El sistema RSA

Federico Cantero Morán

Universidad Autónoma de Madrid

Código César

Cuando el César quería enviar un mensaje a sus centuriones en las Galias, les daba primero un número entre 1 y 27 (la **clave**), y después desplazaba cada letra del mensaje ese número de veces:

$$\textit{Asterix} \longmapsto \textit{Cuvgtkz}, \text{ si la clave es 2.}$$

y enviaba el mensaje *Cuvgtkz* con un mensajero que recorría la Galia a caballo.

Código César

Cuando el César quería enviar un mensaje a sus centuriones en las Galias, les daba primero un número entre 1 y 27 (la **clave**), y después desplazaba cada letra del mensaje ese número de veces:

$$\textit{Asterix} \longmapsto \textit{Cuvgtkz}, \text{ si la clave es 2.}$$

y enviaba el mensaje *Cuvgtkz* con un mensajero que recorría la Galia a caballo.

Para que este sistema funcione,

- César tiene que cambiar de clave a menudo, para que a los galos no les de tiempo a descubrirla por sí mismos.
- César tiene que transmitir su clave al centurión, por ejemplo con un mensajero.

PROBLEMA: **¿Cómo puede transmitir Julio César la clave al centurión sin que los galos la intercepten?**.

Código César

Cuando el César quería enviar un mensaje a sus centuriones en las Galias, les daba primero un número entre 1 y 27 (la **clave**), y después desplazaba cada letra del mensaje ese número de veces:

$$\textit{Asterix} \longmapsto \textit{Cuvgtkz}, \text{ si la clave es 2.}$$

y enviaba el mensaje *Cuvgtkz* con un mensajero que recorría la Galia a caballo.

Para que este sistema funcione,

- César tiene que cambiar de clave a menudo, para que a los galos no les de tiempo a descubrirla por sí mismos.
- César tiene que transmitir su clave al centurión, por ejemplo con un mensajero.

PROBLEMA: **¿Cómo puede transmitir Julio César la clave al centurión sin que los galos la intercepten?**.

La solución a este problema son los **sistemas de clave pública** (descubiertos en los '70). Son los que permiten que hoy en día el comercio electrónico, la privacidad en whatsapp, las firmas electrónicas etc.

Máquina Enigma

Durante la II guerra mundial, el ejército alemán usó un sistema de codificación llamado “ENIGMA”.

Tanto Hitler como cada uno de sus generales tenían una máquina “ENIGMA” y un libro de claves. Para enviar o recibir un mensaje hacía falta tener tanto la máquina como el libro. El libro se renovaba cada mes.

Geheime Kommandosache! Jede einzelne Tagesschlüssel ist geheim. Mitn[illegible] im Flugzeug verboten!

Nr. 00190

Luftwaffen-Maschinen-Schlüssel Nr. 649

Achtung! Schlüsselmittel dürfen nicht unversehrt in Feindeshand fallen. Bei Gefahr restlos und frühzeitig vernichten.

	Monatstag	Walzenlage			Ringstellung			Steckerverbindungen an der Umkehrwalze				Steckerverbindungen am Steckerbrett 1	2	3	4	5	6	7	8	9	10	Kenngruppen			
649	31	I	V	III	14	09	24					SZ	GT	DV	KU	FO	MY	EW	JN	IX	LQ	wny	dgy	ekb	rzg
649	30	IV	III	II	05	26	02					IS	EV	MX	RW	DT	UZ	JQ	AO	CH	NY	ktl	acw	zsi	wao
649	29	III	II	I	12	24	03	KM	AX	PZ	GO	DJ	AT	CV	IO	ER	QS	LW	PZ	FN	BH	ioc	acn	ovw	wvd
649	28	II	III	V	06	08	16	DI	CN	BR	PV	CR	FV	AI	DK	OT	MQ	EU	BX	LP	GJ	lrb	cld	ude	rzh
649	27	III	I	IV	11	03	07	LT	EQ	HS	UW	DY	IN	BV	GR	AM	LO	PP	HT	EX	UW	woj	fbh	vct	uis
649	26	I	IV	V	17	22	19					VZ	AL	RT	KO	CO	EI	BJ	DU	FS	HP	xle	gbo	uev	rxm
649	25	IV	III	I	08	25	12					OR	PV	AD	IT	PK	HJ	LZ	NS	EQ	CW	ouc	uhq	uew	uit
649	24	V	I	IV	05	18	14					TY	AS	OW	KV	JM	DR	HX	GL	CZ	NU	kpl	rwl	vci	tlq
649	23	IV	II	I	24	12	04					QV	FR	AK	EO	DH	CJ	MZ	SX	GN	LT	ebn	rwm	udf	tlo
649	22	II	IV	V	01	09	21	IU	AS	DV	GL	FJ	ES	IM	RX	LV	AY	OU	BG	WZ	CN	jqc	acx	mwe	wve
649	21	I	V	II	13	05	19	PT	OX	EZ	CH	RU	HL	PY	OS	GZ	DM	AW	CE	TV	NX	jpw	del	mwf	wvf
649	20	III	IV	V	24	01	10	MR	KN	BQ	PW	DP	MO	QZ	AU	RY	SV	JL	GX	BE	TW	jqd	cef	nvo	ysh
649	19	V	III	I	17	25	20					OX	PR	FH	WY	DL	CM	AE	TZ	JS	GI	idf	fpx	jwg	tlg
649	18	IV	II	V	15	23	26					EJ	OY	IV	AQ	KW	FX	MT	PS	LU	BD	lsa	[illegible]bw	vcj	rxn
649	17	I	IV	II	21	10	06					IR	KZ	LS	EM	OV	GY	QX	AF	JP	BU	mae	hzi	sog	ysi
649	16	V	II	III	08	16	13					HM	JO	DI	NR	BY	XZ	GS	PU	FQ	CT	tdp	dhb	fkb	uiv
												DS	HY	MR	GW	LX	AJ	BQ	CO	IP	NT	ldw	hzj	soh	wvg

