Financiado por la Unión Europea NextGenerationEU

Gobierno de España · Ministerio para la Transformación Digital y de la Función Pública · Secretaría de Estado de Telecomunicaciones e Infraestructuras Digitales

Plan de Recuperación, Transformación y Resiliencia

incibe_ Instituto Nacional de Ciberseguridad

UC Universidad de Cantabria

Ciberseguridad y Criptografía: la clave está en las matemáticas

Adriana Suárez Corona

estalmat castilla y león

xvii seminario nacional estalmat, castro urdiales 2025

Real Academia de Ciencias Exactas, Físicas y Naturales de España

Purposeful Ventures

CIEM Centro Internacional de Encuentros Matemáticos

Excmo. Ayuntamiento de Castro Urdiales

Y aún me quedan más logos...

Contexto

- 2014-2016. Estalmat Ponferrada. Alumnos 1º y 2º ESO
- 2017-…. Estalmat León. Alumnos 1º y 2º ESO
- 2021-2024 CREECYL. Alumnos 1º y 2º ESO
- 2021. Cátedra Institucional de Ciberseguridad. Alumnos desde 5º primaria a Bachillerato

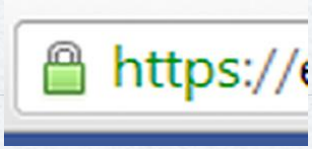
DATOS

- Objetivos:
  - Conocer qué es la criptografía y qué papel juega en la Ciberseguridad
  - Conocer los objetivos de la criptografía
  - Conocer cómo funcionan algunos esquemas criptográficos y su seguridad
  - Realizar actividades prácticas con esquemas de cifrado

DATOS

- Estructura:
  - Primera parte: desarrollo de los conceptos.
  - Segunda parte: resolución de ejercicios prácticos
- Material utilizado:
  - Fotocopias con enunciados
  - Rueda de cifrado de César/ Ordenador

¿HABÉIS USADO CRIPTOGRAFÍA HOY?



Criptografía

- Criptografía significa “escritura secreta”.
- El principal objetivo de la criptografía era conseguir la confidencialidad de los mensajes.
- De forma más general, se encarga de conseguir comunicaciones seguras en presencia de adversarios.
- Hoy en día se utiliza para muchas más cosas: votos electrónicos, firmas digitales, monedas digitales…

Aplicaciones

¿Cuándo necesitamos comunicarnos de forma secreta?

- Poseemos información muy importante que queremos proteger
- Nos encontramos lejos de la persona con la que queremos comunicarnos

¿Cuándo creeis que empezaron a desarrollarse técnicas para establecer comunicaciones secretas?

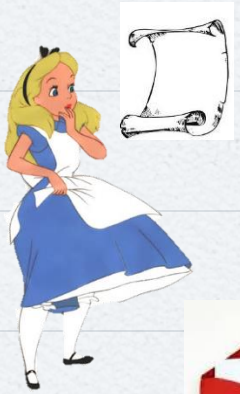
- Desde antes los Griegos y los Romanos….
- Ha tenido un papel muy importante en guerras, y hoy en día lo tiene en transacciones económicas, etc

Envío de mensajes

Canal Inseguro

Adversario

Envío de mensajes secretos



Canal Inseguro

Usan claves

Transforma el mensaje en algo incomprensible para el adversario

Recupera el mensaje original a partir del transformado

Cifrado

- Se necesita que la persona que envía el mensaje y la que lo recibe se pongan de acuerdo en el método de cifrado que se va a usar y/o en la clave.
- Un espía que quiera averiguar el contenido del mensaje deberá averiguar las dos cosas para poder descifrar el mensaje.

Navajos

- En la Segunda Guerra Mundial, el cuerpo de Marines de EEUU utilizó el Código Navajo.
- Se basaba en el idioma de los indios Navajos, que era prácticamente imposible de aprender sin haber estado familiarizado con sus creadores y que sólo los navajos podían decodificar.

Navajos

- La película Códigos de Guerra, de Nicholas Cage, refleja cómo los navajos y su "código" colaboraron con los marines.
- Podéis consultar el diccionario de Navajo aquí: https://www.history.navy.mil/research/library/online-reading-room/title-list-alphabetically/n/navajo-code-talker-dictionary.html

- Sin embargo, lo más usual no es utilizar idiomas poco conocidos para transmitir mensajes confidenciales….

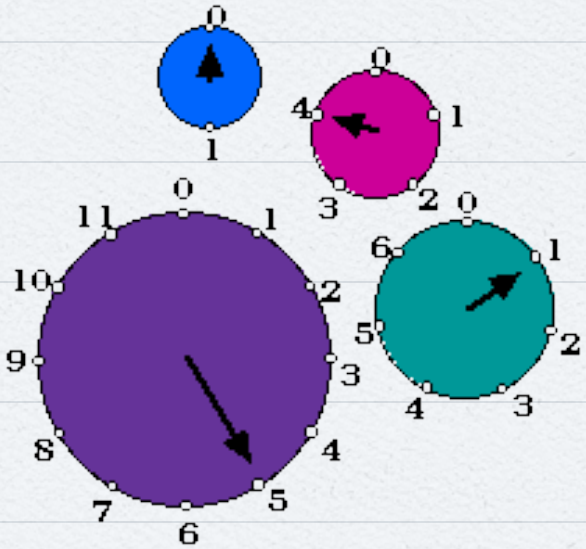
Matemáticas usadas en criptografía

- Si queremos confidencialidad, necesitaremos

  Matemáticas Discretas

- En particular, teoría de números: estudio de los números enteros.

