Para que Serve a Matemática ?

António Machiavelo

Departamento de Matemática da Faculdade de Ciências do Porto

Universidade Popular do Porto
16 de Junho de 2010

Códigos secretos

Uma chave:

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

O SOMBRA DA MENTIRA → YVYDN YTYZH DOHHM SOH

ANTON IOGED EAO ← HDFYD SYJGO GHY

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

Um Criptograma

IOINE PQNPV ITEIT NQEBP TDUIQ NQEBQ IUTPL QENSP ESIWP YFWPS PQLQE LXISP IWIHF
EFWPL QTQQU SXPLQ FNPDU PODUI XLQTQ INSPK IWXPL FERIE SPITD UITIN IESQI WINLP
ENQLQ TQINS IXFVI FXQTP ENQIT NIXIE QNNQV XINNP OSQNL QTQIN SINKF EBIFX QNPOS
QNDUI ITYIX WIIQF XQNIP CFSPT LQTQI NSPNP YINDU ICXFS PTITV IVIWI FXPNW IPRUO
IOINE PQNPV ITDUI QNQEB QIYFE BQIIN KUTPI HIXTI ESQVF LBFEB QPOPL XIINI WIESQ
WIHQL FEBQK QESFP CUWQD UIHQN NPPSX PYINW ISUWQ EUTKI XKISU QTQYF TIESQ IOINE
PQNPV ITDUI QNQEB QISIO PILQX IKFEL IOVPN IHUNS ILPKF SIOPX LQITQ CFYPY FSXPO
KFEPL UOQWI LPSIW XPOLQ ESXPK QESQN FEHQE FPTPN LPXPC XICPT PCFPD UIIXI SQXSP
WIPOD UFTFN SPTPK PWQTU EWQWF NSPES IXQNP WQNYI ESQNF EHPES ILPXP YIOPD UFEBI
ESFNS PDUII LPVQW PVQPI NKIXP ELPQU XQLPE IOPTP XHFTH OQXIS IWIIN KPWPL BFTVP
NSFWQ XKPNN QWIWP ELPLQ OQTVF EPIPX OIDUF TKPNN PXQOP YQPWQ XPKPX PXPFQ
NOQLQ TQSFY PVPXL QWIKX QPHIN SFYPP OSQHQ XEQCI XPWQX PLFNP QWQPS QTQXP
WPXUO SXPNQ TSIOI YFNPQ WINIT VPXDU IITHQ CUISP QEPNU KIXHF LFIOU EPXIO INEPQ
NPVIT EITNQ EBPTD UIQNQ EBQLQ TPEWP PYFWP DUINI TKXID UIUTB QTITN QEBPQ TUEWQ
KUOPI PYPEL PLQTQ VQOPL QOQXF WPIES XIPNT PQNWI UTPLX FPELP

Cifras mono-alfabéticas: segurança

Número de chaves distintas:

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

26 x 25 x 24 x 23 x 22 x 21 x 20 x 19 x 18 x 17 x 16 x 15 x 14 x 13 x 12 x 11 x 10 x 9 x 8 x 7 x 6 x 5 x 4 x 3 x 2 x 1

$= 403\,291\,461\,126\,605\,635\,584\,000\,000 \simeq 4 \times 10^{26}$

chaves distintas para a cifra de substituição

Testando 1 milhão de chaves por segundo...

... demorar-se-ia mais de $6,39 \times 10^{12}$ anos

... para testar metade das chaves!

Idade do Universo: "apenas" cerca de $1,4 \times 10^{10}$ anos.

O Criptograma

IOINE PQNPV ITEIT NQEBP TDUIQ NQEBQ IUTPL QENSP ESIWP YFWPS PQLQE LXISP IWIHF
EFWPL QTQQU SXPLQ FNPDU PODUI XLQTQ INSPK IWXPL FERIE SPITD UITIN IESQI WINLP
ENQLQ TQINS IXFVI FXQTP ENQIT NIXIE QNNQV XINNP OSQNL QTQIN SINKF EBIFX QNPOS
QNDUI ITYIX WIIQF XQNIP CFSPT LQTQI NSPNP YINDU ICXFS PTITV IVIWI FXPNW IPRUO
IOINE PQNPV ITDUI QNQEB QIYFE BQIIN KUTPI HIXTI ESQVF LBFEB QPOPL XIINI WIESQ
WIHQL FEBQK QESFP CUWQD UIHQN NPPSX PYINW ISUWQ EUTKI XKISU QTQYF TIESQ IOINE
PQNPV ITDUI QNQEB QISIO PILQX IKFEL IOVPN IHUNS ILPKF SIOPX LQITQ CFYPY FSXPO
KFEPL UOQWI LPSIW XPOLQ ESXPK QESQN FEHQE FPTPN LPXPC XICPT PCFPD UIIXI SQXSP
WIPOD UFTFN SPTPK PWQTU EWQWF NSPES IXQNP WQNYI ESQNF EHPES ILPXP YIOPD UFEBI
ESFNS PDUII LPVQW PVQPI NKIXP ELPQU XQLPE IOPTP XHFTH OQXIS IWIIN KPWPL BFTVP
NSFWQ XKPNN QWIWP ELPLQ OQTVF EPIPX OIDUF TKPNN PXQOP YQPWQ XPKPX PXPFQ
NOQLQ TQSFY PVPXL QWIKX QPHIN SFYPP OSQHQ XEQCI XPWQX PLFNP QWQPS QTQXP
WPXUO SXPNQ TSIOI YFNPQ WINIT VPXDU IITHQ CUISP QEPNU KIXHF LFIOU EPXIO INEPQ
NPVIT EITNQ EBPTD UIQNQ EBQLQ TPEWP PYFWP DUINI TKXID UIUTB QTITN QEBPQ TUEWQ
KUOPI PYPEL PLQTQ VQOPL QOQXF WPIES XIPNT PQNWI UTPLX FPELP