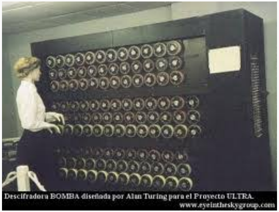
Máquina Enigma

Durante la II guerra mundial, el ejército alemán usó un sistema de codificación llamado "ENIGMA".

Tanto Hitler como cada uno de sus generales tenían una máquina "ENIGMA" y un libro de claves. Para enviar o recibir un mensaje hacía falta tener tanto la máquina como el libro. El libro se renovaba cada mes.

Hacia 1941, un grupo de criptógrafos ingleses y polacos liderados por Alan Turing consiguieron descifrar los mensajes alemanes usando máquinas "ENIGMA" sustraidas a los alemanes sin usar el libro de claves. Se cree que esto fue una de las razones principales de la derrota alemana.

El sistema "ENIGMA" era **simétrico**: tanto el codificado como el descodificado se hacía con la misma máquina y el mismo libro.

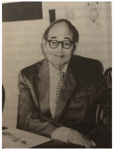


Sistemas de clave pública

Los sistemas de clave pública fueron inventados por Ellis '1970 (Inteligencia, Reino Unido) y por Merkle, Diffie, Hellmann (Stanford) '1979:

Sistemas de clave pública

Los sistemas de clave pública fueron inventados por Ellis '1970 (Inteligencia, Reino Unido) y por Merkle, Diffie, Hellmann (Stanford) '1979:



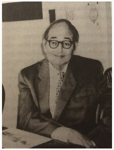
1. El centurión fabrica dos “claves”:
   - La **clave pública**, que **sólo** sirve para codificar el mensaje,
   - LA **clave privada**, que **sólo** sirve para descodificar el mensaje.

   Conocer una de las claves **no** *permite conocer la otra.*

2. El centurión envía la clave pública al César.

Sistemas de clave pública

Los sistemas de clave pública fueron inventados por Ellis '1970 (Inteligencia, Reino Unido) y por Merkle, Diffie, Hellmann (Stanford) '1979:



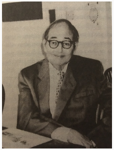
1. El centurión fabrica dos "claves":
   - La **clave pública**, que **sólo** sirve para codificar el mensaje,
   - LA **clave privada**, que **sólo** sirve para descodificar el mensaje.

   Conocer una de las claves **no** *permite conocer la otra.*

2. El centurión envía la clave pública al César.
3. César usa la clave pública para codificar su mensaje, y envía el mensaje codificado al centurión.

Sistemas de clave pública

Los sistemas de clave pública fueron inventados por Ellis '1970 (Inteligencia, Reino Unido) y por Merkle, Diffie, Hellmann (Stanford) '1979:



1. El centurión fabrica dos "claves":
   - La **clave pública**, que **sólo** sirve para codificar el mensaje,
   - LA **clave privada**, que **sólo** sirve para descodificar el mensaje.

   Conocer una de las claves **no** *permite conocer la otra.*

2. El centurión envía la clave pública al César.
3. César usa la clave pública para codificar su mensaje, y envía el mensaje codificado al centurión.
4. El centurión usa la clave privada para descodificar el mensaje codificado.

El intercambio de clave de Merkle,Diffie,Hellmann

Cómo César y el centurión pueden tener una clave secreta común:

$$
\begin{tikzcd}
{[a]\text{César}} \arrow[rr, bend left, "n^a \mod p"] & n, p & \text{centurión}[b] \arrow[ll, bend left, "n^b \mod p"]
\end{tikzcd}
$$

El intercambio de clave de Merkle,Diffie,Hellmann

Cómo César y el centurión pueden tener una clave secreta común:

$$\begin{tikzcd} {[a]}\text{César} \arrow[rr, bend left, "n^a \mod p"] & n, p & \text{centurión}[b] \arrow[ll, bend left, "n^b \mod p"] \end{tikzcd}$$

1. En primer lugar César y el centurión comparten (públicamente) un número primo p y otro número n (que ha de ser una raíz primitiva módulo p, por seguridad).

