Taller de Criptografía, 2014
Semana de la Ciencia y la Tecnología en el CSIC

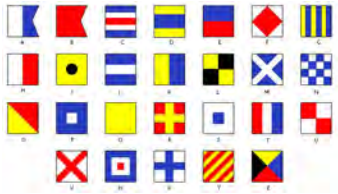
Luis Hernández Encinas
Agustín Martín Muñoz

Instituto de Tecnologías Físicas y de la Información (ITEFI)
Consejo Superior de Investigaciones Científicas, Madrid, España, 2014

{luis, agustin}@iec.csic.es
http://www.itefi.csic.es/es/personal/hernandez-encinas-luis
http://www.itefi.csic.es/es/personal/martin-munoz-agustin

Índice

Un mensaje codificado es una colección de símbolos que son conocidos por una comunidad y no tiene como fin ser secreto.



A: ·−	B: −···	C: −·−·
D: −··	E: ·	F: ··−·
G: −−·	H: ····	I: ··
J: ·−−−	K: −·−	L: ·−··
M: −−	N: −·	O: −−−

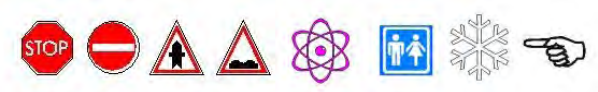


Figura: Códigos con banderas, código Morse y códigos informativos

Figura: Códigos de barras y bidimensionales (EAN13, QR y PDF417)

Figura: Códigos correctores de errores

Todos los códigos se pueden aprender (hasta los más difíciles).

Figura: Escritura jeroglífica y piedra Rosetta

Esteganografía: Técnicas que permiten ocultar la existencia un mensaje secreto.

- Rasurar la cabeza (Heródoto).
- Esconder un mensaje dentro de un huevo cocido (Giovanni Battista della Porta).
- Microfilmes como micropuntos en el · de la letra ı, o en signos de puntuación (Segunda guerra mundial).
- Tintas invisibles, legibles por calentamiento o por reacciones químicas.
- Técnicas digitales para ocultar la información dentro de archivos multimedia (billetes, dibujos, audio, video, sonido) como marcas de agua (watermarking).

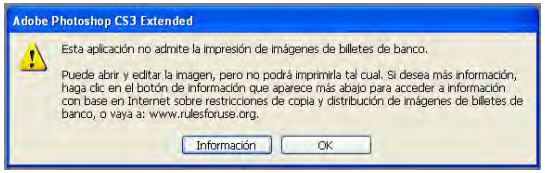


Figura: Protección de billetes contra fotocopia y falsificación

Un mensaje secreto es un mensaje transformado de modo que nadie, salvo quien esté autorizado, puede conocer su contenido.

- Cambiando el lugar que ocupan las letras del mensaje (transposición):

  SEMANA DE LA CIENCIA ↦ ACADEMIA SIN ENLACE

- Cambiando unas letras por otras o por símbolos (sustitución):

  Informacion ↦ Kwbpjqozkpw, Instituto ↦ ¶#♣§¶§‡§♢

- Transformando el mensaje a números y operando con estos números (cifrado):

  ESPAÑA ↦ 125874570954

Criptología: Del griego *kryptos* (secreto) y *logos* (ciencia).

Criptografía: Permitir que dos personas puedan intercambiarse mensajes de forma segura utilizando canales inseguros.

Se utilizan claves y algoritmos para cifrar/descifrar mensajes.

Criptoanálisis: Romper las comunicaciones criptográficas.

Localizar las claves de cifrado o resolver el algoritmo utilizado.

Criptografía + Criptoanálisis = Criptología

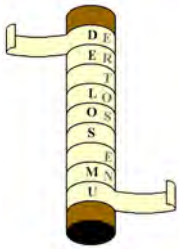
Figura: Proceso de cifrado y descifrado

Grecia

Escítala de Esparta (s. V a.C.): Vara alrededor de la cual se enrolla una tira de pergamino.

El mensaje se escribe a lo largo de la vara —de arriba a abajo— y se envía al destinatario. El mensaje se lee colocando la tira de pergamino alrededor de una vara idéntica.