Uma observação simples

	Português	Espanhol	Inglês	Francês
A	13.8	12.7	7.8	9.4
B	0.9	1.4	1.3	1.0
C	4.5	3.9	2.9	2.6
D	5.6	5.6	4.1	3.4
E	12.0	13.2	13.1	15.9
F	1.0	0.5	2.9	1.0
G	1.2	1.1	1.4	1.0
H	0.6	1.2	5.9	0.8
I	7.0	6.3	6.8	8.4
J	0.6	0.6	0.2	0.9
K	0.0	0.0	0.4	0.0
L	2.8	5.9	3.6	5.3
M	4.1	2.7	2.6	3.2

	Português	Espanhol	Inglês	Francês
N	5.3	7.0	7.3	7.2
O	10.8	9.5	8.2	5.1
P	2.9	2.4	2.2	2.9
Q	0.8	1.2	0.1	1.1
R	6.9	6.3	6.6	6.5
S	7.8	7.6	6.5	7.9
T	4.9	3.9	9.0	7.3
U	3.8	4.6	2.8	6.2
V	1.3	1.1	1.0	2.2
W	0.0	0.0	1.5	0.0
X	0.2	0.1	0.3	0.3
Y	0.0	1.1	1.5	0.2
Z	0.3	0.1	0.1	0.3

O Criptograma

IOINE PQNPV ITEIT NQEBP TDUIQ NQEBQ IUTPL QENSP ESIWP YFWPS PQLQE LXISP IWIHF
EFWPL QTQQU SXPLQ FNPDU PODUI XLQTQ INSPK IWXPL FERIE SPITD UITIN IESQI WINLP
ENQLQ TQINS IXFVI FXQTP ENQIT NIXIE QNNQV XINNP OSQNL QTQIN SINKF EBIFX QNPOS
QNDUI ITYIX WIIQF XQNIP CFSPT LQTQI NSPNP YINDU ICXFS PTITV IVIWI FXPNW IPRUO
IOINE PQNPV ITDUI QNQEB QIYFE BQIIN KUTPI HIXTI ESQVF LBFEB QPOPL XIINI WIESQ
WIHQL FEBQK QESFP CUWQD UIHQN NPPSX PYINW ISUWQ EUTKI XKISU QTQYF TIESQ IOINE
PQNPV ITDUI QNQEB QISIO PILQX IKFEL IOVPN IHUNS ILPKF SIOPX LQITQ CFYPY FSXPO
KFEPL UOQWI LPSIW XPOLQ ESXPK QESQN FEHQE FPTPN LPXPC XICPT PCFPD UIIXI SQXSP
WIPOD UFTFN SPTPK PWQTU EWQWF NSPES IXQNP WQNYI ESQNF EHPES ILPXP YIOPD UFEBI
ESFNS PDUII LPVQW PVQPI NKIXP ELPQU XQLPE IOPTP XHFTH OQXIS IWIIN KPWPL BFTVP
NSFWQ XKPNN QWIWP ELPLQ OQTVF EPIPX OIDUF TKPNN PXQOP YQPWQ XPKPX PXPFQ
NOQLQ TQSFY PVPXL QWIKX QPHIN SFYPP OSQHQ XEQCI XPWQX PLFNP QWQPS QTQXP
WPXUO SXPNQ TSIOI YFNPQ WINIT VPXDU IITHQ CUISP QEPNU KIXHF LFIOU EPXIO INEPQ
NPVIT EITNQ EBPTD UIQNQ EBQLQ TPEWP PYFWP DUINI TKXID UIUTB QTITN QEBPQ TUEWQ
KUOPI PYPEL PLQTQ VQOPL QOQXF WPIES XIPNT PQNWI UTPLX FPELP

Cripto-análise

	pt	cpgr	%
A	13.8	0	0.00
B	0.9	15	1.58
C	4.5	9	0.95
D	5.6	18	1.89
E	12.0	57	6.00
F	1.0	48	5.05
G	1.2	0	0.00
H	0.6	13	1.37
I	7.0	128	13.50
J	0.6	0	0.00
K	0.0	20	2.11
L	2.8	39	4.11
M	4.1	0	0.00

	pt	cpgr	%
N	5.3	70	7.37
O	10.8	30	3.16
P	2.9	127	13.40
Q	0.8	112	11.80
R	6.9	2	0.21
S	7.8	48	5.05
T	4.9	52	5.47
U	3.8	38	4.00
V	1.3	17	1.79
W	0.0	38	4.00
X	0.2	53	5.58
Y	0.0	16	1.68
Z	0.3	0	0.00