Aritmética del reloj

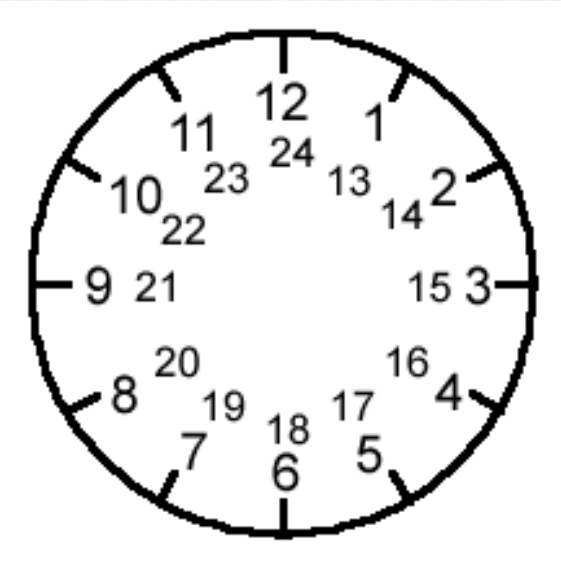


Aritmética del reloj

¿Qué hora es si son las:

- ✗ 13h?
- ✗ 16h?
- ✗ 20h?
- ✗ 23h?

Aritmética del reloj



Aritmética del reloj

¿Cómo hacemos estas transformaciones?

En el primer caso, dividimos el número entre 12 y el resto es nuestro resultado.

¿Y SI PUDIÉRAMOS CONSIDERAR RELOJES CON CUALQUIER NÚMERO DE HORAS?

La operación *a mod n*, es el resto de realizar la división *a entre n*. Se lee *a módulo n*.

- Ejemplos:

20 mod 4?

21 mod 4?

23 mod 6?

-1 mod 6?

El resultado es un entero entre *0* y *n-1*.

La aritmética del reloj sería el caso particular de aritmética módulo 12.

Aritmética modular

- Si ahora son las 4 pm.
- ¿Qué hora era hace 11 horas?
- ¿Y hace 8 horas?

¡Podemos hacer sumas y restas con relojes de cualquier número de horas!

¡También podremos hacer multiplicaciones y potencias!

Haremos las operaciones del modo habitual, considerando los restos de dividir entre el módulo considerado.

Ejercicio

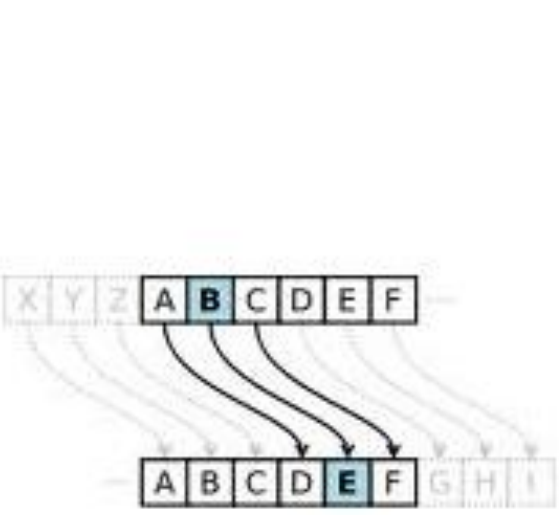
- Calcula las siguientes operaciones:

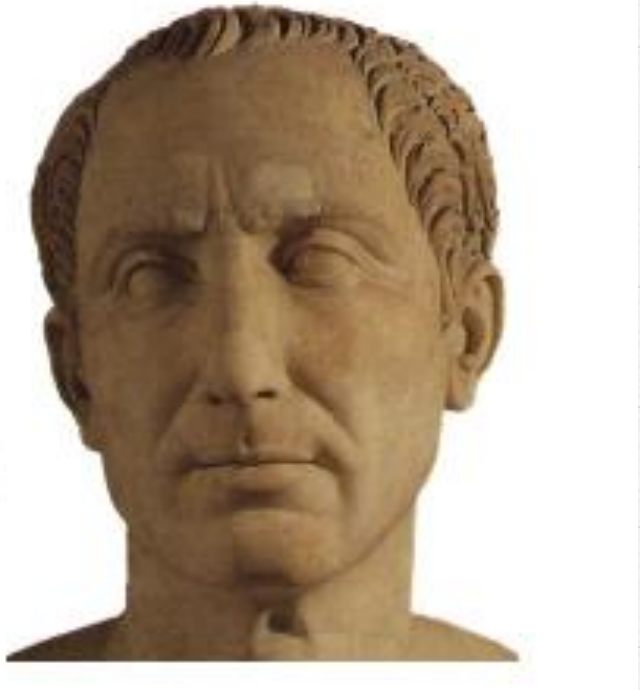
- $3+14 \bmod 7$
- $-3 \bmod 10$
- $4-5 \bmod 6$
- $3x3 \bmod 8$

Criptosistemas clásicos

- Veremos algunos ejemplos de los esquemas de cifrado más antiguos...

