Elementos de Criptografia Contemporânea

António Machiavelo

Departamento de Matemática Pura da FCUP

10 – 21 de Setembro de 2007

Alguns Usos da Criptografia Contemporânea...

Comunicações militares

Pagamentos e transferências bancárias

Comunicação segura via internet

Assinatura e datação de contractos digitais

Autenticação e certificação de documentos digitais

Eleições electrónicas

...

Futuro (próximo?...)

Dinheiro digital...

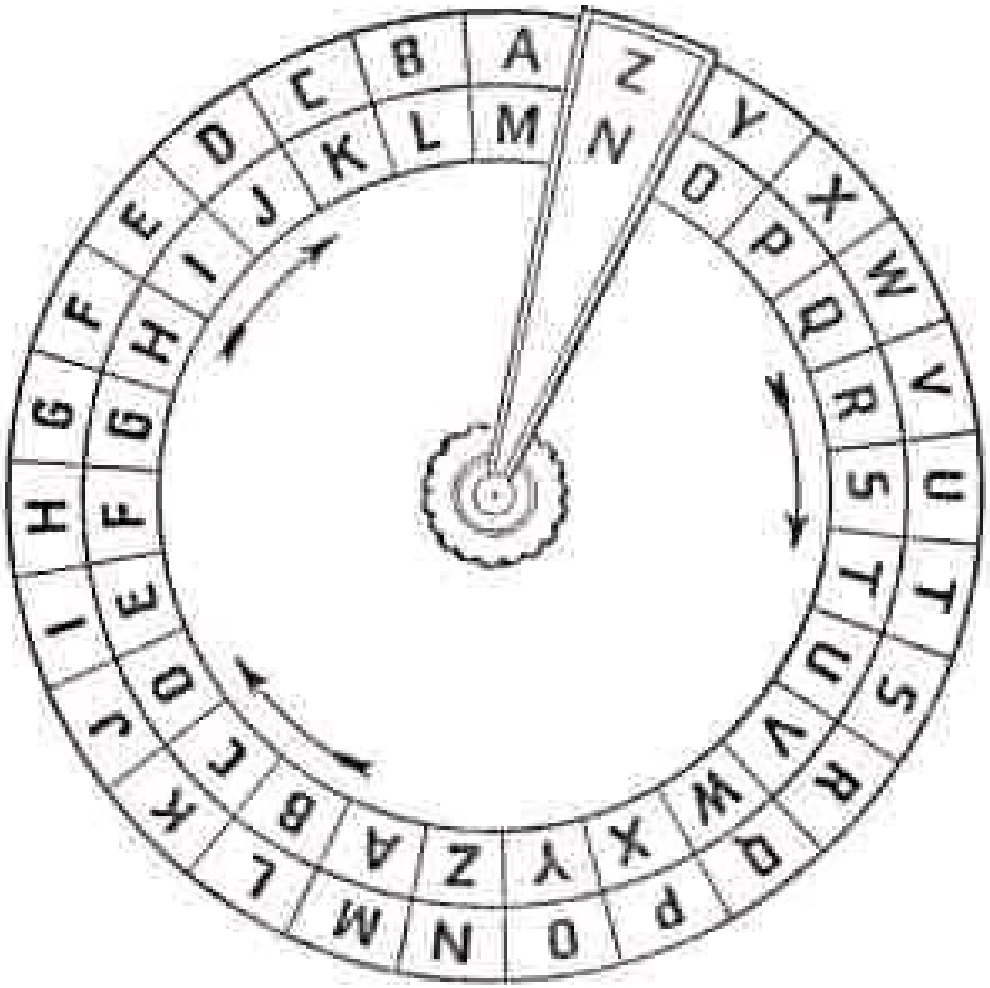
Cifra de César

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

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

MATEMÁTICA → PDWHPDWLFD

JÚLIO ← MXOLR



CODE WHEEL FOR REVERSE CODES

Disco de codificação/descodificação de Leon Battista **Alberti** (1404 - 1472)

Cifra de Substituição

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

CRIPTOGRAFIA → **T X SUFYJXHBSH**

HOJE ← **NYCG**

Há:

26 x **25** x ... x **3** x **2** x **1** = 403291461126605635584000000

~ 4 x 10^26

chaves para a cifra de substituição...

Testando 1 milhão por segundo demorar-se-ia...

...mais de 6,39 x 10^12 anos a testar metade das chaves !!!

Idade do Universo (desde Big Bang)**:**

"apenas" cerca de 1,4 x 10^10 anos...

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

ESTATÍSTICAS...