DE LOS MUERTOS EN LAS
TERMÓPILAS ES
GLORIOSA LA SUERTE



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

DELPGLERAILA TSLO LO ARSOSTSIUS E OE ERESRMNMSATU O E

Roma

Julio César: Cambiar cada letra por la tercera siguiente (A ↦ D).

V	E	N	I		V	I	D	I		V	I	N	C	I
Y	H	Q	L		Y	L	G	L		Y	L	Q	F	L

Octavio Augusto: Cambiar cada letra por la siguiente (A ↦ B).

N	O		T	E		F	I	E	S		D	E		P	O	M	P	E	Y	O
O	P		U	F		G	J	F	T		E	F		Q	P	N	Q	F	Z	P

De tipo César: Cambiar:

- Cada letra por la n-ésima siguiente o la n-ésima anterior.
- La 1ª letra por la 1ª siguiente, la 2ª por la 2ª siguiente, etc.
- Las que ocupan posiciones pares por la n-ésima siguiente y las impares por la n-ésima anterior, etc.

Atbash

En el antiguo Testamento se propone una técnica de cifrado conocida como Atbash.

En el Atbash, la primera letra, **a**leph, se convierte en la última, **t**aw; la segunda, **b**eth, en la penúltima, **sh**in; la tercera, **g**imel, en la antepenúltima, **r**esh; etc.

El proceso para cifrar y descifrar se puede llevar a cabo haciendo uso del siguiente cuadro:

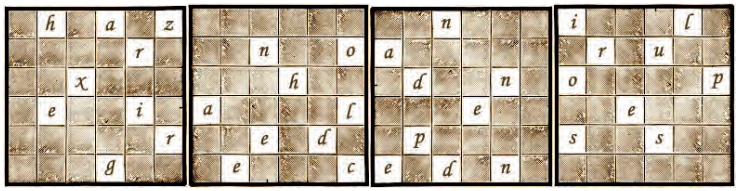
A	B	C	D	E	F	G	H	I	J	K	L	M
↕	↕	↕	↕	↕	↕	↕	↕	↕	↕	↕	↕	↕
Z	Y	X	W	V	U	T	S	R	Q	P	O	N

HVNZMZWVOZXRVMXRZ
SEMANADELACIENCIA

Rejillas de Verne

El mensaje cifrado (Mathias Sandorf de Julio Verne) es:

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



Cifrados por sustitución

5 3 ‡ † 3 0 5)) 6 * ; 4 8 2 6) 4 ‡ .) 4 ‡) ; 8 0 6 * ; 4 8 ‡ 8
¶ 6 0)) 8 5 ; 1 ‡ (; : ‡ * 8 † 8 3 (8 8) 5 * † ; 4 6 (; 8 8 * 9 6
* ? ; 8) * ‡ (; 4 8 5) ; 5 * † 2 : * ‡ (; 4 9 5 6 * 2 (5 * - 4) 8
¶ 8 * ; 4 0 6 9 2 8 5) ;) 6 † 8) 4 ‡ ‡ ; 1 (‡ 9 ; 4 8 0 8 1 ; 8 : 8 ‡
1 ; 4 8 † 8 5 ; 4) 4 8 5 † 5 2 8 8 0 6 * 8 1 (‡ 9 ; 4 8 ; (8 8 ; 4
(‡ ? 3 4 ; 4 8) 4 ‡ ; 1 6 1 ; : 1 8 8 ; ‡ ? ;

El escarabajo de oro, E.A. Poe.

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
5	2	-	†	8	1	3	4	6				0	9	*	‡	.		(	)	;	?	¶		:	

Homófonos y Nulos

Homófonos: Diferentes signos para representar la misma letra.

Nulos: Signos sin significado.

	1	2	3	4	5	6	7	8	9	0
1	i	p	i		o	u	o		p	n
2	w	e	u	t	e	k		l	o	
3	e	u	g	n	b	t	n		s	t
4	t	a	z	m	d		i	o	e	
5	s	v	t	j		e		y		h
6	n	a	o	l	n	s	u	g	o	e
7		c	b	a	f	r	s		i	r
8	i	c	w	y	r	u	a	m		n
9	m	v	t		h	p	d	i	x	q
0	l	s	r	e	t	d	e	a	h	e

Cuadro utilizado en las conversaciones telefónicas de Los Álamos (bomba atómica): cada letra se cifra con dos números.