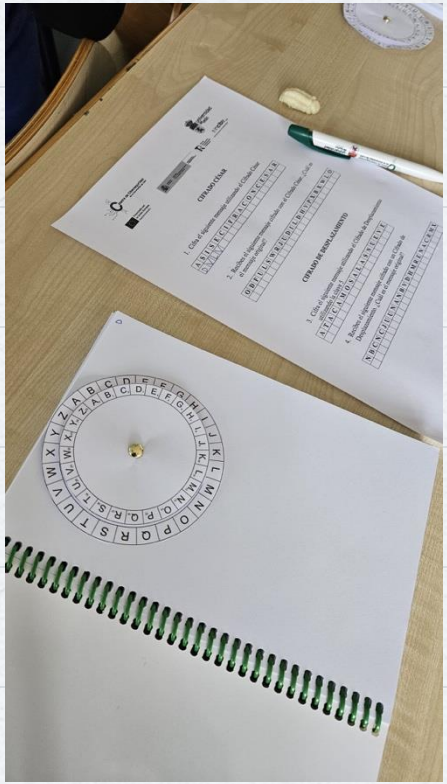
Cifrado César

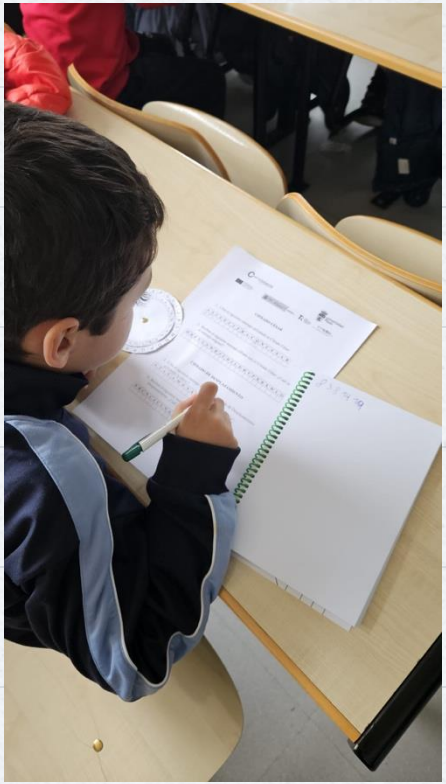




Cifrado César

Cifrado César





Cifrado César

- Se usaba ya en el 54 AC
- Consiste en sustituir cada letra por la que se encuentra 3 posiciones más adelante en el alfabeto.

EJEMPLO:

MENSAJE: ATACAMOS A LAS NUEVE.

MENSAJE CIFRADO: DWDFDORV D ODV PXHYH

Ejercicio

- Cifra el siguiente mensaje usando el cifrado César:

- ASISECIFRACONCESAR

Ejercicio

- Cifra el siguiente mensaje usando el cifrado César:

- ASISECIFRACONCESAR
- DVLVHFLIUDFRQFHVDU

Cifrado César con números

- Como es mucho más fácil realizar operaciones con números que con letras y además tenemos más opciones con estos, la mayoría de los sistemas de cifrado comienzan por pasar el texto a números.
- Para ello, lo más sencillo es asignar a cada letra el lugar que ocupa en el abecedario, empezando en el 0:

A	B	C	D	E	F	G	H	I	J	K	L	M
0	1	2	3	4	5	6	7	8	9	10	11	12

N	O	P	Q	R	S	T	U	V	W	X	Y	Z
13	14	15	16	17	18	19	20	21	22	23	24	25

Cifrado César con números

- Si a cada letra le damos un valor numérico,

A=0, B=2, C=3,…., Z=25

- El cifrado César consistiría en sumar 3 a cada letra, usando la aritmética de un reloj de 26 horas (aritmética módulo 26).

A	T	A	C	A	M	O	S	A	L	A	S	N	U	E	V	E
0	19	0	2	0	12	14	18	0	11	0	18	13	20	4	21	4

Cifrado César más general

- Si nuestro adversario sabe que estamos usando el Cifrado César, si intercepta un mensaje, sería capaz de descifrarlo.

- Podemos hacerlo más difícil de descifrar si permitimos elegir el número de posiciones que movemos las letras.

- En este caso, la clave secreta sería ese número, que deberíamos compartir con la persona con la que nos queremos comunicar.

- ¿Cuántas claves diferentes se pueden elegir?

Ejemplo

Cifra el siguiente mensaje con clave 5:

A	T	A	C	A	M	O	S	A	L	A	S	N	U	E	V	E
0	19	0	2	0	12	14	18	0	11	0	18	13	20	4	21	4

Ejemplo

Cifra el siguiente mensaje con clave 5:

A	T	A	C	A	M	O	S	A	L	A	S	N	U	E	V	E
0	19	0	2	0	12	14	18	0	11	0	18	13	20	4	21	4

FYFHFRTXFQFXSZJAJ

Atacando el cifrado César generalizado

- Este mensaje se ha cifrado usando el método anterior, pero no sabemos cuál es la clave secreta, ¿Podríais descifrar este mensaje?

- Lzallzbulqltwsvklhahjhybujypwavzpzalthbzhukvshmblyghiybah
- ¿Cómo se os ocurriría atacarlo?

Atacando el cifrado César generalizado

- Este mensaje se ha cifrado usando el método anterior, pero no sabemos cuál es la clave secreta, ¿Podríais descifrar este mensaje?
- Lzallzbulqltwsvklhahjhybujypwavzpzalthbzhukvshmblyghiybah
- El mensaje, utilizando la clave 7, sería:
- esteesunejemplodeatacaruncriptosistemausandolafuerzabruta

Cifrado Monoalfabético

- Otra opción para aumentar el tamaño de claves, es poder sustituir cada letra por otra de nuestra elección.