Português		Espanhol		Inglês		Francês	
A	13,8	A	12,7	A	7,8	A	9,4
B	0,9	B	1,4	B	1,3	B	1,0
C	4,5	C	3,9	C	2,9	C	2,6
D	5,6	D	5,6	D	4,1	D	3,4
E	12,0	E	13,2	E	13,1	E	15,9
F	1,0	F	0,5	F	2,9	F	1,0
G	1,2	G	1,1	G	1,4	G	1,0
H	0,6	H	1,2	H	5,9	H	0,8
I	7,0	I	6,3	I	6,8	I	8,4
J	0,3	J	0,6	J	0,2	J	0,9
K	0,0	K	0,0	K	0,4	K	0,0
L	2,8	L	5,9	L	3,6	L	5,3
M	4,1	M	2,7	M	2,6	M	3,2
N	5,3	N	7,0	N	7,3	N	7,2
O	10,8	O	9,5	O	8,2	O	5,1
P	2,9	P	2,4	P	2,2	P	2,9
Q	0,8	Q	1,2	Q	0,1	Q	1,1
R	6,9	R	6,3	R	6,6	R	6,5
S	7,8	S	7,6	S	6,5	S	7,9
T	4,9	T	3,9	T	9,0	T	7,3
U	3,8	U	4,6	U	2,8	U	6,2
V	1,3	V	1,1	V	1,0	V	2,2
W	0,0	W	0,0	W	1,5	W	0,0
X	0,2	X	0,1	X	0,3	X	0,3
Y	0,0	Y	1,1	Y	1,5	Y	0,2
Z	0,3	Z	0,3	Z	0,1	Z	0,3

Cripto-análise

Frequência das letras na língua portuguesa		Frequência das letras no criptograma		
A	13,8	A	0 (0.)	
B	0,9	B	15 (1.58)	
C	4,5	C	9 (.947)	
D	5,6	D	18 (1.89)	
E	12,0	E	57 (6.00)	R ?
F	1,0	F	48 (5.05)	
G	1,2	G	0 (0.)	
H	0,6	H	13 (1.37)	
I	7,0	I	128 (13.5)	A, E ?
J	0,3	J	0 (0.)	
K	0,0	K	20 (2.11)	
L	2,8	L	39 (4.11)	
M	4,1	M	0 (0.)	
N	5,3	N	70 (7.37)	S ?
O	10,8	O	30 (3.16)	
P	2,9	P	127 (13.4)	E, A ?
Q	0,8	Q	112 (11.8)	O ?
R	6,9	R	2 (.211)	
S	7,8	S	48 (5.05)	
T	4,9	T	52 (5.47)	
U	3,8	U	38 (4.00)	
V	1,3	V	17 (1.79)	
W	0,0	W	38 (4.00)	
X	0,2	X	53 (5.58)	R ?
Y	0,0	Y	16 (1.68)	
Z	0,3	Z	0 (0.)	

Digramas mais frequentes (em permilagem)

	0	1	2	3	4	5	6	7	8	9	10
es	21.4	7.37	8.41	8.78	8.73	10.53	9.17	9.49	9.76	9.89	9.53
de	21.35	2.87	10.93	5.61	6.67	7.37	6.02	7.06	6.97	7.06	7.46
os	17.67	7.67	9.63	8.36	8.05	8.73	8.98	8.57	8.68	9.02	9.34
ra	17.28	10.19	9.25	9.33	8.28	10.92	9.52	9.77	9.56	10.08	9.25
as	16.13	8.68	11.66	11.64	9.57	10.13	10.23	10.03	10.14	10.23	10.31
do	15.53	1.85	7.76	4.87	4.95	7.2	5.78	6.37	7.27	6.48	6.33
ad	15.44	9.05	6.07	8.22	6.69	8.1	7.94	7.97	7.87	8.69	7.67
en	14.79	4.48	7.13	7.07	6.83	7.07	6.79	6.95	6.14	6.83	7.37
ar	14.14	5.81	10.68	9.61	9.86	10.12	9.61	9.7	9.05	9.49	9.12
re	14.14	6.11	8.11	9.19	8.45	8.19	7.59	8.79	8.11	8.14	7.83
co	14.01	7.04	5.09	7.08	4.21	5.38	5.37	4.27	4.61	4.85	5.08
se	13.96	11.97	8.66	10.45	9.49	8.79	10.12	9.16	8.79	9.9	8.79
er	13.19	6.51	10.72	9.25	7.02	8.99	8.29	8.62	8.42	8.37	8.62
nt	13.17	1.3	1.72	3.09	2.81	3.09	2.6	2.62	2.86	3.16	2.81
ca	12.86	4.04	6.11	6.09	5.72	5.88	6	5.74	6.09	6.29	6.33
da	12.63	5.32	8.56	5.15	8.08	7.76	7.46	8.47	7.39	7.57	7.44
or	12.55	5.59	9.86	7.74	8.8	7.31	7.81	7.95	7.29	7.44	7.64
te	12.49	2.78	5.96	6.09	5.52	6.39	6.19	5.91	5.89	5.66	5.84
ao	12.06	18.49	18.16	10.99	15.8	12.12	14.06	14.29	15.51	15.16	16.39
an	11.71	3.65	8.05	8.1	7.22	8.23	6.32	7.5	7.41	7.08	7.46
on	11.23	3.27	6.55	6.12	5.83	6.4	6.48	6.53	5.55	6.32	5.86
ta	10.91	5.28	9.75	7.13	6.81	6.21	6.49	6.49	6.85	6.76	7.18
ma	10.76	2.64	4.3	5.18	6.05	5.61	5.54	5.13	5.18	5.44	5.33
od	10.67	4.9	4.82	6.23	5.12	6.6	6.48	7.06	6.63	6.46	6.57
em	10.54	3.51	4.85	4.71	4.57	4.86	4.4	4.81	5.41	5.03	4.92
ac	10.19	4.87	4.63	6.84	5.83	7.16	5.88	7.03	6.93	6.24	5.77
sa	9.66	12.4	7.16	11.71	9.66	10.92	11.01	10.96	10.13	10.72	10.63
st	9.63	1.2	4.77	3.94	4.24	4.26	3.71	3.47	3.74	3.92	3.97
to	9.51	2.82	7.58	6.11	5.17	5.97	5.37	5.26	5.4	5.35	5.51
ro	9.02	7.73	6.65	8.56	7.8	8.33	7.83	8.41	7.18	7.86	8.03
na	9.01	7.6	8.06	7.36	8.04	7.96	6.74	7.63	7.82	7.55	7.72

português

percentagem)