Los sistemas anteriores no se consideran seguros.

1. Ataques pasivos: Se intenta obtener el mensaje original o la clave.
   - Ataques por fuerza bruta (exhaustivos) probando todas las posibles claves.
   - Ataques por máxima verosimilitud.
   - Ataques estadísticos basados en estudios de las frecuencias de las letras.
2. Ataques activos: Se intenta, además, modificar la información del mensaje original.

Leon Battista Alberti, Secretario de Claves del Vaticano (1402-1472), inventó los cifrados por rotación.

El Nomenclátor de Felipe II o *Cifra general* (1556) consta de una sustitución con homófonos, un silabario y un diccionario.

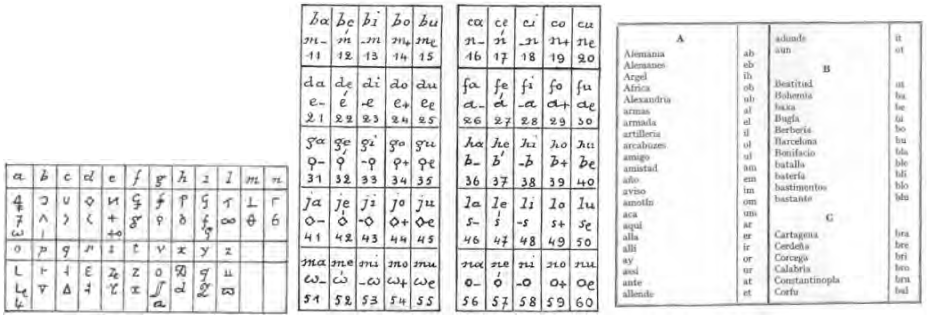


Figura: Abecedario, Silabario y Diccionario, de la *Cifra general*

Blaise de Vigenère publicó en 1586 el *Traicté des chiffres*, donde presenta la Chiffre indechiffrable.

Es un sistema polialfabético que utiliza como alfabetos de cifrado las 26 permutaciones circulares del alfabeto habitual.

Los alfabetos se utilizan de acuerdo con una clave previamente establecida entre el emisor y el receptor del mensaje.

Cifrado de *Acabo de llegar de Francia* con la clave BLAISE:

a c a b o d e l l e g a r d e f r a n c i a
B L A I S E B L A I S E B L A I S E B L A I

Así, la letra *a* se cifra con el alfabeto B, la letra *c* con el alfabeto L, la *a* con el A, etc. El texto cifrado resultante es:

BNAJG HFWLM YESOE NJEON II

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

Telegrama Zimmermann

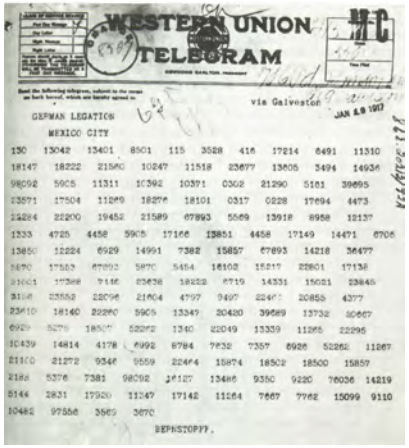


Figura: Telegrama de Arthur Zimmermann, 16 de Enero de 1917

Guerra civil española

Figura: Comunicados de la Guerra Civil Española

Máquinas Otros

Figura: Jefferson(1820) y Hagelin(1925)

Figura: Cryptex e Infiltración

Seducción

Figura: Seducción

Idiomas desconocidos

Figura: Wind Talkers

Máquina Enigma

Figura: Máquina Enigma

Bomba de Turing y Colossus

Nuevos principios

El atacante lo conoce "casi" todo.

Uso de técnicas computacionales.

Empleo de problemas matemáticos "difíciles" (intratables desde el punto de vista computacional).