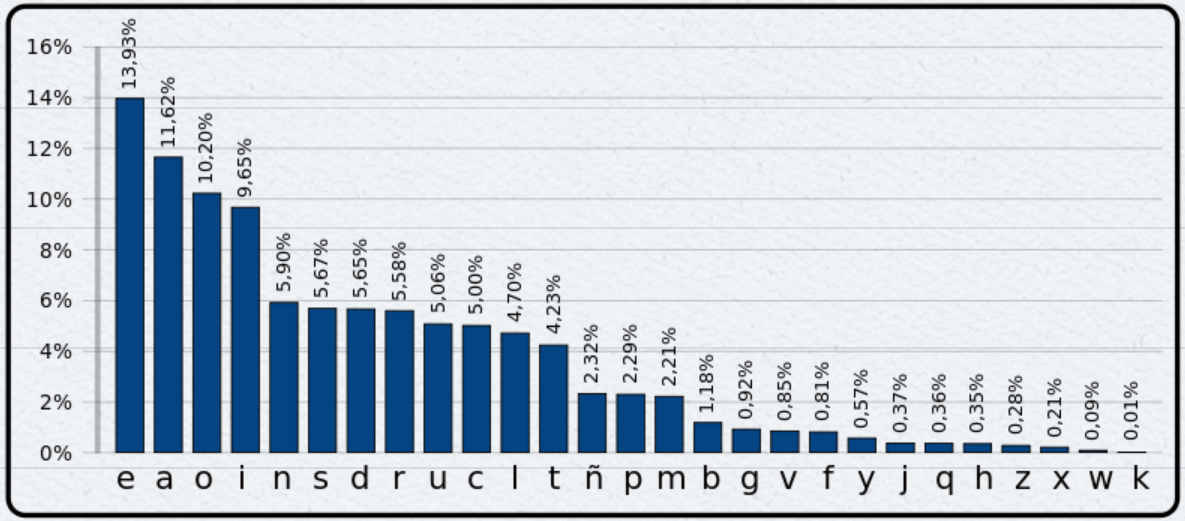
A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z

- ¿Cuántas claves posibles habría?
- ¿Se puede atacar este esquema de cifrado?

Análisis de frecuencias

- Este es uno de los métodos que se utilizan para criptoanalizar.
- Consiste en comparar las frecuencias de los caracteres en el texto cifrado con las frecuencias de las letras en el castellano.
- Si para cifrar se realizan sustituciones de un carácter por otro, estas frecuencias nos permitirán asociar los caracteres del mensaje con los del texto cifrado.

Frecuencias de letras en castellano



Digramas más frecuentes en castellano

- EL
- DE
- EN
- LA
- ES

Análisis de frecuencias

- Se basa en analizar las frecuencias de los caracteres en el texto cifrado y asociar caracteres del texto en claro con ellos.
- Por ejemplo, la letra más repetida es muy probable que corresponda a la letra E, aunque también podría corresponder a la letra A.
- A veces, se necesita intentar el criptoanalisis con varias combinaciones o analizar tambien digramas o trigramas.
- Observa que para este criptoanálisis, el tamaño del espacio de clave no importa.

Métodos de transposición

- Sustituir un símbolo por otro, hace que se pueda atacar el esquema de cifrado por análisis de frecuencias.

- ¿Qué otros métodos se utilizaban en la antigüedad para cifrar?

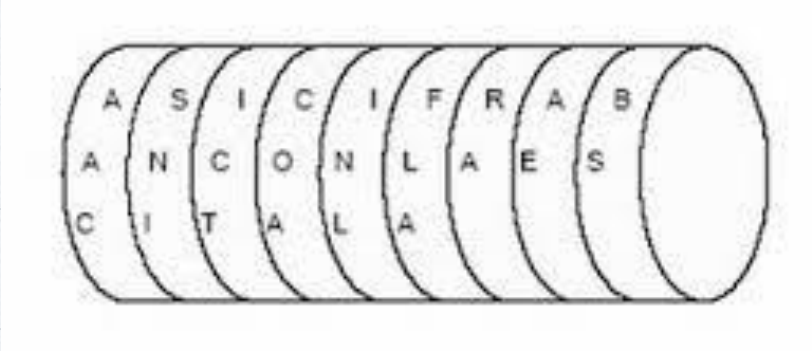
- Otra posibilidad era reordenar los símbolos del mensaje. Esto es lo que se conoce por transposición.

Escitala

- En la antigua Grecia, los espartanos usaban este método para cifrar mensajes.
- Con este método en lugar de sustituir un símbolo por otro (sustitución), se descolocan las letras del mensaje (trasposición).
- Consistía en dos cilindros similares, uno para el emisor y otro para el receptor y una tira de cuero o papiro.
- El emisor enrollaba la tira alrededor del cilindro y escribía el mensaje a lo largo del tubo.
- Al desenrollar la tira, se tiene el mensaje cifrado, que se enviaba al receptor.
- Para descifrarlo, el receptor enrollaba de nuevo la tira alrededor del cilindro gemelo, y así podía leer el mensaje original.
- ¿Cuál es la clave secreta en este caso?

Escitala

Ejemplo



AACSNIICTCOAINLFLARAAEBS

Criptoanálisis

- ¿Cómo podríamos descifrar un texto escrito con escitala si no conocemos el radio del cilindro?

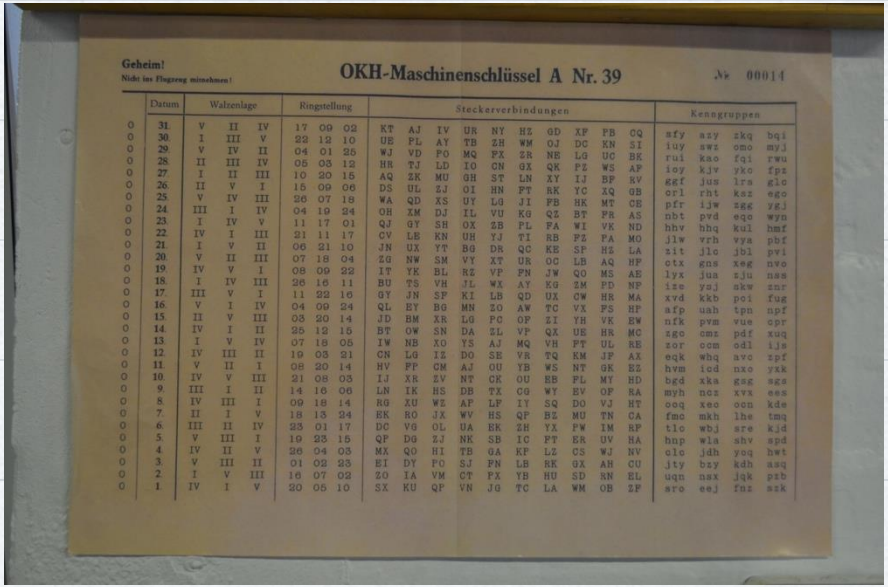
Máquina Enigma

- La criptografía tuvo un papel muy importante en la Segunda Guerra Mundial.
- Los alemanes utilizaban máquinas de rotores, llamadas Enigma, que permitían cifrar de forma mecánica y rápida.
- Los británicos, entre ellos, Alan Turing, consiguieron romper el esquema, construyendo la Máquina Bombe.
- Gracias a esto, la guerra acabó mucho antes, salvándose muchas vidas.