A	13.86
B	0.99
C	4.48
D	5.58
E	12.07
F	1.05
G	1.26
H	0.71
I	6.98
J	0.35
K	0.08
L	2.87
M	4.14
N	5.38
O	10.86
P	2.91
Q	0.84
R	6.95
S	7.83
T	4.95
U	3.85
V	1.34
W	0.05
X	0.24
Y	0.05
Z	0.33

Cripto-análise...

I --> E
P --> A
Q -->O
N --> S
X --> R
T" --> M

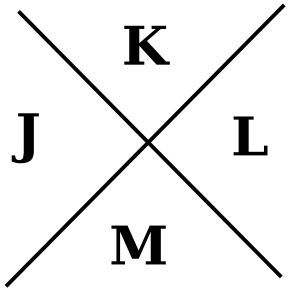
E-ES- AOSA- EM-EM SO--A M--EO SO--O E-MA- O-S-A --E-A ---A-
AO-O- -RE-A E-E-- ---A- OMOO- -RA-O -SA-- A---E R-OMO ES-A-
E-RA- ---E- -AEM- -EMES E--OE -ES-A -SO-O MOES- ER--E -ROMA
-SOEM SERE- OSSO- RESSA --OS- OMOES -ES-- --E-R OSA-- OS--E
EM-ER -EEO- ROSEA ---AM -OMOE S-ASA -ES-- E-R-- AMEM- E-E-E
-RAS- EA--- E-ES- AOSA- EM--E OSO-- OE--- -OEES --MAE -ERME
--O-- ----- OA-A- REESE -E--O -E-O- ---O- O---A ---O- -E-OS
SAA-R A-ES- E---O --M-E R-E-- OMO-- ME--O E-ES- AOSA- EM--E
OSO-- OE-E- AE-OR E---- E--AS E--S- E-A-- -E-AR -OEMO ---A-
--RA- ---A- --O-E -A-E- RA--O --RA- O--OS ---O- -AMAS -ARA-
RE-AM A--A- -EERE -OR-A -EA-- --M-S -AMA- A-OM- --O-- S-A--
EROSA -OS-E --OS- --A-- E-ARA -E-A- ----E ---S- A--EE -A-O-
A-OAE S-ERA --AO- RO-A- E-AMA R--M- -ORE- E-EES -A-A- --M-A
S---O R-ASS O-E-A --A-O -OM-- -AEAR -E--- M-ASS ARO-A -OA-O
RA-AR ARA-O S-O-O MO--- A-AR- O-E-R OA-ES ---AA --O-O R-O-E
RA-OR A--SA O-OA- OMORA -AR-- -RASO M-E-E --SAO -ESEM -AR--
EEM-O --E-A O-AS- -ER-- --E-- -ARE- ES-AO SA-EM -EMSO --AM-
-EOSO --O-O MA--A A---A --ESE M-RE- -E-M- OMEMS O--AO M---O
---AE A-A-- A-OMO -O-A- O-OR- -AE-- REASM AOS-E -MA-R -A--A

Mensagem Original:

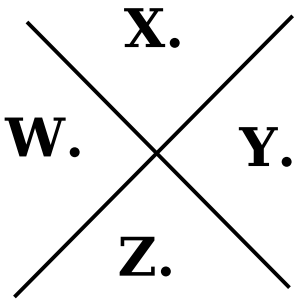
**ELESN AOSAB EMNEM SONHA MQUEO SONHO EUMAC ONSTA NTEDA VIDAT
AOCON CRETA EDEFI NIDAC OMOOU TRACO ISAQU ALQUE RCOMO ESTAP
EDRAC INZEN TAEMQ UEMES ENTOE DESCA NSOCO MOEST ERIBE IROMA
NSOEM SEREN OSSOB RESSA LTOSC OMOES TESPI NHEIR OSALT OSQUE
EMVER DEEOI ROSEA GITAM COMOE STASA VESQU EGRIT AMEMB EBEDE
IRASD EAZUL ELESN AOSAB EMQUE OSONH OEVIN HOEES PUMAE FERME
NTOBI CHINH OALAC REESE DENTO DEFOC INHOP ONTIA GUDOQ UEFOS
SAATR AVESD ETUDO NUMPE RPETU OMOVI MENTO ELESN AOSAB EMQUE
OSONH OETEL AECOR EPINC ELBAS EFUST ECAPI TELAR COEMO GIVAV
ITRAL PINAC ULODE CATED RALCO NTRAP ONTOS INFON IAMAS CARAG
REGAM AGIAQ UEERE TORTA DEALQ UIMIS TAMAP ADOMU NDODI STANT
EROSA DOSVE NTOSI NFANT ECARA VELAQ UINHE NTIST AQUEE CABOD
ABOAE SPERA NCAOU ROCAN ELAMA RFIMF LORET EDEES PADAC HIMBA
STIDO RPASS ODEDA NCACO LOMBI NAEAR LEQUI MPASS AROLA VOADO
RAPAR ARAIO SLOCO MOTIV ABARC ODEPR OAFES TIVAA LTOFO RNOGE
RADOR ACISA ODOAT OMORA DARUL TRASO MTELE VISAO DESEM BARQU
EEMFO GUETA ONASU PERFI CIELU NAREL ESNAO SABEM NEMSO NHAMQ
UEOSO NHOCO MANDA AVIDA QUESE MPREQ UEUMH OMEMS ONHAO MUNDO
PULAE AVANC ACOMO BOLAC OLORI DAENT REASM AOSDE UMACR IANCA**

Outra Cifra...