1. Generar de números (pseudo)aleatorios.
2. Problema de la mochila (suma de un subconjunto).
3. Determinar números primos grandes ("fácil").
4. Factorizar números enteros grandes con pocos factores.
5. Calcular logaritmos discretos.
6. Calcular logaritmos elípticos.

Criptografía de clave secreta

Se utiliza la misma clave para cifrar que para descifrar (ejércitos, diplomáticos, gobiernos).

Cifrado en flujo (óptimo: cifrado de Vernam, 1917).

Data Encryption Standard: DES (1976) —TripleDES—. Bloques de 64 bits y claves de 64 bits —128 ó 192—.

International Data Encryption Algorithm: IDEA (1991). Bloques de 64 bits y claves de 128 bits.

Advanced Encryption Standard: AES (2000, Rijndael). Bloques y claves de longitud variable (128, 192 y 256 bits).

Criptografía de clave pública

Se utiliza diferente clave para cifrar mensajes que para descifrarlos (Internet, empresas, usuarios).

Criptosistemas de Mochila (Merkle-Hellman, 1976). Dificultad de resolver el problema de la mochila. Claves de 1024-2048 bits.

Criptosistema RSA (Rivest-Shamir-Adelman, 1978). Dificultad de factorizar números enteros. Claves de 1024-2048 bits.

Criptosistema de ElGamal (1985). Dificultad de calcular logaritmos discretos. Claves de 1024-2048 bits.

Criptosistemas de curvas elípticas e hiperelípticas (1986-1989). Dificultad de calcular logaritmos elípticos. Claves de 160-320 y 80-160 bits.

Problemas matemáticos "difíciles"

Primalidad: Decidir si un número grande dado es o no primo.

$a =$ 3512510886 9228775768 5546909064 4016491791 2238198248 0951709229 7572707870 9606576633 1683281246 129191,

$b =$ 2852005978 1207481410 9967592921 0535255327 9220575725 1,

$c =$ 1231273481 2348972184 9712347123 4123412341 234121111.

$$a = 29 \cdot 113 \cdot 659 \cdot 941^3 \cdot 1151 \cdot 2053^2 \cdot 2819 \cdot 3181 \cdot 3727^7 \cdot 4297^2 \cdot 5387 \cdot 7919^6 \cdot 18313.$$

b es primo.

$$c = 1867 \cdot 17107 \cdot 24523878278002301461 \cdot 1571980667373642599179.$$

Problemas matemáticos difíciles

Factorización: Calcular la descomposición de un número dado como producto de números primos elevados a potencias.

$$3630 = 10 \cdot 363 = 2 \cdot 5 \cdot 3 \cdot 121 = 2 \cdot 3 \cdot 5 \cdot 11^2.$$

RSA768 = 1230186684 5301177551 3049495838 4962720772 8535695953 3479219732 2452151726 4005072636 5751874520 2199786469 3899564749 4277406384 5925192557 3263034537 3154826850 7917026122 1429134616 7042921431 1602221240 4792747377 9408066535 1419597459 8569021434 13

= 3347807169 8956898786 0441698482 1269081770 4794983713 7685689124 3138898288 3793878002 2876147116 5253174308 7737814467 999489

× 3674604366 6799590428 2446337996 2795263227 9158164343 0876426760 3228381573 9666511279 2333734171 4339681027 0092798736 308917.

Problemas matemáticos difíciles

RSA2048 = 2519590847 5657893494 0271832400 4839857142
9282126204 0320277771 3783604366 2020707595 5562640185
2588078440 6918290641 2495150821 8929855914 9176184502
8084891200 7284499268 7392807287 7767359714 1834727026
1896375014 9718246911 6507761337 9859095700 0973304597
4880842840 1797429100 6424586918 1719511874 6121515172
6546322822 1686998754 9182422433 6372590851 4186546204
3576798423 3871847744 4792073993 4236584823 8242811981
6381501067 4810451660 3773060562 0161967625 6133844143
6038339044 1495263443 2190114657 5444541784 2402092461
6515723350 7787077498 1712577246 7962926386 3563732899
1215483143 8167899885 0404453640 2352738195 1378636564
3912120103 9712282212 0720357.