El intercambio de clave de Merkle,Diffie,Hellmann

Cómo César y el centurión pueden tener una clave secreta común:

$$\begin{tikzcd} {[a]\text{César}} \arrow[rr, bend left, "n^a \mod p"] & n, p & \text{centurión}[b] \arrow[ll, bend left, "n^b \mod p"] \end{tikzcd}$$

1. En primer lugar César y el centurión comparten (públicamente) un número primo p y otro número n (que ha de ser una raíz primitiva módulo p, por seguridad).
2. Después, César elige un número grande a y el centurión otro número grande b (secretamente).

El intercambio de clave de Merkle,Diffie,Hellmann

Cómo César y el centurión pueden tener una clave secreta común:

$$\begin{tikzcd}[a]\text{César} \arrow[rr, bend left, "n^a \mod p"] & n, p & \text{centurión}[b] \arrow[ll, bend left, "n^b \mod p"]\end{tikzcd}$$

1. En primer lugar César y el centurión comparten (públicamente) un número primo p y otro número n (que ha de ser una raíz primitiva módulo p, por seguridad).
2. Después, César elige un número grande a y el centurión otro número grande b (secretamente).
3. Después, César envía al centurión el número $n_a = n^a \mod p$ y el centurión envía a César el número $n_b = n^b \mod p$.

El intercambio de clave de Merkle,Diffie,Hellmann

Cómo César y el centurión pueden tener una clave secreta común:

$$\begin{tikzcd} {[a]\text{César}} \arrow[rr, bend left, "n^a \mod p"] & n, p & {\text{centurión}[b]} \arrow[ll, bend left, "n^b \mod p"] \end{tikzcd}$$

1. En primer lugar César y el centurión comparten (públicamente) un número primo p y otro número n (que ha de ser una raíz primitiva módulo p, por seguridad).
2. Después, César elige un número grande a y el centurión otro número grande b (secretamente).
3. Después, César envía al centurión el número $n_a = n^a \mod p$ y el centurión envía a César el número $n_b = n^b \mod p$.
4. Finalmente César y el centurión toman el número recibido y lo elevan a los números que habían elegido. Así el César obtiene $(n^b)^a \mod p$ y el centurión obtiene $(n^b)^a \mod p$. Ese número común será la clave.

Convertir un mensaje en un número

TABLA DE CARACTERES DEL CÓDIGO ASCII

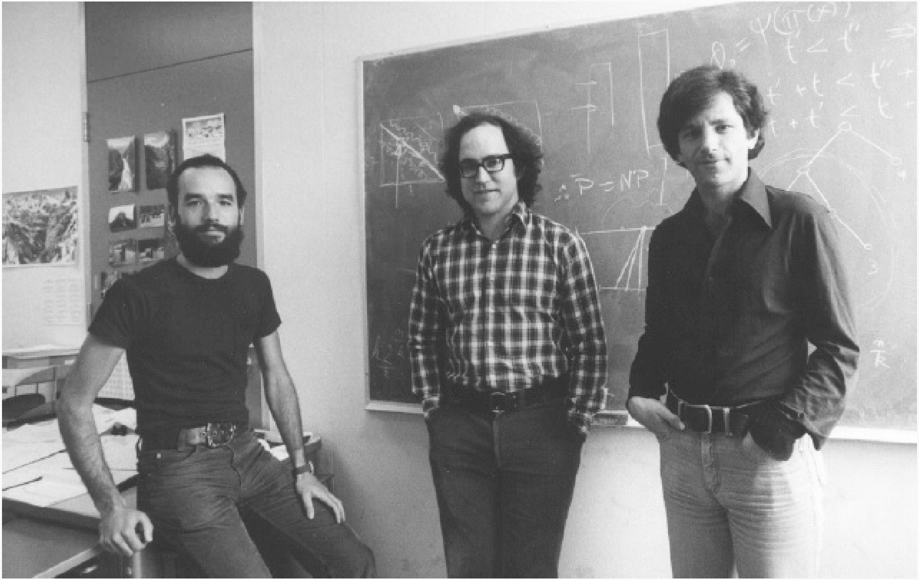
1	☺	25	↓	49	1	73	I	97	a	121	y	145	æ	169	⌐	193	┴	217	┘	241	±
2	☻	26		50	2	74	J	98	b	122	z	146	Æ	170	¬	194	┬	218	┌	242	≥
3	♥	27		51	3	75	K	99	c	123	{	147	ô	171	½	195	├	219	█	243	≤
4	♦	28	∟	52	4	76	L	100	d	124	|	148	ö	172	¼	196	─	220	▄	244	⌠
5	♣	29	↔	53	5	77	M	101	e	125	}	149	ò	173	¡	197	┼	221	▌	245	⌡
6	♠	30	▲	54	6	78	N	102	f	126	~	150	û	174	«	198	╞	222	▐	246	÷
7		31	▼	55	7	79	O	103	g	127	⌂	151	ù	175	»	199	╟	223	▀	247	≈
8		32		56	8	80	P	104	h	128	Ç	152	ÿ	176	░	200	╚	224	α	248	°
9		33	!	57	9	81	Q	105	i	129	ü	153	Ö	177	▒	201	╔	225	ß	249	∙
10		34	"	58	:	82	R	106	j	130	é	154	Ü	178	▓	202	╩	226	Γ	250	·
11		35	#	59	;	83	S	107	k	131	â	155	¢	179	│	203	╦	227	π	251	√
12		36	$	60	<	84	T	108	l	132	ä	156	£	180	┤	204	╠	228	Σ	252	^{n}
13		37	%	61	=	85	U	109	m	133	à	157	¥	181	╡	205	═	229	σ	253	^{2}
14		38	&	62	>	86	V	110	n	134	å	158	₧	182	╢	206	╬	230	µ	254	■
15		39	'	63	?	87	W	111	o	135	ç	159	ƒ	183	╖	207	╧	231	τ	255	
16	►	40	(	64	@	88	X	112	p	136	ê	160	á	184	╕	208	╨	232	Φ		
17		41	)	65	A	89	Y	113	q	137	ë	161	í	185	╣	209	╤	233	Θ		
18	↕	42	*	66	B	90	Z	114	r	138	è	162	ó	186	║	210	╥	234	Ω		
19	‼	43	+	67	C	91	[	115	s	139	ï	163	ú	187	╗	211	╙	235	δ		
20	¶	44	,	68	D	92	\	116	t	140	î	164	ñ	188	╝	212	╘	236	∞		
21	§	45	-	69	E	93	]	117	u	141	ì	165	Ñ	189	╜	213	╒	237	φ		
22	▬	46	.	70	F	94	^	118	v	142	Ä	166	ª	190	╛	214	╓	238	ε		
23	↨	47	/	71	G	95	_	119	w	143	Å	167	º	191	┐	215	╫	239	∩		
24	↑	48	0	72	H	96	`	120	x	144	É	168	¿	192	└	216	╪	240	≡		