A , E → I , P

O → Q

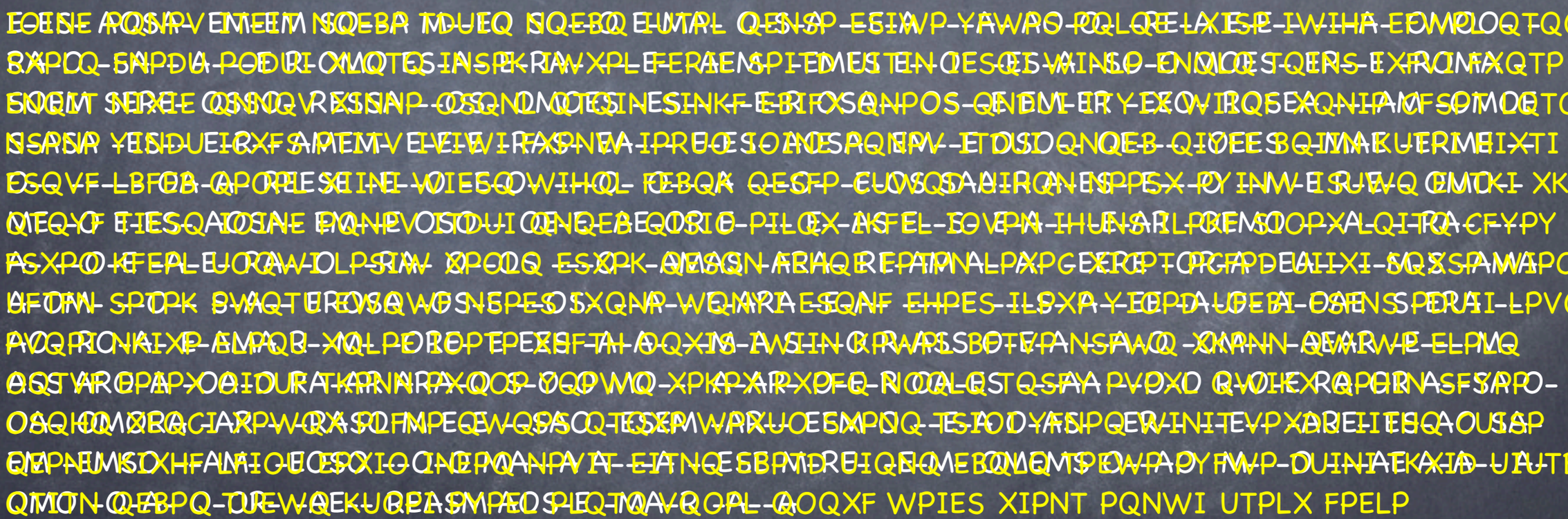
S → N

R → E ou X

Cripto-análise

E ⟷ I O ⟷ Q R ⟷ X

A ⟷ P S ⟷ N M ⟷ T

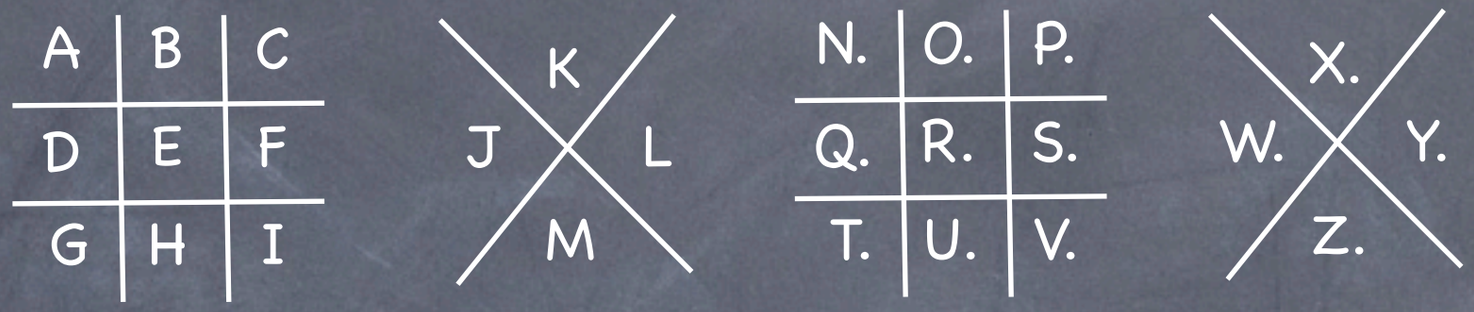


O texto original...

[illegible]

Uma cifra masónica

Uma chave:



Poema →

Enigma ←

Cifra de Vigenère

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
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
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
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
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
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
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
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
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
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
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
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
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
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
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
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
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
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
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
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
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
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
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
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
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

Uma chave: HILBERT

HILBE RTHIL BERTH ILBER THI

OSEGREDOEAMALMA DOSEGREDO

VAPHV VWVML BPDTK WYFKF VPW

A Bífida

Uma chave — uma tabela:

	0	1	2	3	4
0	H	I	L	B	E
1	R	T	A	C	D
2	F	G	K	M	N
3	O	P	Q	S	U
4	V	W	X	Y	Z

(I = J)