Problemas matemáticos difíciles

Logaritmo (discreto): Calcular la potencia a la que hay que elevar un número —base— para obtener otro número dado: $\log_a b = x$ porque $a^x = b$ (en conjuntos con un número finito de elementos).

$$\log_{10} 1000 = 3, \quad \log_{10} 346 = 2,539076098792776609774269153483,$$
$$\log_2 1024 = 10, \quad \ln 346 = 5,846438775057724256350732509 8992.$$

En el conjunto de los restos de 11 (módulo 11): $\{0, 1, \ldots, 10\}$:

$$\log_2 10 \equiv 5 \pmod{11}, 2^5 = 32 = 11 \cdot 2 + 10 \equiv 10 \pmod{11},$$
$$\log_3 269191591 \equiv 1000 \pmod{1234567891},$$
$$\log_5 34561 \equiv x \pmod{12345678910111213141516171819 67}.$$

Firma digital	Tarjetas de identificación y Pasaportes
Venta de secretos	Correo electrónico cifrado y firmado
Votación electrónica	Protección de software y hardware
Intercambio de secretos	Transacciones bancarias seguras
Juegos por teléfono	Identificación Amigo-Enemigo
Reparto de secretos	Acceso a páginas web seguras
Certificados digitales	Comercio electrónico seguro

DNIe

La principal diferencia del nuevo DNIe con respecto al anterior, al margen de las propias relacionadas con la seguridad física, es la inclusión de un chip con capacidades criptográficas.

Figura: Ejemplar de muestra del DNIe

Usos del DNIe y Certificados

Criptoanálisis

- Antes de 1996:
  Seguridad basada en la fortaleza matemática de los algoritmos criptográficos.

- En 1996:
  - Ataque por inducción de fallos contra el RSA CRT (Boneh, Demillo y Lipton).
  - Ataque por análisis temporal contra Diffie-Hellman, RSA, DSS, y otros sistemas (Kocher).

Ataques a las implementaciones físicas

Nuevas estrategias de ataque:

- Introducir sondas para la lectura directa de la información de los buses o de las memorias RAM y caché.
- Intentar *saltarse* las medidas de seguridad, por ejemplo evitando la ejecución de ciertas instrucciones.
- Intentar acceder a los secretos por vías alternativas, sin tratar de romper los algoritmos criptográficos.

Ejemplos de canales laterales

Vías a través de las cuales se puede obtener información:

- Tiempo de cálculo.
- Temperatura.
- Ruido (sonido).
- Consumo de potencia.
- Radiación electromagnética.

Preparación - Ingeniería inversa - Desencapsulado

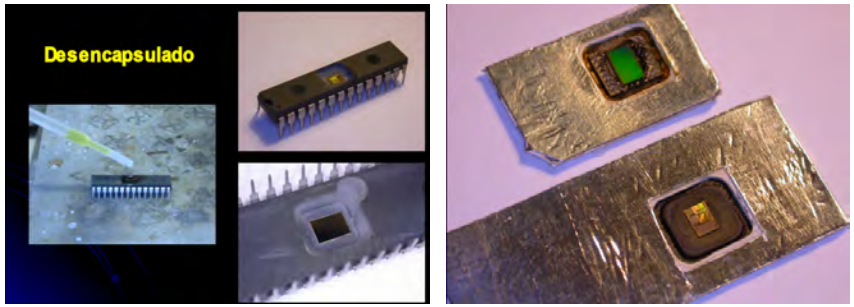


Figura: Acceso a las capas internas del chip

Preparación - Ingeniería inversa - Desencapsulado

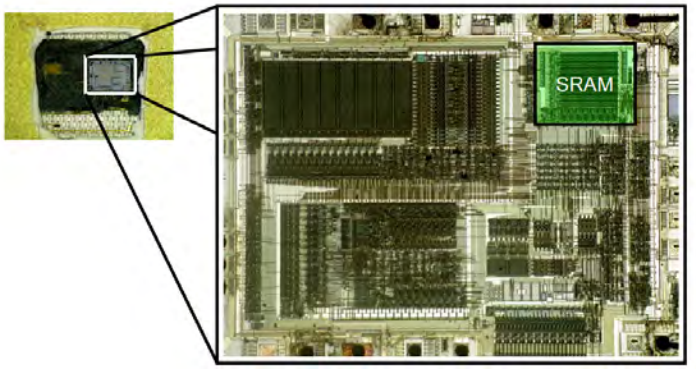


Figura: Identificación de las regiones sensibles

Preparación - Acceso a capas internas

Figura: Máquina de haces de iones focalizados (FIB)