PRESIONA LA TECLA Alt MÁS EL NÚMERO

CORTESÍA DE:

www.rey-dec.com

Shamir, Rivest y Adleman en 1978 (MIT)



El pequeño teorema de Fermat

Teorema (Fermat '1640, Euler'1736, Leibniz'1683)

Si N es un número primo y $0 < m < N$, entonces

$$m^{N-1} \equiv 1 \mod N.$$

El pequeño teorema de Fermat

Teorema (Fermat '1640, Euler'1736, Leibniz'1683)

Si N es un número primo y $m < N$, entonces

$$m^{N-1} \equiv 1 \mod N.$$

Corolario (Euler)

Si $N = p \cdot q$ es un producto de dos números primos que no dividen a m y $0 < m < N$,

$$m^{(p-1)\cdot(q-1)} \equiv 1 \mod N.$$

El pequeño teorema de Fermat

Teorema (Fermat '1640, Euler'1736, Leibniz'1683)

Si N es un número primo y $0 < m < N$, entonces

$$m^{N-1} \equiv 1 \quad \text{mod } N.$$

Corolario (Euler, Carmichael)

Si $N = p \cdot q$ es un producto de dos números primos que no dividen a m y $0 < m < N$,

$$m^{mcm(p-1,q-1)} \equiv 1 \quad \text{mod } N.$$

El pequeño teorema de Fermat

Teorema (Fermat '1640, Euler'1736, Leibniz'1683)

Si N es un número primo y $0 < m < N$, entonces

$$m^{N-1} \equiv 1 \mod N.$$

Corolario (Euler, Carmichael)

Si $N = p \cdot q$ es un producto de dos números primos que no dividen a m y $0 < m < N$,

$$m^{mcm(p-1,q-1)} \equiv 1 \mod N.$$

1. $N = p \cdot q$ y elijo números e, f tales que $e \cdot f - 1 = r \cdot \mathrm{mcm}(p-1, q-1)$.

El pequeño teorema de Fermat

Teorema (Fermat '1640, Euler'1736, Leibniz'1683)

Si N es un número primo y $0 < m < N$, entonces

$$m^{N-1} \equiv 1 \mod N.$$

Corolario (Euler, Carmichael)

Si $N = p \cdot q$ es un producto de dos números primos que no dividen a m y $0 < m < N$,

$$m^{mcm(p-1,q-1)} \equiv 1 \mod N.$$

1. $N = p \cdot q$ y elijo números e, f tales que $e \cdot f - 1 = r \cdot \mathrm{mcm}(p-1, q-1)$.
2. Codifico un mensaje m de la siguiente manera: $m \mapsto c = m^e \mod N$.

El pequeño teorema de Fermat

Teorema (Fermat '1640, Euler'1736, Leibniz'1683)

Si N es un número primo y $0 < m < N$, entonces

$$m^{N-1} \equiv 1 \mod N.$$

Corolario (Euler, Carmichael)

Si $N = p \cdot q$ es un producto de dos números primos que no dividen a m y $0 < m < N$,

$$m^{mcm(p-1,q-1)} \equiv 1 \mod N.$$

1. $N = p \cdot q$ y elijo números e, f tales que $e \cdot f - 1 = r \cdot \mathrm{mcm}(p-1, q-1)$.
2. Codifico un mensaje m de la siguiente manera: $m \mapsto c = m^e \mod N$.
3. Descodifico el mensaje codificado c: $c \mapsto \sqrt[e]{c}$,

El pequeño teorema de Fermat

Teorema (Fermat '1640, Euler'1736, Leibniz'1683)