+ um período: 7

PEDRAFILOSOFAL

3011120 0333210

1440201 2030022

OTAIZLI BSGLBHK

A. M. & R. Reis, "Automated Ciphertext-only Criptanalysis of the Bifid Cipher", Cryptologia 31 (2007) 112-124

Números Primos

2, 3, 5, 7, 11, 13, 17, 19, 23, 29, 31, 37, 41, 43, 47, 53, 59, 61, 67, 71, 73,
79, 83, 89, 97, 101, 103, 107, 109, 113, 127, 131, 137, 139, 149, 151, 157,
163, 167, 173, 179, 181, 191, 193, 197, 199, 211, 223, 227, 229, 233, 239,
241, 251, 257, 263, 269, 271, 277, 281, 283, 293, 307, 311, 313, 317,
331, 337, 347, 349, 353, 359, 367, 373, 379, 383, 389, 397, 401, 409,
419, 421, 431, 433, 439, 443, 449, 457, 461, 463, 467, 479, 487, 491,
499, 503, 509, 521, 523, 541, 547, 557, 563, 569, 571, 577, 587, 593,
599, 601, 607, 613, 617, 619, 631, 641, 643, 647, 653, 659, 661, 673,
677, 683, 691, 701, 709, 719, 727, 733, 739, 743, 751, 757, 761, 769,
773, 787, 797, 809, 811, 821, 823, 827, 829, 839, 853, 857, 859, 863,
877, 881, 883, 887, 907, 911, 919, 929, 937, 941, 947, 953, 967, 971,
977, 983, 991, 997, 1009, 1013, 1019, 1021, 1031, 1033, 1039, 1049, 1051

Uma assimetria fundamental

$$7432339208719 \times 34111753100319412 9 = ?$$

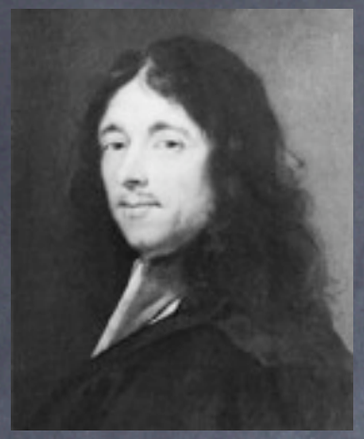
$$2^{101} - 1 = 2535301200456458802993406410751 = ? \times ?$$

Problema: o número...

2519590847565789349402718324004839857142928212620403202777713783604366202070759555626401852588078440691829064124951508218929855914917618450280848912007284499268739280728777673597141834727026189637501497182469116507761337985909570009733045974880842840179742910064245869181719511874612151517265463228221686998754918242243363725908514186546204357679842338718477444792073993423658482382428119816381501067481045166037730605620161967625613384414360383390441495263443219011465754445417842402092461651572335077870774981712577246796292638635637328991215483143816789988504044536402352738195137863656439121201039712282212072035 7

...é o produto de dois primos. Encontrar esses primos.

Dois resultados extraordinários



Pierre de Fermat
(1601/7/8? - 1665)

O "pequeno" teorema de Fermat:

$$a^{p-1} \equiv 1 \pmod{p}$$

p primo ; a inteiro não divisível por p

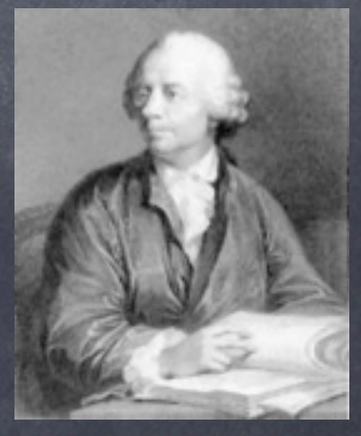
$$a^{m-1} \equiv r \pmod{m}$$

$$r \neq 1 \implies m \text{ é composto}$$

A generalização de Euler:

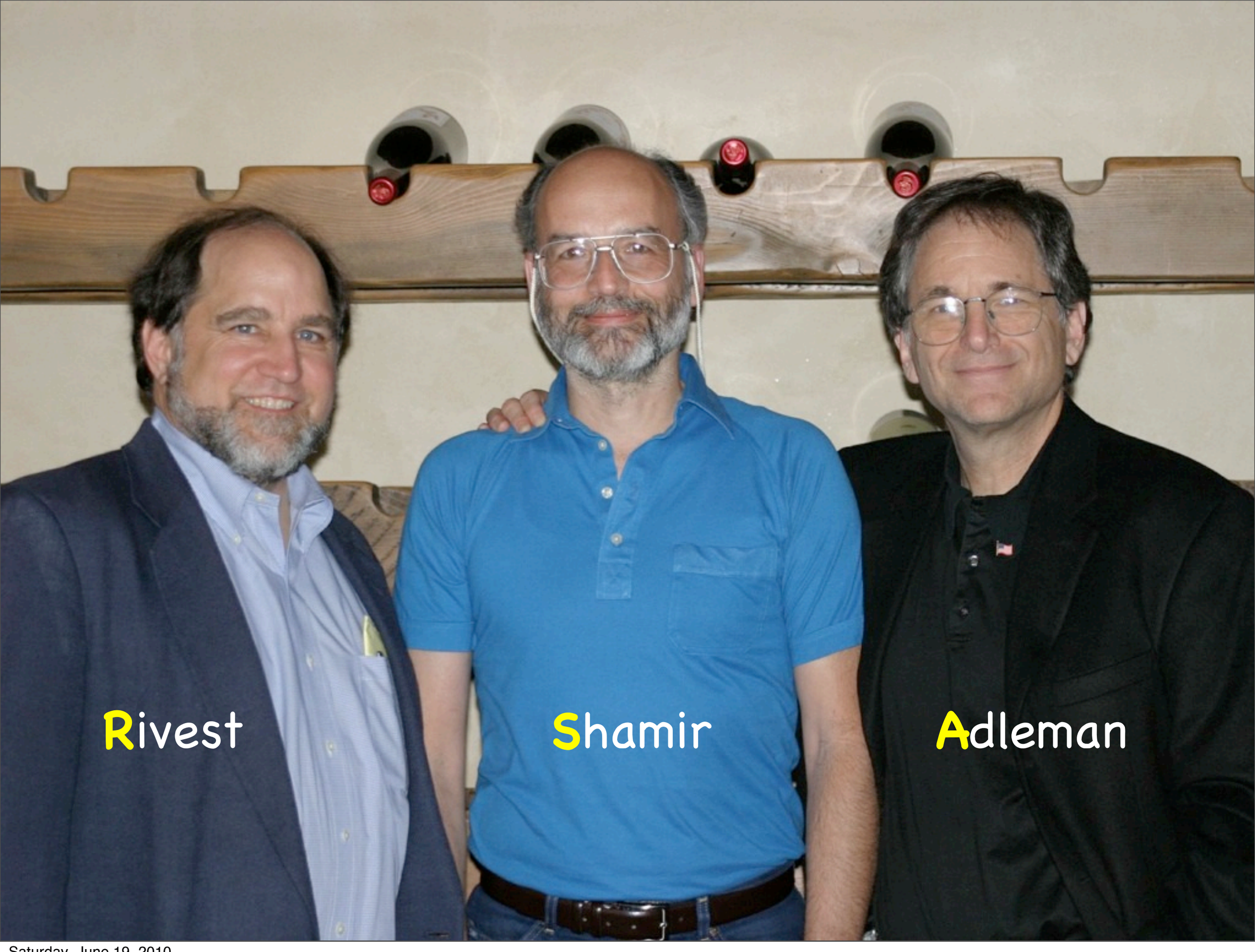
$$a^{\varphi(n)} \equiv 1 \pmod{n}$$

n natural qualquer
a inteiro sem factores comuns com n



Leonhard Euler
(1707-1783)

RSA


Rivest
Shamir
Adleman

Receita para construir uma cifra RSA

- p e q dois números primos "grandes" ($\sim$ 600 algarismos...)
- $n = pq$
- c um número sem factores comuns com $\varphi(n) = (p-1)(q-1)$
- Calcule-se (usando o *algoritmo de Euclides*) "o" número inteiro d tal que cd deixe resto 1 quando dividido por $\varphi(n)$

$$\begin{array}{rcl} \text{chave pública} & : & n, c \\ \text{chave privada} & : & d \end{array}$$

Segurança reside no facto de, para obter d a partir de n e c, ser necessário factorizar n...

RSA: como se cifra e se decifra

Alice cria uma cifra RSA, (n,c,d), publica n,c e mantém d secreto

Bob → Alice

Mensagem (em forma numérica) é dividida em blocos correspondentes a números inferiores a n

M = bloco a transmitir

↓

C = resto da divisão de M^c por n → resto da divisão de C^d por n = M

Graças a Fermat e Euler!