Preparación - Acceso a capas internas

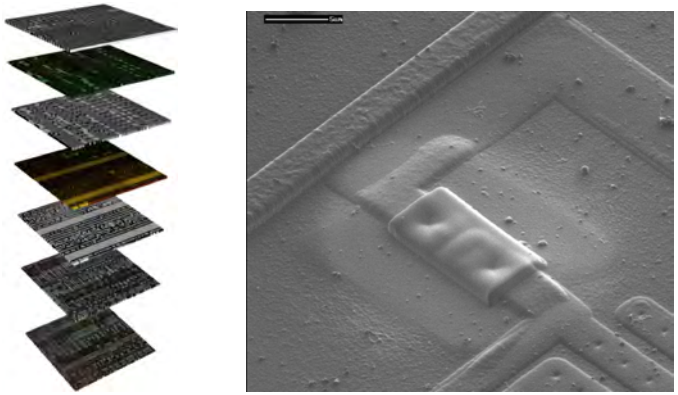


Figura: Reparación de pistas dañadas tras hacer microperforaciones

Ataques por sonda

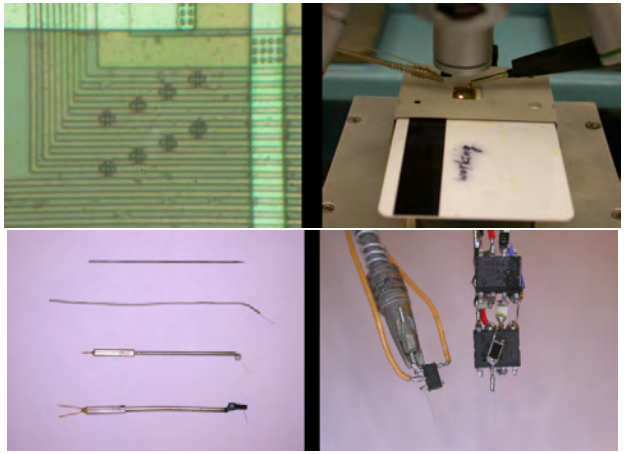


Figura: Acceso directo a señales en pistas y registros internos

Ataques por inducción de fallos

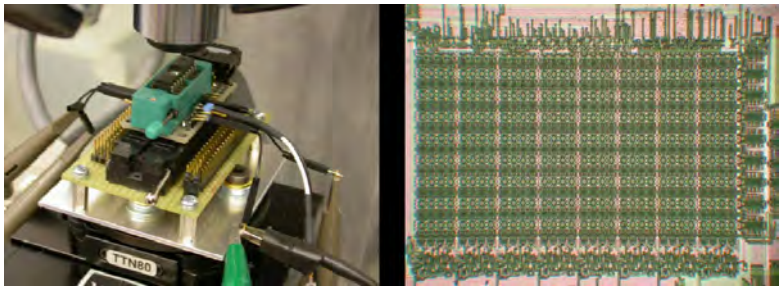


Figura: Disparo de luz láser contra el área de memoria del chip

Ataques por inducción de fallos

Figura: Modificación del estado de una celda de memoria

Análisis del consumo de potencia

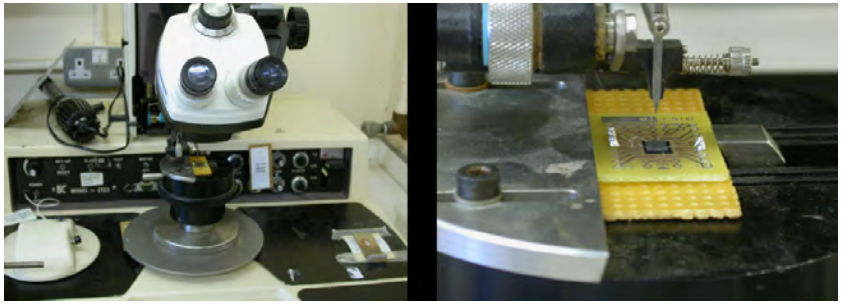


Figura: Cableado para medida del consumo de potencia del chip

Ataque por análisis de las emanaciones electromagnéticas (EMA)