Si N es un número primo y $0 < m < N$, entonces

$$m^{N-1} \equiv 1 \quad \text{mod } N.$$

Corolario (Euler, Carmichael)

Si $N = p \cdot q$ es un producto de dos números primos que no dividen a m y $0 < m < N$,

$$m^{mcm(p-1,q-1)} \equiv 1 \quad \text{mod } N.$$

1. $N = p \cdot q$ y elijo números e, f tales que $e \cdot f - 1 = r \cdot \text{mcm}(p-1, q-1)$.
2. Codifico un mensaje m de la siguiente manera: $m \mapsto c = m^e \quad \text{mod } N$.
3. Descodifico el mensaje codificado c: $c \mapsto \sqrt[e]{c}$, **pero** $\sqrt[e]{c} \equiv c^f \quad \text{mod } N$**!:**

El pequeño teorema de Fermat

Teorema (Fermat '1640, Euler'1736, Leibniz'1683)

Si N es un número primo y $0 < m < N$, entonces

$$m^{N-1} \equiv 1 \mod N.$$

Corolario (Euler, Carmichael)

Si $N = p \cdot q$ es un producto de dos números primos que no dividen a m y $0 < m < N$,

$$m^{mcm(p-1,q-1)} \equiv 1 \mod N.$$

1. $N = p \cdot q$ y elijo números e, f tales que $e \cdot f - 1 = r \cdot \mathrm{mcm}(p-1, q-1)$.
2. Codifico un mensaje m de la siguiente manera: $m \mapsto c = m^e \mod N$.
3. Descodifico el mensaje codificado c: $c \mapsto \sqrt[e]{c}$, **pero** $\sqrt[e]{c} \equiv c^f \mod N$**!:**

$$c^f \equiv (m^e)^f$$

El pequeño teorema de Fermat

Teorema (Fermat '1640, Euler'1736, Leibniz'1683)

Si N es un número primo y $0 < m < N$, entonces

$$m^{N-1} \equiv 1 \mod N.$$

Corolario (Euler, Carmichael)

Si $N = p \cdot q$ es un producto de dos números primos que no dividen a m y $0 < m < N$,

$$m^{\mathrm{mcm}(p-1,q-1)} \equiv 1 \mod N.$$

1. $N = p \cdot q$ y elijo números e, f tales que $e \cdot f - 1 = r \cdot \mathrm{mcm}(p-1, q-1)$.
2. Codifico un mensaje m de la siguiente manera: $m \mapsto c = m^e \mod N$.
3. Descodifico el mensaje codificado c: $c \mapsto \sqrt[e]{c}$, **pero** $\sqrt[e]{c} \equiv c^f \mod N$**!:**

$$c^f \equiv (m^e)^f \equiv m^{e \cdot f}$$

El pequeño teorema de Fermat

Teorema (Fermat '1640, Euler'1736, Leibniz'1683)

Si N es un número primo y $0 < m < N$, entonces

$$m^{N-1} \equiv 1 \mod N.$$

Corolario (Euler, Carmichael)

Si $N = p \cdot q$ es un producto de dos números primos que no dividen a m y $0 < m < N$,

$$m^{mcm(p-1,q-1)} \equiv 1 \mod N.$$

1. $N = p \cdot q$ y elijo números e, f tales que $e \cdot f - 1 = r \cdot \mathrm{mcm}(p-1, q-1)$.
2. Codifico un mensaje m de la siguiente manera: $m \mapsto c = m^e \mod N$.
3. Descodifico el mensaje codificado c: $c \mapsto \sqrt[e]{c}$, **pero** $\sqrt[e]{c} \equiv c^f \mod N$**!:**

$$c^f \equiv (m^e)^f \equiv m^{e\cdot f} \equiv m \cdot m^{e\cdot f-1}$$

El pequeño teorema de Fermat

Teorema (Fermat '1640, Euler'1736, Leibniz'1683)

Si N es un número primo y $0 < m < N$, entonces

$$m^{N-1} \equiv 1 \mod N.$$

Corolario (Euler, Carmichael)

Si $N = p \cdot q$ es un producto de dos números primos que no dividen a m y $0 < m < N$,

$$m^{mcm(p-1,q-1)} \equiv 1 \mod N.$$

1. $N = p \cdot q$ y elijo números e, f tales que $e \cdot f - 1 = r \cdot \mathrm{mcm}(p-1, q-1)$.
2. Codifico un mensaje m de la siguiente manera: $m \mapsto c = m^e \mod N$.
3. Descodifico el mensaje codificado c: $c \mapsto \sqrt[e]{c}$, **pero** $\sqrt[e]{c} \equiv c^f \mod N$**!:**

$$c^f \equiv (m^e)^f \equiv m^{e\cdot f} \equiv m \cdot m^{e\cdot f-1} \equiv m\cdot\left(m^{r\cdot \mathrm{mcm}(p-1,q-1)}\right)$$

El pequeño teorema de Fermat

Teorema (Fermat '1640, Euler'1736, Leibniz'1683)

Si N es un número primo y $0 < m < N$, entonces

$$m^{N-1} \equiv 1 \mod N.$$

Corolario (Euler, Carmichael)