Assinaturas digitais com a cifra RSA

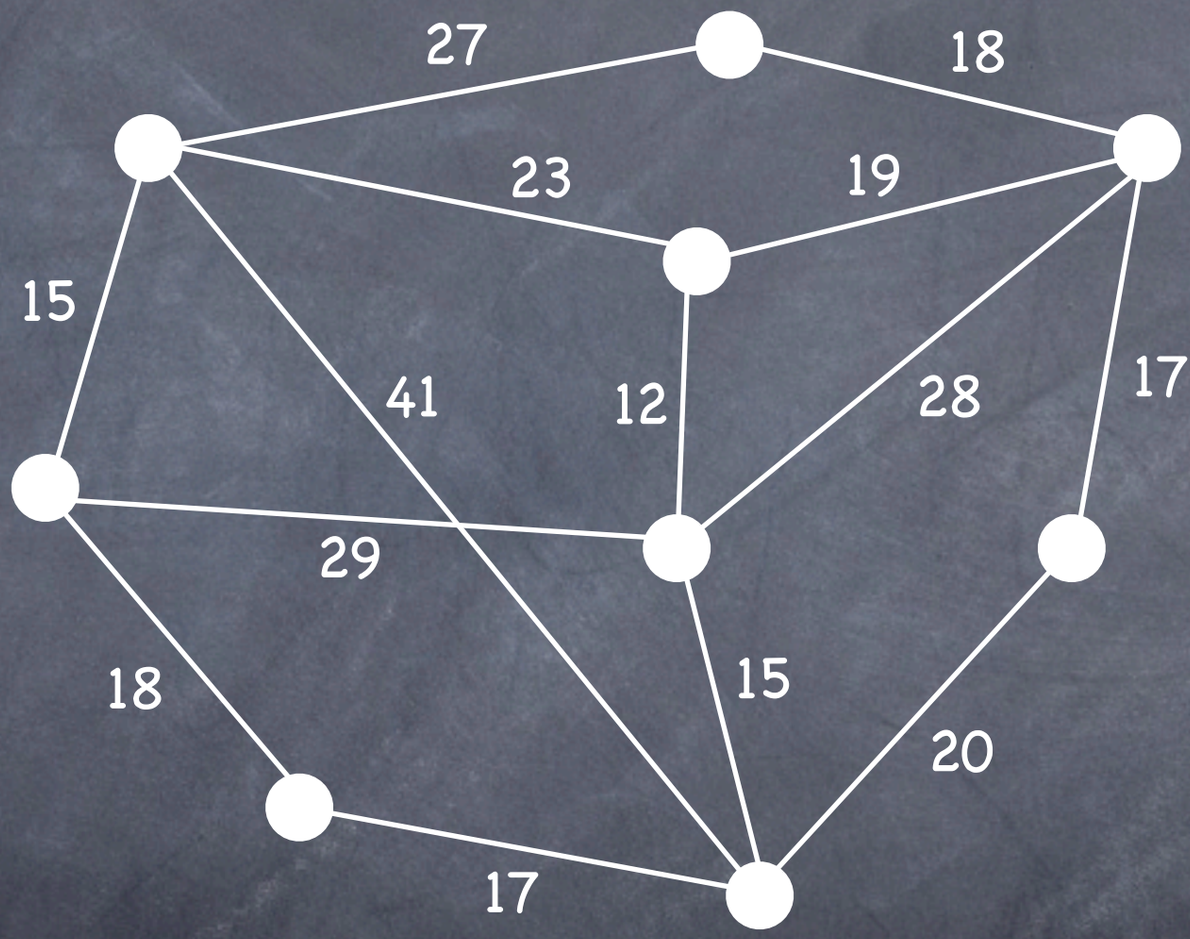
Alice cria uma cifra RSA: n,c,d

Para assinar um contrato C, que Bob lhe manda, Alice envia-lhe:

M = resto da divisão de C^d por n.

Só Alice pode produzir M a partir de C e qualquer pessoa pode verificar que o resto da divisão de M^c por n é igual a C.

O problema do caixeiro viajante



Mais algumas aplicações...

- Códigos correctores de erros, telemóveis e CDs.
- Obtenção de imagens médicas: tomografia.
- GPS, Google, "data mining", fotografias de alta resolução tiradas de satélites...
- Matemática no basquetebol...

Extracto de ``Um Diálogo sobre as Aplicações da Matemática" de Alfréd Rényi

Arquimedes: Recentemente recebi uma carta do meu amigo Eratóstenes na qual ele descreve um método simples mas muito engenhoso -- a que ele chama o "método do crivo" -- que ele inventou para encontrar números primos. Pensando um pouco sobre o método, fiz o esboço de uma máquina que aplica esta ideia. Esta máquina funciona com um conjunto de rodas dentadas: quando se gira uma delas um certo número de vezes, digamos n, e se olha por um orifício, se a vista não estiver obstruída, o número n é primo; mas se a vista estiver obstruída, então n é composto.

Hierão: Isso é realmente fantástico! Quando a guerra acabar, tens de construir essa máquina! Os meus convidados vão adorá-la.

Arquimedes: Se eu estiver vivo, certamente o farei. Mostrarei assim que as máquinas podem resolver problemas matemáticos. Talvez ajude os matemáticos a perceber que, mesmo do seu próprio ponto de vista, podem ganhar algo em estudar a relação entre a matemática e as máquinas.

Hierão: Por falar em ganhos, lembro-me de uma história sobre Euclides. Um dos seus alunos, estudando geometria, perguntou a Euclides: «O que é que eu ganho em aprender estas coisas?»

Extracto de ``Um Diálogo sobre as Aplicações da Matemática'' de Alfréd Rényi

Hierão: De imediato Euclides chamou um dos seus criados e disse-lhe: «Dá-lhe uma moeda, pois ele quer ganhar alguma coisa com o que aprende». Parece-me que esta história mostra que Euclides achava desnecessário um matemático preocupar-se com o uso prático dos seus resultados.

Arquimedes: Conheço, é claro, essa história, mas surpreender-te-á certamente saber que simpatizo completamente com Euclides. No seu lugar faria exactamente o mesmo.

Hierão: Agora fiquei confuso. Até agora falaste entusiasticamente acerca das aplicações da Matemática, e agora concordas com os puristas que pensam que a única recompensa que um cientista deve esperar é o prazer do conhecimento.

Arquimedes: Acho que tu e a maior parte das pessoas não entenderam a história sobre Euclides. Não significa que ele não estivesse interessado nas consequências práticas dos resultados matemáticos, e que as considerasse indignas de um filósofo. Isto é completamente disparatado; Euclides escreveu, como certamente sabes, um livro chamado Phaenomena, sobre astronomia, e um livro sobre óptica, e é provavelmente o autor do livro Catoptrica, que eu usei para construir os meus espelhos; e estava também interessado em mecânica.

Extracto de ``Um Diálogo sobre as Aplicações da Matemática" de Alfréd Rényi

Arquimedes: Como eu entendo a história, Euclides queria apenas realçar o facto notável que a Matemática recompensa apenas aqueles que nela estão interessados, não apenas pelas recompensas mas também por ela própria.

A Matemática é como a tua filha, Helena, que fica desconfiada cada vez que aparece um pretendente que não está realmente apaixonado por ela, mas cujo interesse nela tem apenas a ver com o facto de querer ser genro do rei. Ela quer um marido que a ama pela sua própria beleza, inteligência e charme, e não pela riqueza e poder que este obterá ao casar com ela.

Analogamente, a Matemática revela os seus segredos apenas àqueles que a abordam com amor puro, pela sua própria beleza. Aqueles que o fazem são obviamente recompensados com resultados de importância prática. Mas alguém que pergunte, a cada passo, «O que é que eu ganho com isto?», esse não irá longe.

Lembrar-te-ás de eu te ter dito que os romanos nunca seriam bem sucedidos em aplicar a matemática. Agora, vês porquê: são demasiado práticos!