Figura: Ataque EMA contra una tarjeta inteligente

Ataque EMA contra una tarjeta inteligente

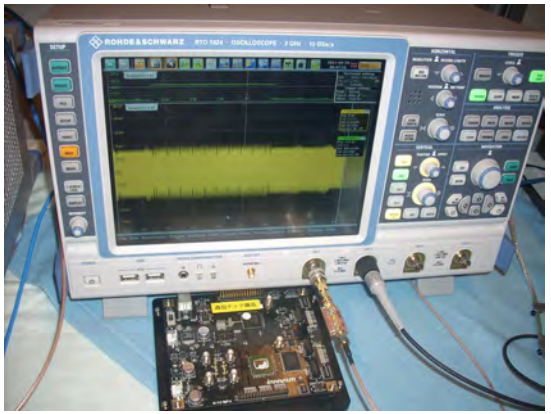


Figura: Señal medidas en un ataque EMA

Análisis simple de potencia (SPA, *Simple Power Analysis*)

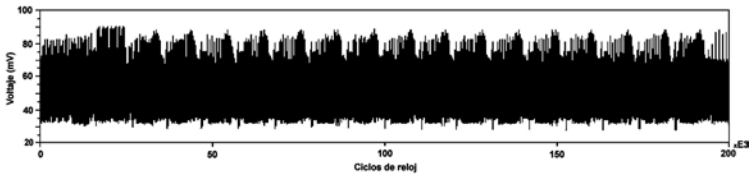


Figura: Consumo de potencia durante el cálculo de un DES

Análisis simple de potencia (SPA, *Simple Power Analysis*)

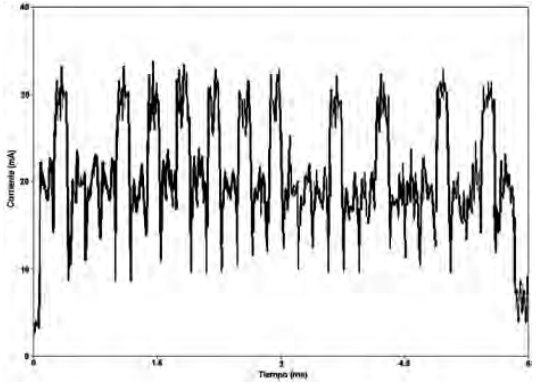


Figura: Consumo de potencia durante el cálculo de un RSA

Análisis SPA de un RSA sin contramedidas

Exponenciación modular: $y = x^k \pmod{n}$.

La clave en binario: $k = (k_{r-1} \dots k_0)$. Ejemplo: $23 = 10111$

Algoritmo de elevar al cuadrado y multiplicar, procesando los bits de izquierda a derecha:

1. $y = 1$.
2. For $i = (r-1)$ to 0 do:
   1. $y = y^2 \pmod{n}$.
   2. If $(k_i = 1)$ then $y = (y \cdot x) \pmod{n}$.
3. Return (y).

Ejemplo: $a^{23} = (((a^2)^2 a)^2 a)^2 a$.