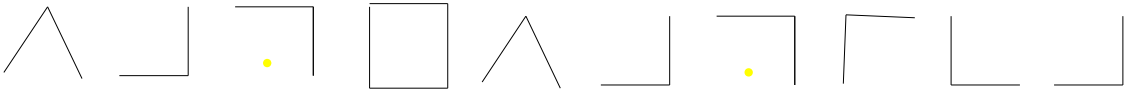
A	B	C
D	E	F
G	H	I



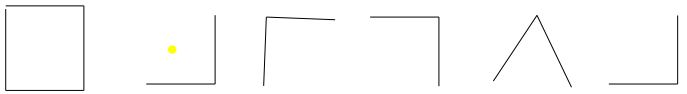
N.	O.	P.
Q.	R.	S.
T.	U.	V.



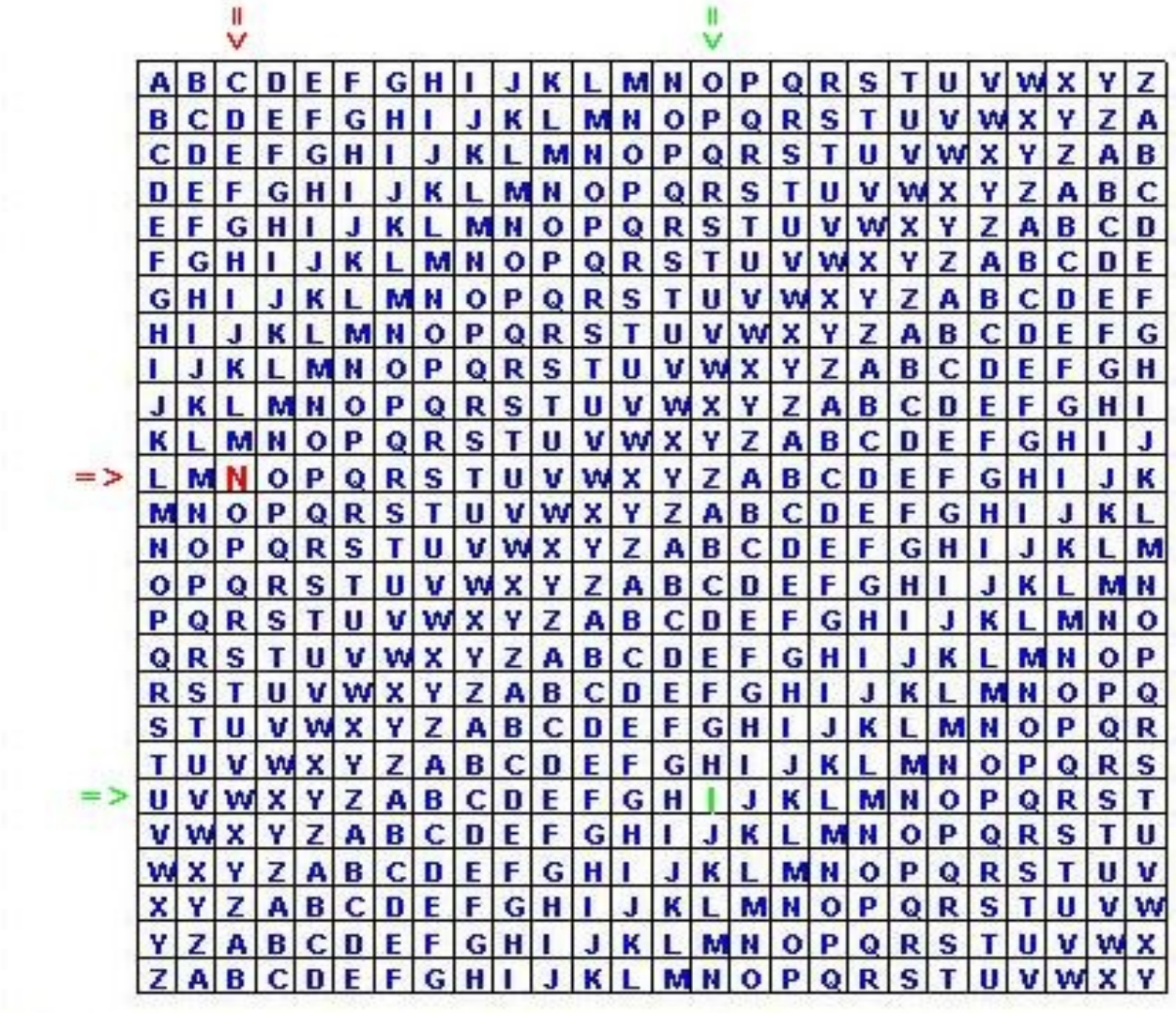
MATEMÁTICA →



ENIGMA ←



Cifra de Vigenère



Chave:

LUCIFER

L U C I F E R L U C I F E R L U C I F E R L U C I F E

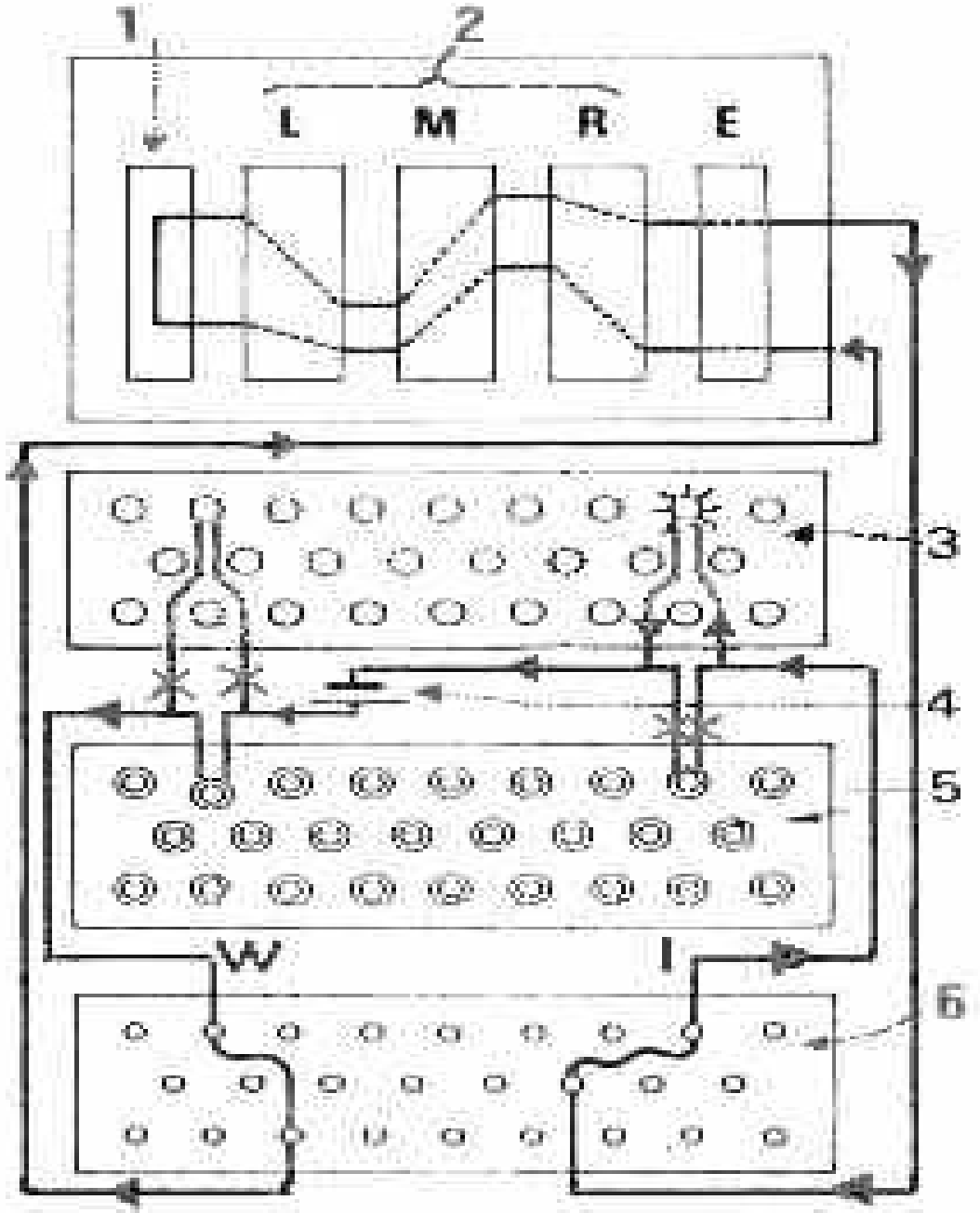
C O M B A T E I N T E N S O N A F R E N T E O E S T E

N I O J F X V T H V M S W F Y U H Z J R K P I G A Y I

ENIGMA

ENIGMA

Esboço do interior de uma ENIGMA



A “Chave” na cifra Enigma

Geheim!

Nicht ins Flugzeug mitnehmen!

Sonder-Maschinenschlüssel BGT

Datum	Walzenlage			Ringstellung			Steckerverbindungen										Kenngruppe		
31.	I	V	III	06	20	24	UA	PF	RQ	SO	NI	EY	BG	HL	TX	ZJ	jeu	nyq	aqm
30.	V	II	III	01	07	12	GF	KV	JM	IB	UW	LX	TD	QS	NA	ZH	azs	zds	kck
29.	IV	I	V	11	17	26	CI	OK	PV	ZL	HX	NB	AW	DJ	FE	ST	kap	gwh	lyx

A ARMA MAIS SECRETA...

Bletchley Park

Alan Turing (1912 - 1954)

A internet...

Os Problemas:

(1) Distribuição de chaves:

Como trocar chaves por um canal que não é seguro?

(2) Assinaturas digitais:

Como assinar documentos sem as partes envolvidas estarem presentes no mesmo local?