FIM

Bibliografia

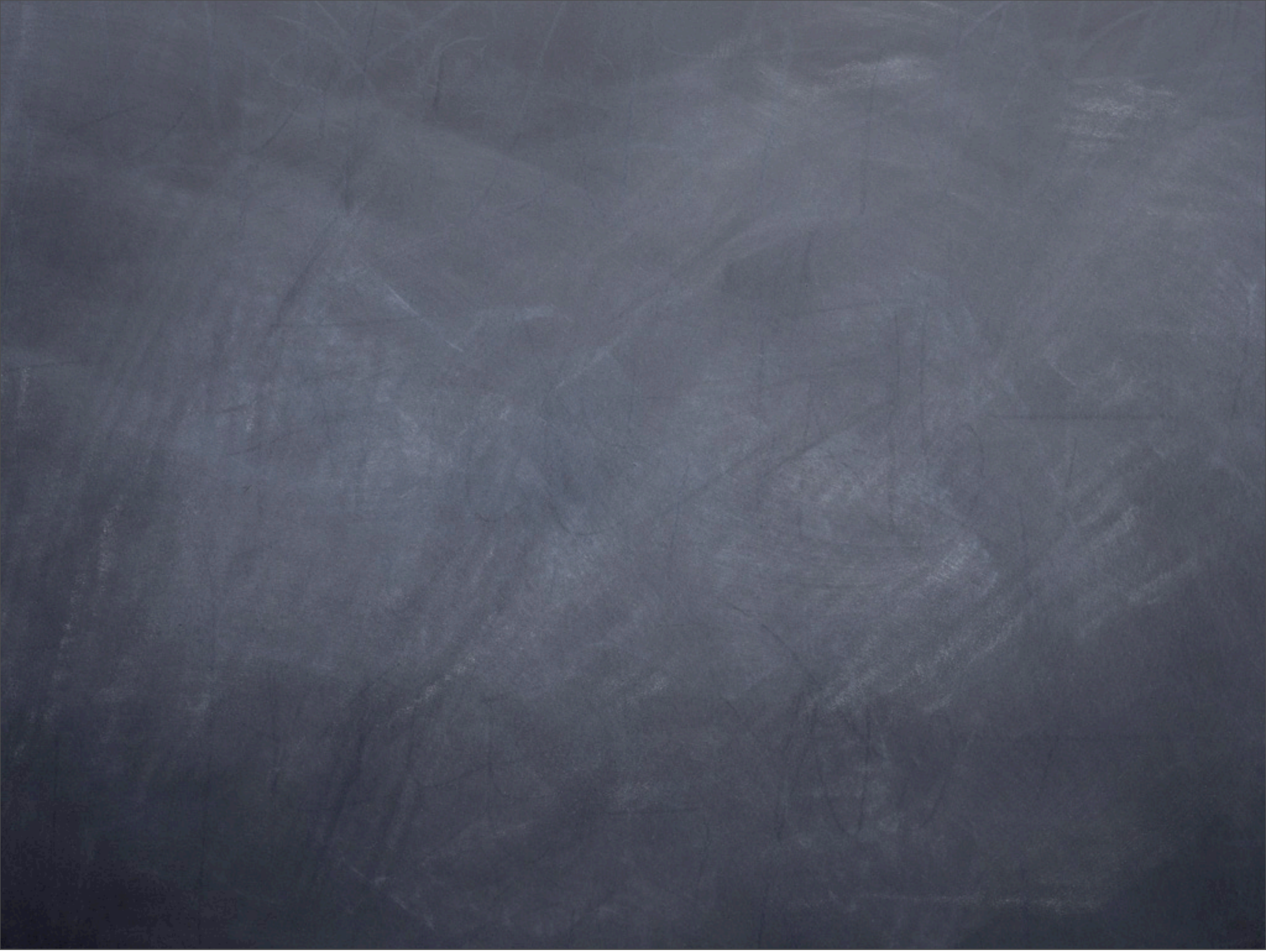
Martin G[illegible]er, Codes, Ciphers and Secret Writing [illegible]non & Schuste[illegible]2.

David Kha[illegible] The Codebreakers, The [illegible]cmillian Co[illegible]96[illegible]eeditado pel[illegible]ribn[illegible]m 1996).

Simon Sin[illegible] O Livro dos Códigos, T[illegible]s e Deba[illegible]1999.

Webgrafia

RSA Labo[illegible]ories: http://www.rsasecurity.com/r[illegible]labs



Safari File Edit View History Bookmarks Window Help

Caixadirecta on-line

https://caixadirecta.cgd.pt/CaixaDirecta/loginStart.do — Caixa Geral de Depositos S.A.

Google

InfoCiências MatemáticaPura CatálogoBiblioUP JSTOR UniversalDigitalLibrary Babylon YouTube Apple Google Maps News (585) Popular

caixadirecta on-line

que é? | FAQ's | Operações | Pre

Autenticaçã

Bem-vindo ao

Número de c

Código de ac

Se ainda não

Conheça

© 2010 Todos os direitos reservados | Linh

VeriSign Class 3 Public Primary Certification Authority - G5
↳ VeriSign Class 3 Extended Validation SSL SGC CA
↳ caixadirecta.cgd.pt