Si $N = p \cdot q$ es un producto de dos números primos que no dividen a m y $0 < m < N$,

$$m^{mcm(p-1,q-1)} \equiv 1 \mod N.$$

1. $N = p \cdot q$ y elijo números e, f tales que $e \cdot f - 1 = r \cdot \mathrm{mcm}(p-1, q-1)$.
2. Codifico un mensaje m de la siguiente manera: $m \mapsto c = m^e \mod N$.
3. Descodifico el mensaje codificado c: $c \mapsto \sqrt[e]{c}$, **pero** $\sqrt[e]{c} \equiv c^f \mod N$**!:**

$$c^f \equiv (m^e)^f \equiv m^{e\cdot f} \equiv m \cdot m^{e\cdot f-1} \equiv m \cdot \left(m^{r\cdot \mathrm{mcm}(p-1,q-1)}\right) \equiv m \cdot \left(m^{\mathrm{mcm}(p-1,q-1)}\right)^r$$

El pequeño teorema de Fermat

Teorema (Fermat '1640, Euler'1736, Leibniz'1683)

Si N es un número primo y $0 < m < N$, entonces

$$m^{N-1} \equiv 1 \mod N.$$

Corolario (Euler, Carmichael)

Si $N = p \cdot q$ es un producto de dos números primos que no dividen a m y $0 < m < N$,

$$m^{mcm(p-1,q-1)} \equiv 1 \mod N.$$

1. $N = p \cdot q$ y elijo números e, f tales que $e \cdot f - 1 = r \cdot \mathrm{mcm}(p-1, q-1)$.
2. Codifico un mensaje m de la siguiente manera: $m \mapsto c = m^e \mod N$.
3. Descodifico el mensaje codificado c: $c \mapsto \sqrt[e]{c}$, **pero** $\sqrt[e]{c} \equiv c^f \mod N$**!:**

$$c^f \equiv (m^e)^f \equiv m^{e \cdot f} \equiv m \cdot m^{e \cdot f - 1} \equiv m \cdot \left(m^{r \cdot \mathrm{mcm}(p-1,q-1)}\right) \equiv m \cdot \left(m^{\mathrm{mcm}(p-1,q-1)}\right)^r \equiv m \cdot 1^r$$

El pequeño teorema de Fermat

Teorema (Fermat '1640, Euler'1736, Leibniz'1683)

Si N es un número primo y $0 < m < N$, entonces

$$m^{N-1} \equiv 1 \mod N.$$

Corolario (Euler, Carmichael)

Si $N = p \cdot q$ es un producto de dos números primos que no dividen a m y $0 < m < N$,

$$m^{mcm(p-1,q-1)} \equiv 1 \mod N.$$

1. $N = p \cdot q$ y elijo números e, f tales que $e \cdot f - 1 = r \cdot \mathrm{mcm}(p-1, q-1)$.
2. Codifico un mensaje m de la siguiente manera: $m \mapsto c = m^e \mod N$.
3. Descodifico el mensaje codificado c: $c \mapsto \sqrt[e]{c}$, **pero** $\sqrt[e]{c} \equiv c^f \mod N$**!:**

$$c^f \equiv (m^e)^f \equiv m^{e \cdot f} \equiv m \cdot m^{e \cdot f - 1} \equiv m \cdot \left(m^{r \cdot \mathrm{mcm}(p-1,q-1)}\right) \equiv m \cdot \left(m^{\mathrm{mcm}(p-1,q-1)}\right)^r \equiv m \cdot 1^r \equiv m$$

RSA (Rivest, Shamir, Adleman '1979 (MIT))

Como transmitir un mensaje m (un número). Por ejemplo, $m = 42$.

RSA (Rivest, Shamir, Adleman '1979 (MIT))

Como transmitir un mensaje m (un número). Por ejemplo, $m = 42$.

1. El centurión elige 2 números primos p, q que no dividan a m de manera que $m < N = p \cdot q$.

$$p = 5 \qquad q = 11 \qquad N = 55$$

RSA (Rivest, Shamir, Adleman '1979 (MIT))

Como transmitir un mensaje m (un número). Por ejemplo, $m = 42$.

1. El centurión elige 2 números primos p, q que no dividan a m de manera que $m < N = p \cdot q$.

$$p = 5 \qquad q = 11 \qquad N = 55$$

2. El centurión elige dos números e, f de manera que $e \cdot f - 1$ sea múltiplo de $\mathrm{mcm}(p-1, q-1)$.

$$e = 7 \qquad f = 3 \qquad 21 - 1 = 1 \cdot 20.$$

RSA (Rivest, Shamir, Adleman '1979 (MIT))

Como transmitir un mensaje m (un número). Por ejemplo, $m = 42$.

1. El centurión elige 2 números primos p, q que no dividan a m de manera que $m < N = p \cdot q$.

$$p = 5 \qquad q = 11 \qquad N = 55$$

2. El centurión elige dos números e, f de manera que $e \cdot f - 1$ sea múltiplo de $\mathrm{mcm}(p-1, q-1)$.

$$e = 7 \qquad f = 3 \qquad 21 - 1 = 1 \cdot 20.$$

3. La clave pública será N, e. El mensaje original se codifica así: $c = m^e \bmod N$.

$$c \equiv 42^7 \equiv 42^2 \cdot 42^2 \cdot 42^2 \cdot 42 \equiv 4 \cdot 4 \cdot 4 \cdot 42 \equiv 9 \cdot 42 \equiv 48.$$

RSA (Rivest, Shamir, Adleman '1979 (MIT))

Como transmitir un mensaje m (un número). Por ejemplo, $m = 42$.