Merkle, Hellman & Diffie

Ralph Merkle
(1952)

Martin Hellman
(1945)

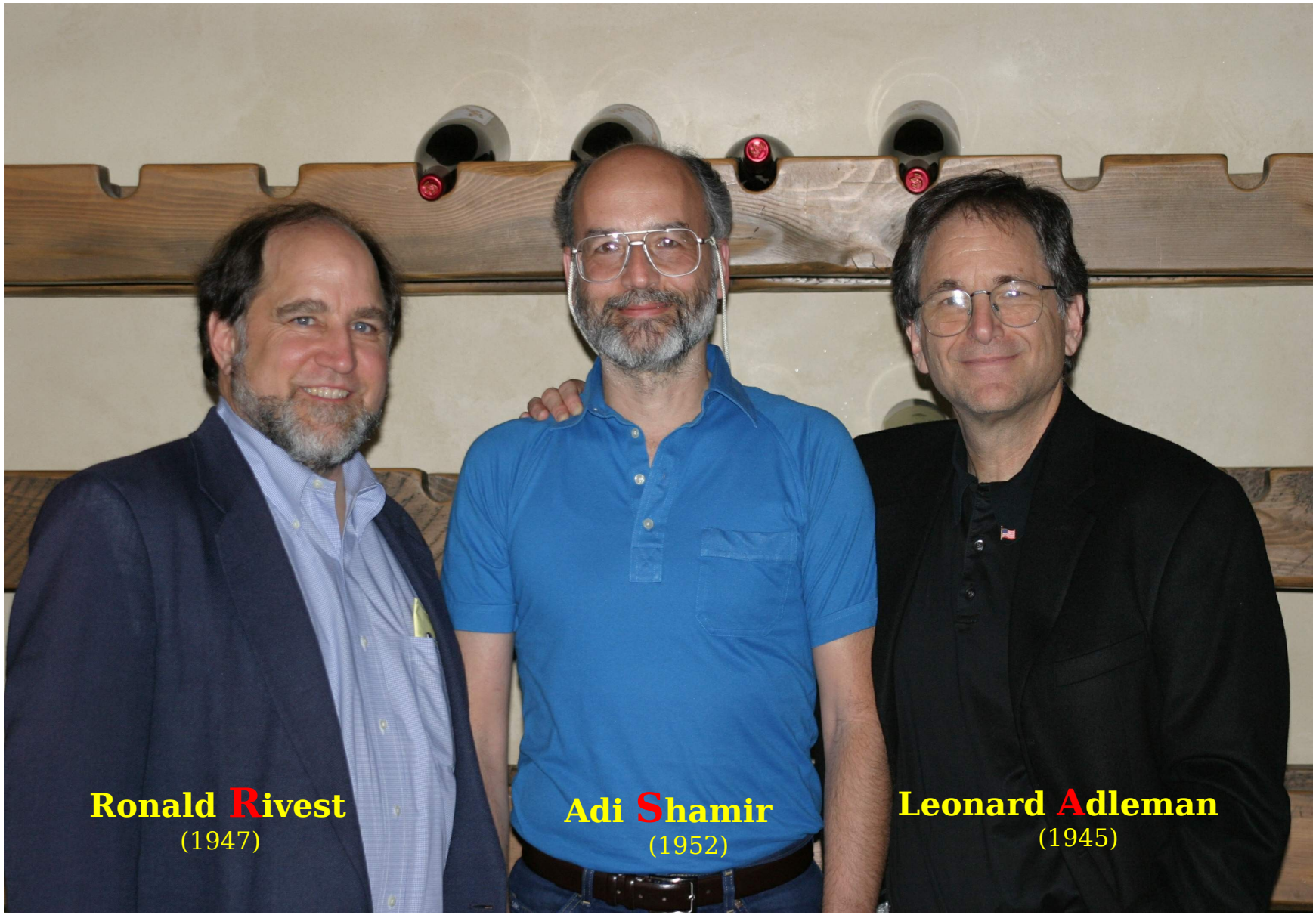
Whitfield Diffie
(1944)

«Estamos hoje à beira de uma revolução em criptografia. O desenvolvimento de “hardware” digital barato libertou-nos das limitações da computação mecânica e tornou o custo de dispositivos criptográficos acessível a aplicações comerciais tão remotas quanto máquinas para levantar dinheiro e terminais de computador. Por seu lado, tais aplicações criam a necessidade para novos tipos de sistemas criptográficos que minimizem a necessidade de canais de distribuição de chaves seguras e forneçam o equivalente a um assinatura escrita. Simultaneamente, avanços teóricos em teoria da informação e ciência dos computadores dão indícios de vir a fornecer sistemas comprovadamente seguros, transformando esta arte antiga numa ciência.»

Whitfield Diffie & Martin E. Hellman,
“New Directions in Cryptography”,
IEEE Transactions on Information Theory 22 (1976), 644-654

RSA (fins dos anos 70...)

RSA...em 2003



«A era do “correio electrónico” pode em breve ser uma realidade; devemos assegurar que duas propriedades importantes do sistema de “correio em papel” sejam preservadas: (a) as mensagens sejam privadas, e (b) as mensagens possam ser assinadas. Demonstramos neste artigo como construir estas capacidades num sistema de correio electrónico.»

Rivest, Shamir, and Adleman,
“A Method for Obtaining Digital Signatures and Public-Key Cryptosystems”,
Communications of the ACM **21** (1978), 120-126.