Ataques por canales laterales

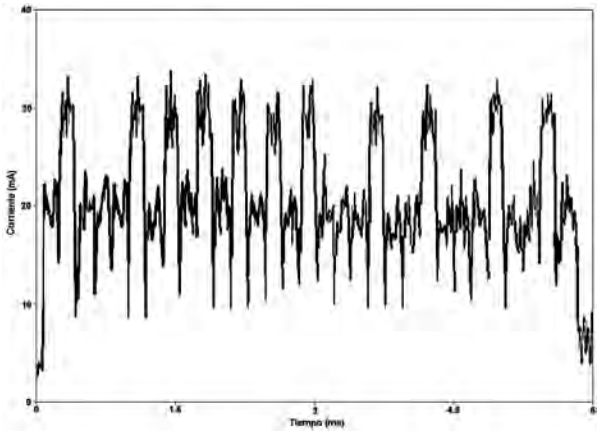


Figura: Consumo de potencia durante el cálculo de un RSA

Ataques por canales laterales

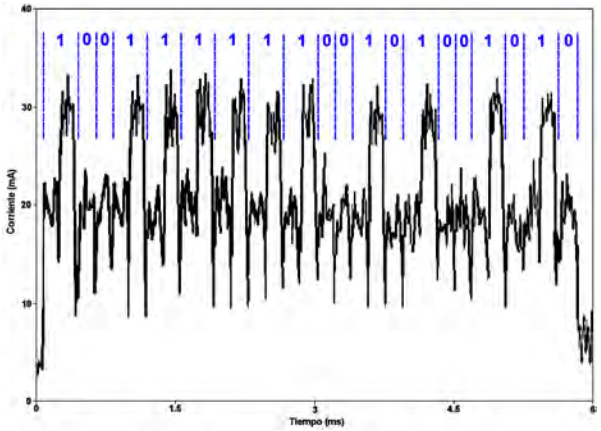
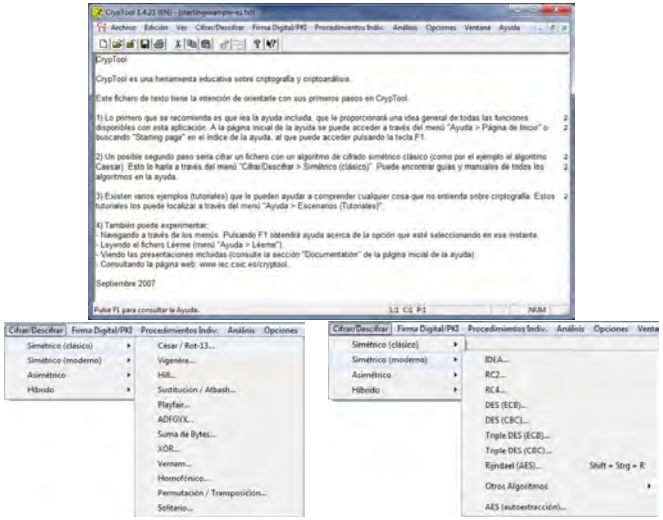


Figura: La clave es $k = 653642$

Cryptool

http://www.cryptool.com/index.php/es.html



- P. Caballero Gil, *Introducción a la Criptografía*, 2ª ed., RA-MA, Madrid, 2002.
- R. Durán Díaz, L. Hernández Encinas y J. Muñoz Masqué, *El criptosistema RSA*, RA-MA, Madrid, 2005.
- A. Fúster Sabater, L. Hernández Encinas, A. Martín Muñoz, F. Montoya Vitini y J. Muñoz Masqué, *Criptografía, protección de datos y apliaciones. Guía para estudiantes y profesionales*, RA-MA, Madrid, 2012.
- A. Menezes, P. van Oorschot, S. Vanstone, *Handbook of applied cryptography*, CRC Press, Boca Raton, FL, 1997. `www.cacr.math.uwaterloo.ca/hac`
- E.A. Poe, *Cuentos*, traducción de J. Cortázar, Alianza, Madrid, 2003.
- J. Verne, *Matias Sandorf*, RBA, Barcelona, 1984.
- S. Singh, *Los códigos secretos*, Debate, Barcelona, 2000. `http://simonsingh.net`
- A. Sgarro, *Códigos secretos*, Pirámide, Madrid, 1990.
- Criptonomicon, `http://www.iec.csic.es/criptonomicon/default2.html`
- Kriptópolis, `http://www.kriptopolis.org`

Muchas gracias

¿Preguntas?

Formulario de evaluación y encuesta:

`http://www.semanadelaciencia.csic.es/`

Pincha en: “Queremos saber tu opinión”