Máquina Enigma

- Se trataba de un cifrado de sustitución.
- El número posible de claves era muy grande: se podía elegir entre varios rotores, y varias posiciones de cada uno de ellos: había unas 158.000.000.000.000.000.000 posibilidades.
- La máquina Bombe que se usó para romperla, iba descartando las posibilidades, una vez se iban haciendo conclusiones a partir del texto cifrado.

Claves



Geheim!
Nicht ins Flugzeug mitnehmen!

OKH-Maschinenschlüssel A Nr. 39

№ 00014

	Datum	Walzenlage			Ringstellung			Steckerverbindungen										Kenngruppen			
0	31.	V	II	IV	17	09	02	KT	AJ	IV	UR	NY	HZ	GD	XF	PB	GQ	xfy	aay	zkq	bqi
0	30.	I	III	V	22	12	10	UE	PL	AY	TB	ZH	WM	OJ	DC	KN	SI	iuy	awz	omo	myj
0	29.	V	IV	II	04	01	25	WJ	VD	PO	MQ	FX	ZR	NE	LG	UC	BK	rui	kao	fqi	rwu
0	28.	II	III	IV	05	03	12	HH	TJ	LD	IO	CN	GX	QK	FZ	WS	AF	ioy	kjv	yko	fpz
0	27.	I	II	III	10	20	15	AQ	ZK	MU	GH	ST	LN	XY	IJ	BP	RV	ggf	jus	lrs	glc
0	26.	II	V	I	15	09	06	DS	UL	ZJ	OI	HN	FT	RK	YC	XQ	GB	orl	rht	kaz	ego
0	25.	V	IV	III	26	07	18	WA	QD	XS	UY	LG	JI	PB	HK	MT	CE	pfr	ijw	sgg	ygj
0	24.	III	I	IV	04	19	24	OH	XM	DJ	IL	VU	KG	QZ	BT	PR	AS	nbt	pvd	eqo	wyn
0	23.	I	IV	V	11	17	01	QJ	GY	SH	OX	ZB	PL	FA	WI	VK	ND	hhv	hhq	kul	hmf
0	22.	IV	I	III	21	11	17	CV	LE	KN	UH	YJ	TI	RB	FZ	FA	MO	jlw	vrh	vya	pbf
0	21.	I	V	II	06	21	10	JN	UX	YT	BG	DR	QC	KE	SP	HZ	LA	zlt	jlc	jbl	pvi
0	20.	V	II	III	07	18	04	ZG	NW	SM	VY	XT	UR	OC	LB	AQ	HF	otx	gns	xeg	nvo
0	19.	IV	V	I	08	09	22	IT	YK	BL	RZ	VP	FN	JW	QO	MS	AE	lyx	jus	zju	nas
0	18.	I	IV	III	26	16	11	BU	TS	VH	JL	WX	AY	KG	ZM	PD	NF	ize	ysj	skw	znr
0	17.	III	V	I	11	22	16	GY	JN	SP	KI	LB	QD	UX	CW	HR	MA	xvd	kkb	poi	fug
0	16.	V	I	IV	04	09	24	QL	EY	BG	MN	ZO	AW	TC	VX	PS	HF	afp	uah	tpn	npf
0	15.	II	V	III	03	20	14	JD	BM	XR	LG	FC	OP	ZI	YH	VK	EW	nfk	pvm	vue	cpr
0	14.	IV	I	II	25	12	15	BT	OW	SN	DA	ZL	VP	QX	UE	HR	MC	zgo	cmz	pdf	xuq
0	13.	I	V	IV	07	18	05	IW	NB	XO	YS	AJ	MQ	VH	FT	UL	KE	zor	ccm	odl	ijs
0	12.	IV	III	II	19	03	21	CN	LG	IZ	DO	SE	VR	TQ	KM	JF	AX	eqk	whq	avc	zpf
0	11.	V	II	I	08	20	14	HV	FP	CM	AJ	OU	YB	WS	NT	GK	EZ	hvm	icd	nxo	yxk
0	10.	IV	V	III	21	08	03	IJ	XR	ZV	NT	CK	OU	EB	FL	MY	HD	bgd	xka	gsg	sgs
0	9.	III	I	II	14	16	06	LN	IK	HS	DB	TX	CG	WY	EV	OF	RA	myh	ncz	xvx	ees
0	8.	IV	III	I	09	18	14	RG	XU	WE	AF	LF	IY	SQ	DO	VJ	HT	ooq	xeo	ocn	kde
0	7.	II	I	V	18	15	24	EK	RO	JX	WV	HS	QF	BZ	MU	TN	CA	fmo	mkh	lhe	tmq
0	6.	III	II	IV	23	01	17	DC	VG	OL	UA	BK	ZH	YX	FW	IM	RF	tlc	wbj	sre	kjd
0	5.	V	III	I	19	23	15	QF	DG	ZJ	NK	SB	IC	FT	ER	UV	HA	hnp	wla	shv	spd
0	4.	IV	II	V	26	04	03	MX	QO	HI	TB	GA	KF	LZ	CS	WJ	NV	clo	jdh	yoq	hwt
0	3.	V	III	II	01	02	23	EI	DY	PO	SJ	FN	LB	RK	GX	AH	CU	jty	bzy	kdh	asq
0	2.	I	V	III	16	07	02	ZO	IA	VM	CT	FX	YB	HU	SD	SN	EL	uqn	nsx	jqk	ptb
0	1.	IV	I	V	20	05	10	SX	KU	QF	VN	JG	TC	LA	WM	OB	ZF	sro	eej	fnz	szk