Números Primos...

Número Primo: Número natural, maior que um, que não pode ser escrito como um produto de números menores.

Os 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, ... há uma infinidade !!!

2^{32 582 657} - 1, um número com 9 808 358 algarismos, é o maior primo hoje conhecido, um recorde que pertence ao grupo GIMPS, e foi descoberto em 4 de Setembro de 2006.

Getting Started
Main page
How it works
Download
FAQ
Benchmarks
Prizes
Project Status
Status
Top producers
PrimeNet

GIMPS

The Great Internet Mersenne Prime Search

Finding 10 World Record Primes!

2^P-1 MAY BE PRIME!

Learning More
History
The math
Source code
Mailing list
Miscellaneous
Manual testing
Credits
Links
Feedback
Other projects

GIMPS Home Page

September 2006: New Mersenne Prime!

Pages available in Chinese, Danish, Dutch, French, German, Italian, and Spanish. Warning: These translations may not be up-to-date - use AltaVista as necessary.

44th Known Mersenne Prime Found!!

Lightning strikes twice. On September 4, 2006, in the same room just a few feet away from their last find, Dr. Curtis Cooper and Dr. Steven Boone's CMSU team broke their own world record, discovering the 44th known Mersenne prime, $2^{32,582,657}$-1. The new prime at 9,808,358 digits is 650,000 digits larger than their previous record prime found last December. However, the new prime falls short of the 10 million digits required for GIMPS to claim the Electronic Frontier Foundation $100,000 award.

With five record primes found in less than 3 years, GIMPS has been on an incredible lucky streak. Never before have Mersenne primes been bunched so closely together. When looking at the exponents, we expect only 1.78 Mersenne primes between powers of two, and prior to 2003, a maximum of 3 Mersenne primes were found between powers of two. The last 5 Mersenne prime exponents all fell between 2^{24} and 2^{25} -- and we haven't finished testing all the exponents in that range!

The new prime was independently verified in 6 days by Tony Reix of Bull S.A. in Grenoble, France using 16 Itanium2 1.5 GHz CPUs of a Bull NovaScale 6160 HPC at Bull Grenoble Research Center, running the Glucas program by Guillermo Ballester Valor of Granada, Spain.

Uma assimetria importante...

Primalidade: Há algoritmos “rápidos” de verificar se um número é ou não primo.

Factorização: Não são conhecidos algoritmos “rápidos” para factorizar números compostos “genéricos”.

Por exemplo:

Sabe-se que o número

2^(2^14) +1 (Tem 4933 algarismos...)

é composto mas não se conhece nenhum seu factor...

Outro exemplo:

2^739 – 1 = 184603056517613273120809 x
4805068358409200438080546379011 1 x **C168**

Descrição sumária da cifra RSA

Sejam p e q dois números primos "grandes" (~300 algarismos...)

Considere-se $n = p \times q$

Encontre-se um número c que não tenha factores comuns com o número $(p-1) \times (q-1)$

Calcule-se (usando o "Algorimo de Euclides") **"o" número d tal que o número $c \times d$ deixe resto igual a 1 quando dividido por $(p-1) \times (q-1)$**

n , c públicos **d privado**

M = (bloco de) **uma mensagem a transmitir** (numa forma numérica)

Calcule-se C= resto da divisão de $M\hat{}c$ por n

É C que é enviada...

Receptor calcula resto da divisão de $C\hat{}d$ por n e recupera mensagem original, M.

Com o RSA não é necessário compartilhar segredos!

Alice cria a sua cifra RSA: $\mathbf{n_A}$, $\mathbf{c_A}$; $\mathbf{d_A}$ e publica $\mathbf{n_A}$ e $\mathbf{c_A}$, mantendo $\mathbf{d_A}$ secreto.

Bruno cria a sua cifra RSA: $\mathbf{n_B}$, $\mathbf{c_B}$; $\mathbf{d_B}$ e publica $\mathbf{n_B}$ e $\mathbf{c_B}$, mantendo $\mathbf{d_B}$ secreto.

Para comunicarem, cada um usa a cifra do outro...

A única maneira de três pessoas compartilharem um segredo...

... é se duas delas estiverem mortas!

Benjamin Franklin

Como provar que se tem um número de identificação sem o mostrar!

Alice cria uma cifra RSA: $\mathbf{n_A}$, $\mathbf{c_A}$; $\mathbf{d_A}$.

Alice publica $\mathbf{n_A}$ e $\mathbf{c_A}$; mantém $\mathbf{d_A}$ secreto.

Para se assegurar da identidade de **Alice**, **Bruno** codifica uma mensagem **M** com a cifra de **Alice** e envia-lhe o resultado, **C**.

Alice, **prova** que tem $\mathbf{d_A}$ descodificando **C** e enviando **M** a **Bruno**, que fica assim com a garantia da identidade de **Alice** sem que esta tenha mostrado o seu número de identificação!

Assinaturas digitais com o RSA

$\mathfrak{C}_A(\mathbf{M})$ = criptograma obtido quando se cifra a mensagem **M** com a chave pública da **Alice**, $\mathbf{c}_A$ (… **e** $\mathbf{n}_A$).

$\mathcal{D}_A(\mathbf{C})$= mensagem que **Alice** obtém quando decifra o "criptograma" **C** com a sua chave privada, $\mathbf{d}_A$ (… **e** $\mathbf{n}_A$).