1. El centurión elige 2 números primos p, q que no dividan a m de manera que $m < N = p \cdot q$.

$$p = 5 \qquad q = 11 \qquad N = 55$$

2. El centurión elige dos números e, f de manera que $e \cdot f - 1$ sea múltiplo de $\mathrm{mcm}(p-1, q-1)$.

$$e = 7 \qquad f = 3 \qquad 21 - 1 = 1 \cdot 20.$$

3. La clave pública será N, e. El mensaje original se codifica así: $c = m^e \bmod N$.

$$c \equiv 42^7 \equiv 42^2 \cdot 42^2 \cdot 42^2 \cdot 42 \equiv 4 \cdot 4 \cdot 4 \cdot 42 \equiv 9 \cdot 42 \equiv 48.$$

4. La clave privada será N, f. El mensaje codificado se descodifica así: $m = c^f \bmod N$.

$$m \equiv 48^3 \equiv 48^2 \cdot 48 \equiv 49 \cdot 48 \equiv 42$$

¿Cómo crea el centurión las claves N, f y N, e?

¿Cómo crea el centurión las claves N, f y N, e?

1. Elijo 2 números primos p, q, de manera que $m < N = p \cdot q$ y N tenga unas **700 cifras**.
    - *Se toman números aleatorios p, q de unas 350 cifras.*

2. Elijo dos números e, f de manera que $e \cdot f - 1$ sea múltiplo de $mcm(p-1) \cdot (q-1)$.

¿Cómo crea el centurión las claves N, f y N, e?

1. Elijo 2 números primos p, q, de manera que $m < N = p \cdot q$ y N tenga unas **700 cifras**.
   - *Se toman números aleatorios p, q de unas 350 cifras.*
   - *La probabilidad de que un número de 350 cifras sea primo es $\frac{1}{ln(10^{350})} = \frac{1}{350 \ln(10)} \sim \frac{1}{806}$, así que después de probar 2000 veces tenemos una probabilidad del 92% de haber encontrado un primo.*

Teorema (Hadamard, de la Vallée Poussin, 1896)

La cantidad de números primos menores que r es $\frac{r}{\ln r}$ (aprox.).

2. Elijo dos números e, f de manera que $e \cdot f - 1$ sea múltiplo de $mcm(p-1) \cdot (q-1)$.

¿Cómo crea el centurión las claves N, f y N, e?

1. Elijo 2 números primos p, q, de manera que $m < N = p \cdot q$ y N tenga unas **700 cifras**.
   - *Se toman números aleatorios p, q de unas 350 cifras.*
   - *La probabilidad de que un número de 350 cifras sea primo es $\frac{1}{ln(10^{350})} = \frac{1}{350 \ln(10)} \sim \frac{1}{806}$, así que después de probar 2000 veces tenemos una probabilidad del 92% de haber encontrado un primo.*
   - *Comprobar si un número es primo es* **muy rápido**. *El último gran avance fue en el año 2002 con el algoritmo AKS de Agrawal, Kayal y Saxena (Kanpur).*

Teorema (Hadamard, de la Vallée Poussin, 1896)

La cantidad de números primos menores que r es $\frac{r}{\ln r}$ (aprox.).

2. Elijo dos números e, f de manera que $e \cdot f - 1$ sea múltiplo de $mcm(p-1) \cdot (q-1)$.

¿Cómo crea el centurión las claves N, f y N, e?

1. Elijo 2 números primos p, q, de manera que $m < N = p \cdot q$ y N tenga unas **700 cifras**.
   - *Se toman números aleatorios p, q de unas 350 cifras.*
   - *La probabilidad de que un número de 350 cifras sea primo es $\frac{1}{ln(10^{350})} = \frac{1}{350 \ln(10)} \sim \frac{1}{806}$, así que después de probar 2000 veces tenemos una probabilidad del 92% de haber encontrado un primo.*
   - *Comprobar si un número es primo es* **muy rápido**. *El último gran avance fue en el año 2002 con el algoritmo AKS de Agrawal, Kayal y Saxena (Kanpur).*

Teorema (Hadamard, de la Vallée Poussin, 1896)

La cantidad de números primos menores que r es $\frac{r}{\ln r}$ (aprox.).

2. Elijo dos números e, f de manera que $e \cdot f - 1$ sea múltiplo de $mcm(p-1) \cdot (q-1)$.

¿Cómo crea el centurión las claves N, f y N, e?