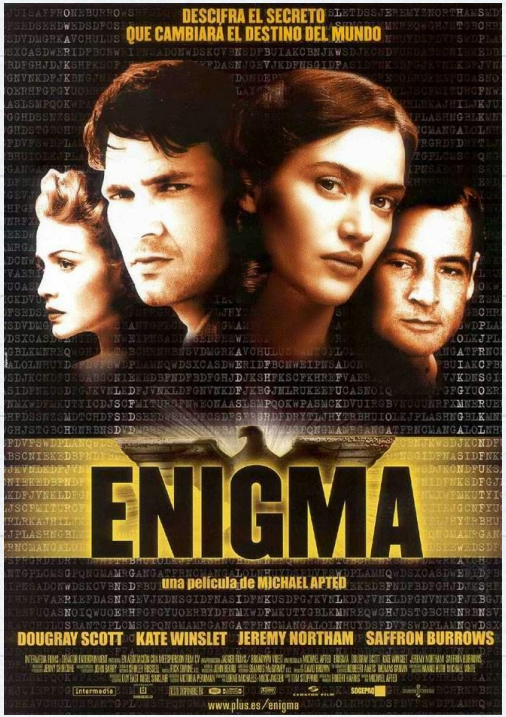
- ✗ Las claves se distribuían con la fecha en que debían usarse.
- ✗ Cada noche se cambiaba la configuración.

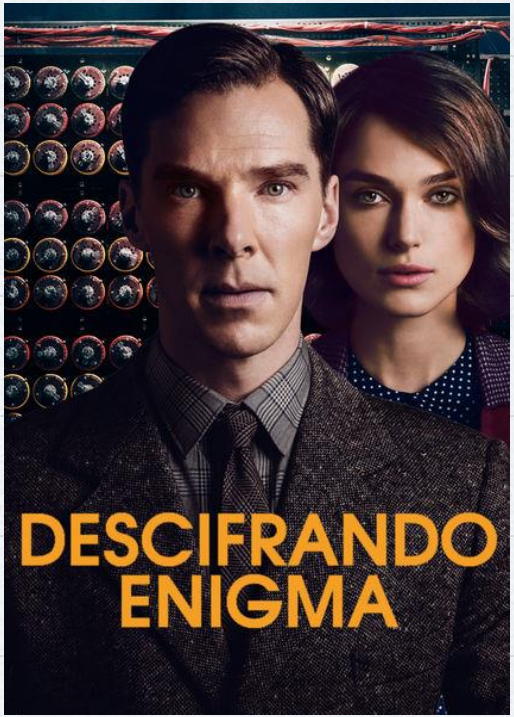
Bletchley Park

Las mujeres de Bletchley Park

- Más de 8.000 personas que trabajaron allí como descifradoras. Más de 6.000 eran mujeres
- Entre ellas estaban Joan Clarke, Margaret Rock, Ruth Briggs o Mavis Batey

