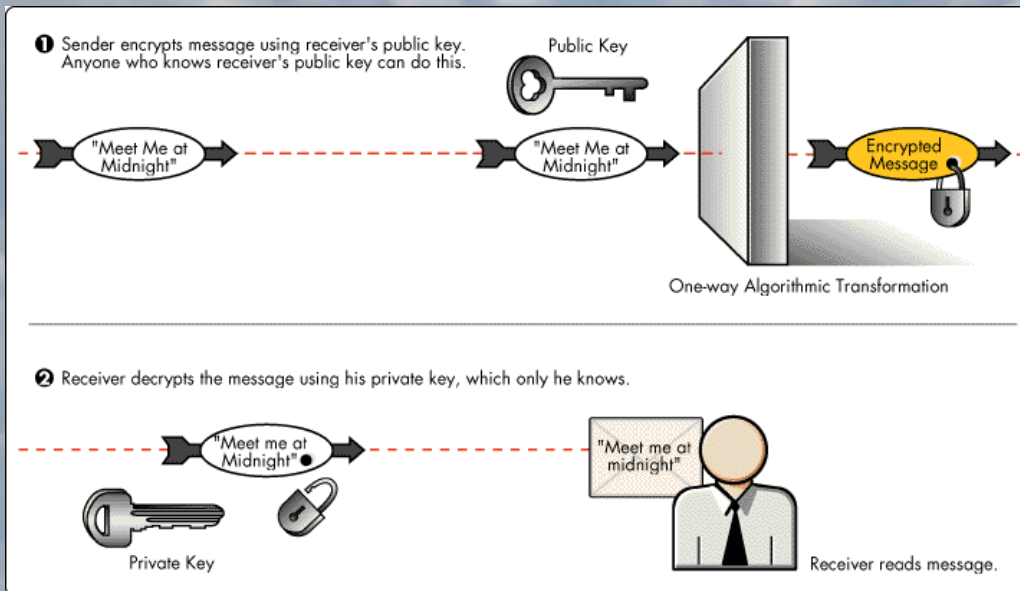
$$23360947609 = 152041 \times 153649$$

12 cifras → 1 seg.

20 cifras → 1 año = 31536000 seg

50 cifras → 10³⁰ años

Formación Conento: febrero 2008



Clave pública: se recomienda al menos 1024 bits.

RSA-640, Noviembre, 2005.

Factores:

1634733645809253848443133883865090859
8417836700330923121811108523893331001
04508151212118167511579

y

1900871281664822113126851573935413975
4718967899685154936666385390880271038
02104498957191261465571

Aprox. 30 2.2GHz-Opteron-CPU años en cinco meses.



Simón Singh. *Los Códigos Secretos.*
El arte y la ciencia de la criptografía, desde el antiguo Egipto a la era Internet.
Editorial Debate. ISBN. 84-8606-278-X

Preguntas:

¿Cuántos números se pueden escribir con n bits?