1. Elijo 2 números primos p, q, de manera que $m < N = p \cdot q$ y N tenga unas **700 cifras**.
   - *Se toman números aleatorios p, q de unas 350 cifras.*
   - *La probabilidad de que un número de 350 cifras sea primo es $\frac{1}{ln(10^{350})} = \frac{1}{350 \ln(10)} \sim \frac{1}{806}$, así que después de probar 2000 veces tenemos una probabilidad del 92% de haber encontrado un primo.*
   - *Comprobar si un número es primo es* **muy rápido**. *El último gran avance fue en el año 2002 con el algoritmo AKS de Agrawal, Kayal y Saxena (Kanpur).*

Teorema (Hadamard, de la Vallée Poussin, 1896)

La cantidad de números primos menores que r es $\frac{r}{\ln r}$ (aprox.).

2. Elijo dos números e, f de manera que $e \cdot f - 1$ sea múltiplo de $mcm(p-1) \cdot (q-1)$.
   - *Primero elijo e coprimo con $p-1$ y $q-1$ y luego encuentro f usando el* **algoritmo de Euclides**.

Para los galos es **difícil** descubrir la clave privada?

¿Cómo crea el centurión las claves N, f y N, e?

1. Elijo 2 números primos p, q, de manera que $m < N = p \cdot q$ y N tenga unas **700 cifras**.

   Generar números primos es **fácil***, gracias a AKS, Hadamard y de la Vallée Poussin.*

2. Elijo dos números e, f de manera que $e \cdot f - 1$ sea múltiplo de $(p-1)\cdot(q-1)$.

   También es **fácil** *usando el algoritmo de Euclides.*

Para los galos es **difícil** descubrir la clave privada?

¿Cómo crea el centurión las claves N, f y N, e?




1. Elijo 2 números primos p, q, de manera que $m < N = p \cdot q$ y N tenga unas **700 cifras**.

   Generar números primos es **fácil***, gracias a AKS, Hadamard y de la Vallée Poussin.*

2. Elijo dos números e, f de manera que $e \cdot f - 1$ sea múltiplo de $(p-1) \cdot (q-1)$.

   También es **fácil** *usando el algoritmo de Euclides.*

¿Pueden los galos conseguir la clave privada N, f conociendo la clave pública N, e?

Para los galos es **difícil** descubrir la clave privada?

¿Cómo crea el centurión las claves N, f y N, e?

1. Elijo 2 números primos p, q, de manera que $m < N = p \cdot q$ y N tenga unas **700 cifras**.

   Generar números primos es **fácil**, *gracias a AKS, Hadamard y de la Vallée Poussin.*

2. Elijo dos números e, f de manera que $e \cdot f - 1$ sea múltiplo de $(p-1) \cdot (q-1)$.

   También es **fácil** *usando el algoritmo de Euclides.*

¿Pueden los galos conseguir la clave privada N, f conociendo la clave pública N, e?

Hay que descomponer el número N de 700 cifras en factores primos.

- *este es (hoy en día) un problema* **muy difícil** *para un ordenador (un PC lo puede resolver si N tiene menos de 80 cifras)...*

Para los galos es **difícil** descubrir la clave privada ?

¿Cómo crea el centurión las claves N, f y N, e ?

1. Elijo 2 números primos p, q, de manera que $m < N = p \cdot q$ y N tenga unas **700 cifras**.

   Generar números primos es **fácil***, gracias a AKS, Hadamard y de la Vallée Poussin.*

2. Elijo dos números e, f de manera que $e \cdot f - 1$ sea múltiplo de $(p - 1) \cdot (q - 1)$.

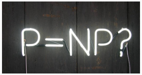
   También es **fácil** *usando el algoritmo de Euclides.*




¿Pueden los galos conseguir la clave privada N, f conociendo la clave pública N, e ?

Hay que descomponer el número N de 700 cifras en factores primos.

- *este es (hoy en día) un problema* **muy difícil** *para un ordenador (un PC lo puede resolver si N tiene menos de 80 cifras)...* **¡...pero no para un ordenador cuántico!**



Ordenadores cuánticos

Los ordenadores cuánticos fueron diseñados (teóricamente) en la década de los 80. Las propiedades del mundo cuántico hacen que estos qubits puedan hacer operaciones inaccesibles para los ordenadores convencionales. En 1994, Peter Shor (MIT) diseñó un algoritmo cuántico que permite factorizar números muy rápidamente. Esto haría inútil el sistema RSA.

Ordenadores cuánticos

Los ordenadores cuánticos fueron diseñados (teóricamente) en la década de los 80. Las propiedades del mundo cuántico hacen que estos qubits puedan hacer operaciones inaccesibles para los ordenadores convencionales. En 1994, Peter Shor (MIT) diseñó un algoritmo cuántico que permite factorizar números muy rápidamente. Esto haría inútil el sistema RSA.

La tecnología necesaria para construirlos (en la práctica) ha ido llegando poco a poco, pero ya está aquí. En octubre de 2019 Sergio Boixo y John Martinis (Google) anunciaron que habían conseguido fabricar un pequeño ordenador cuántico capaz de realizar, por primera vez en la historia, un cálculo mucho más rápido que un ordenador convencional.

`https://www.youtube.com/watch?v=OaMLmGsNkDg`
`https://www.youtube.com/embed/gylmjTOUfCQ`
`https://www.cuatro.com/planetacalleja/sergio-boixo-completo_18_2912970276.html`

Sergio Boixo

John Martinis