Enigma en el cine





Y las mujeres que ayudaron a romperla

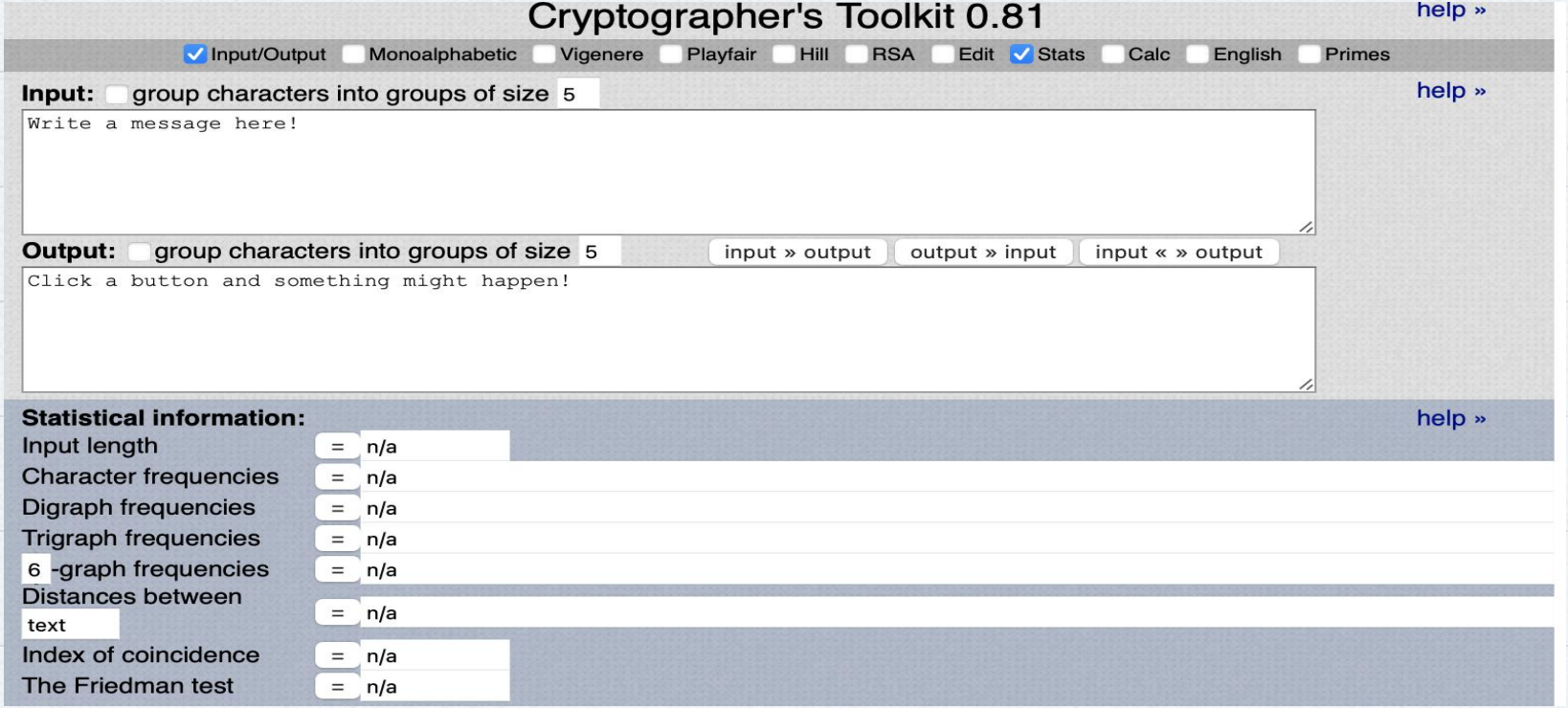
Ahora vamos a romper códigos…

Cuenta de gmail:

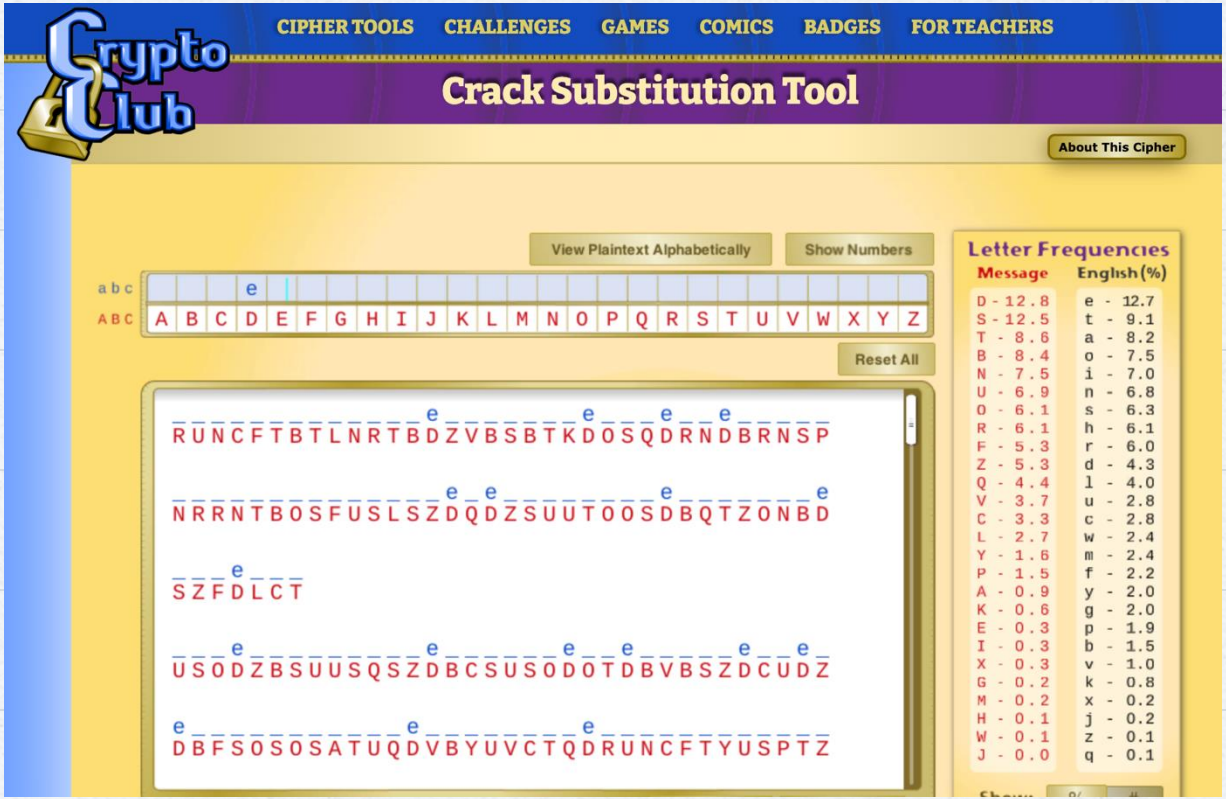
- tallerescriptografia@gmail.com
- Contraseña: TalleresCriptografia2024

- https://www.cs.du.edu/~petr/cryptographers_toolkit/cryptographers_toolkit.html
- https://www.cryptoclub.org

Ahora vamos a romper códigos...



Ahora vamos a romper códigos...



Problema de la criptografía

- En los esquemas que hemos visto, las personas que quieren comunicarse deben ponerse de acuerdo en una clave común: el número de posiciones que hay que mover, o el diámetro de la escitala…
- Esta clave se usa tanto para cifrar como para descifrar.
- Si el adversario consigue la clave, puede descifrar el texto cifrado y recuperar el mensaje.
- Si los usuarios pueden encontrarse en persona, podrían comunicarse la clave de forma confidencial, pero…¿ en el mundo digital en el que podemos estar unos muy lejos de otros? ¿cómo pueden ponerse de acuerdo en esa clave común?