Common Name	VeriSign Class 3 Extended Validation SSL SGC CA
Serial Number	62 78 61 C6 FE FD 0E A7 9B 01 75 E6 41 1E D4 3D
Version	3
Signature Algorithm	SHA-1 with RSA Encryption (1 2 840 113549 1 1 5)
Parameters	none
Not Valid Before	Tuesday, December 15, 2009 00:00:00 GMT+00:00
Not Valid After	Wednesday, December 15, 2010 23:59:59 GMT+00:00
Public Key Info	
Algorithm	RSA Encryption (1 2 840 113549 1 1 1)
Parameters	none
Public Key	128 bytes : D1 E2 D6 C0 3F 56 05 F4 B7 CB C2 D7 E0 63 AA BF 0E 35 DE C7 C3 CA A0 2E BA 59 FA 02 49 2E 1D 95 44 1B 2B D7 88 27 47 42 2C 4F EB E0 CA 75 BF E8 2A 00 F8 86 0B FA FA 61 D3 C3 79 08 6F 17 DD 03 88 0B 6B 87 21 56 B0 A1 00 C6 D7 11 E7 3C AA 21 F4 06 97 62 80 4A FD 6F 04 42 56 F2 B1 07 0E 15 00 86 C0 CF 98 35 7C CC DC 84 84 D8 E6 C0 67 ED E2 4B 34 D2 47 3E 1D 0E 29 14 6E 64 94 37 60 F9
Exponent	65537
Key Size	1024 bits
Key Usage	Encrypt, Verify, Wrap
Signature	256 bytes : 56 15 F1 FD 19 CB 42 B1 53 70 BC 59 1D E7 8F A4 3E E0 7F 2A CD AC 1C F2 2B 17 87 50 1C 51 2A E3 AB 4A 97 B3 23 DE AD 69 72 E8 02 E6 2B 1B B0 CE 1A 56 52 81 6B 22 54 89 AA D9 DC 96 A0 C9 51 7C 39 9C 57 1A 46 5B 93 7E F8 30 E0 3A D2 93 1A A2 A5 0A 3F 56 E1 43 70 F1 2A 39 DD BB 6F 0E 4E 0C E6 A5 AE C4 95 15 1F 56 49 C0 EF F8 C7 8A 18 80 CB 3E 07 75 D5 88 1F E3 97 2F FF 6F 1E E6 46 E6 95 30 13 00 EC 36 62 84 05 32 33 41 2D 21 E8 E8 D4 A0 31 B0 59 82 45 50 27 44 2C CE F1 F6 1F E6 A6 A5 03 89 CC C8 72 44 0A 48 E2 63 41 AC 8D 8A 32 D4 24 FC C9 B3 C4 A4 61 76 DD A0 50 63 82 5C 0D 3B D9 04 6A 27 78 40 52 71 3B 22 B2 AD 82 0C 60 7C A1 21 26 D9 1F AC AA A5 63 B3 72 91 72 67 13 82 37 A9 DF 6A 17 A6 FE B3 12 3D 21 E9 B4 DF A2 3C 9E 84 3C D4 A1 26 FB 0B 7F 88 CD FB 59 9F

?

OK

Saturday, June 19, 2010

File Edit View History Bookmarks Window Help (3:47) Tu
Welcome to the National Security Agency - NSA/CSS
http://www.nsa.gov/ RSS Google
ências MatemáticaPura CatálogoBiblioUP JSTOR UniversalDigitalLibrary Babylon YouTube Apple Google Maps News (585) Popular

NATIONAL SECURITY AGENCY CENTRAL SECURITY SERVICE

Defending Our Nation. Securing The Future.

SEARCH

INSIDE NSA

Learn more about
What We Do

- Information Assurance
- Signals Intelligence
- Research

Our Mission

The NSA/CSS core missions are to protect U.S. national security systems and to produce foreign signals intelligence information.

LEARN MORE

Today's NSA

- Leadership
- Mission/Vision/Values
- Strategic Plan
- FAQ
- Photo Gallery

Cryptologic Heritage

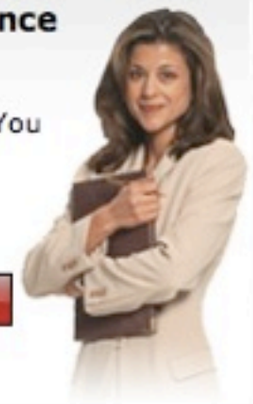
- Center for Cryptologic History
- National Cryptologic Museum
  - Take the virtual tour
- Cryptologic Memorial Wall
- Hall of Honor
- National Vigilance Park

CAREERS AT NSA

Where Intelligence Goes To Work

- Opportunities for You
- Life at NSA
- Benefits

EXPLORE CAREERS



LATEST NSA NEWS

NSA Goes "Greener," Leads the Nation in Recycling Ceiling Tiles

The National Security Agency (NSA) was recognized by Armstrong World Industries (AWI) on December 18 for being the nation's leader in recycling ceiling tiles. NSA started recycling ceiling tiles in September 2008 and processed more than 400,000 ceiling tiles by November 2009.

Read Full Story

DOING BUSINESS WITH NSA

Saturday, June 19, 2010

Where Intelligence Goes to Work

Intelligence. It's the ability to think abstractly. Challenge the unknown. Solve the impossible. And at NSA, it's about protecting the Nation. A career at NSA offers the opportunity to work with the best, shape the course of the world, and secure your own future. Isn't it time to put your intelligence to work?

Mathematics

NSA Mathematicians spend their days focusing on some of today's most distinctive challenges and problems. They apply Number Theory, Group Theory, Finite Field Theory, Linear Algebra, Probability Theory, Mathematical Statistics, Combinatorics, and more. We encourage our Mathematicians to participate in interdisciplinary assignments and train with professionals in such fields as Computer Science and Signals Analysis.

Your education is far from complete when you join NSA. Both formal and informal seminars are routinely organized among our scholars to study specific, timely, Mathematics-related topics, while professional organizations sponsor regular discussions on issues of broader interest.