Intercambio de claves

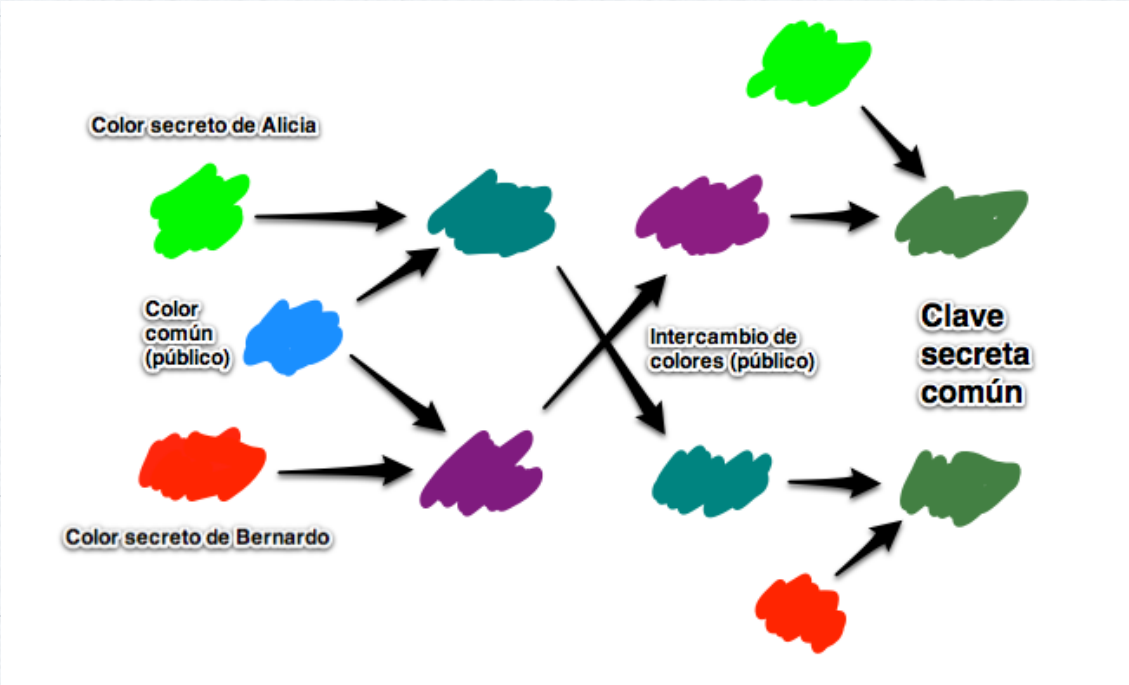
- Diffie y Hellman revolucionaron el mundo de la criptografía al proponer una forma de intercambiarse claves de forma segura sin necesidad de encontrarse en persona.

- El emisor (Alicia) y el receptor (Bernardo), se envían mensajes que todo el mundo puede leer, pero al final solo ellos dos podrán calcular una clave común.

Intercambio de claves

- Diffie y Hellman se dieron cuenta de la asimetría que hay en el mundo:
  - Un candado se puede cerrar fácilmente sin llave, pero no puede abrirse.
  - Se puede romper un jarron fácilmente, pero no es tan fácil reconstruirlo.
- Lo mismo ocurre con algunas operaciones matemáticas:
  - Es fácil elevar números a un exponent usando la aritmética del reloj, pero no es fácil, si conocemos la base y el resultado, hallar el exponente.
  - Es fácil realizar el producto de dos primos, pero es difícil, dado un número, encontrar sus factores primos.
- Este tipo de operaciones son las que vamos a usar en criptografía de cláve pública, se llaman funciones trampa.

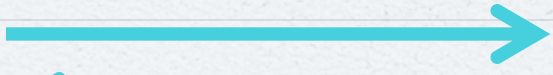
Intercambio de claves



Diffie-Hellman

Se elige un primo p, que es público

A



B

Elige a, entero aleatorio menor que p, secreto

$$A = g^a mod\ p$$

Elige b, entero aleatorio menor que p,secreto

$$B = g^b mod\ p$$

Diffie-Hellman

¡¡¡Han conseguido una Clave común!!!

A

B

Elige a, entero aleatorio menor que p, secreto

Elige b, entero aleatorio menor que p,secreto

$$K = B^a = g^{ab} = A^b = K$$

Ejemplo

- Alice y Bob acuerdan usar el número primo p=23 y la base g=5.
- Alice elige un número secreto a=6, luego envía a Bob (g^a mod p)
  - 5^6 mod 23 = 8.
- Bob elige un número secreto b=15, luego envía a Alice (g^b mod p)
  - 5^{15} mod 23 = 19.
- Alice calcula (g^b mod p)^a mod p
  - 19^6 mod 23 = 2.
- Bob calcula (g^a mod p)^b mod p
  - 8^{15} mod 23 = 2.

Mujeres criptógrafas

- Fue la primera criptógrafa americana
- Ayudo a capturar a contrabandistas y mafiosos en los años de la Ley Seca
- Descifró mensajes de espías Nazis, ayudando a ganar la Batalla del Atlántico
- El director del FBI, Hoover, se llevó todo el mérito.

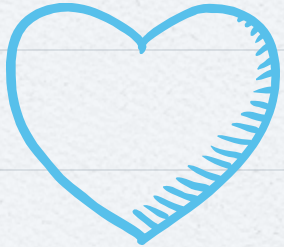
Elizebeth Friedman

Mujeres criptógrafas actuales

SOCIEDAD

La Fundación BBVA premia a los matemáticos investigadores de la criptografía moderna

En la imagen y de izquierda a derecha: Adi Shamir; Ronald Rivest; Shafi Goldwasser y Silvio Micali.



¡GRACIAS!

¿Alguna pregunta?

asuac@unileon.es