$\mathfrak{C}_A$ e $\mathcal{D}_A$ *são operações inversas…*

Alice assina a mensagem **M**, calculando $\mathbf{A} = \mathcal{D}_A(\mathbf{M})$ (!)

Alice envia $\mathbf{C} = \mathfrak{C}_B(\mathbf{M})$ e **A** ao **Bruno**.

Bruno pode ler a mensagem e a assinatura de **Alice** calculando:

$\mathcal{D}_B(\mathbf{C})$ e $\mathfrak{C}_A(\mathbf{A})$ …

Bibliografia

F. L. Bauer, **Decrypted Secrets**, Springer 2002 [3ª edição].

A. Beutelspacher, **Cryptology**, MAA 1994.

Niels Ferguson & Bruce Shneier, **Practical Cryptography**, Wiley, 2003.

Martin Gardner, **Codes, Ciphers and Secret Writing**, Simon & Schuster, 1972.
[reeditado pela Dover em 1984]

David Kahn, **The Codebreakers**, The Macmillan Co., 1967. [reeditado pela Scribner em 1996]

Bruce Shneier, **Applied Cryptography**, Wiley, 1996 [2nd edition].

Simon Singh, **O Livro dos Códigos**, Temas e Debates, 1999.

Páginas na WWW

RSA Laboratories: **http://www.rsasecurity.com/rsalabs/**

Decoding Nazi Secrets (NOVA - PBS): **http://www.pbs.org/wgbh/nova/decoding/**

Bletchley Park - Station X: **http://www.bletchleypark.org.uk/**

The Principle of the Enigma (Tony Sale) :
http://www.codesandciphers.org.uk/enigma/enigma1.htm

DES (**D**ata **E**ncryption **S**tandard): 1977 -- 2002

Uma Cifra de Feistel (Hosrt Feistel [1915—1990], criador da cifra LUCIFER, “ancestral” do DES) **é uma cifra que encripta uma mensagem de 2t bits (L_0,R_0) constituída por dois blocos, L_0,R_0, com t-bits cada, num criptograma (L_r,R_r) através de um processo envolvendo r etapas, e onde, para $0 \leq i \leq r$, a i-ésima etapa envia**

$$(L_{i-1},R_{i-1}) \text{ ---- } (K_i) \text{ ----> } (L_i,R_i)$$

da seguinte forma:

$$L_i := R_{i-1}$$

$$R_i := L_{i-1} \oplus f(R_{i-1},K_i),$$

onde cada subchave K_i é obtida da chave inicial K da cifra em questão, por um determinado processo.

DES (**D**ata **E**ncryption **S**tandard): 1977 -- 2002

Aprovado pelo NIST (National Institute of Standards and Technology) para uso na transmissão de documentos/informação confidenciais pelos departamentos e agências federais dos EUA.

Solicitado: Maio de 1973

Revisto e Reconfirmado: 1983, 1988, 1993, 1999.

7.82 Algorithm Data Encryption Standard (DES)

INPUT: plaintext $m_1 \dots m_{64}$; 64-bit key $K = k_1 \dots k_{64}$ (includes 8 parity bits).
OUTPUT: 64-bit ciphertext block $C = c_1 \dots c_{64}$. (For decryption, see Note 7.84.)

1. (key schedule) Compute sixteen 48-bit round keys K_i from K using Algorithm 7.83.
2. $(L_0, R_0) \leftarrow \text{IP}(m_1 m_2 \dots m_{64})$. (Use IP from Table 7.2 to permute bits; split the result into left and right 32-bit halves $L_0 = m_{58} m_{50} \dots m_8$, $R_0 = m_{57} m_{49} \dots m_7$.)
3. (16 rounds) for i from 1 to 16, compute L_i and R_i using Equations (7.4) and (7.5) above, computing $f(R_{i-1}, K_i) = P(S(E(R_{i-1}) \oplus K_i))$ as follows:
   (a) Expand $R_{i-1} = r_1 r_2 \dots r_{32}$ from 32 to 48 bits using E per Table 7.3: $T \leftarrow E(R_{i-1})$. (Thus $T = r_{32} r_1 r_2 \dots r_{32} r_1$.)
   (b) $T' \leftarrow T \oplus K_i$. Represent T' as eight 6-bit character strings: $(B_1, \dots, B_8) = T'$.
   (c) $T'' \leftarrow (S_1(B_1), S_2(B_2), \dots S_8(B_8))$. (Here $S_i(B_i)$ maps $B_i = b_1 b_2 \dots b_6$ to the 4-bit entry in row r and column c of S_i in Table 7.8, page 260 where $r = 2 \cdot b_1 + b_6$, and $b_2 b_3 b_4 b_5$ is the radix-2 representation of $0 \le c \le 15$. Thus $S_1(011011)$ yields $r = 1$, $c = 13$, and output 5, i.e., binary 0101.)
   (d) $T''' \leftarrow P(T'')$. (Use P per Table 7.3 to permute the 32 bits of $T'' = t_1 t_2 \dots t_{32}$, yielding $t_{16} t_7 \dots t_{25}$.)
4. $b_1 b_2 \dots b_{64} \leftarrow (R_{16}, L_{16})$. (Exchange final blocks L_{16}, R_{16}.)
5. $C \leftarrow \text{IP}^{-1}(b_1 b_2 \dots b_{64})$. (Transpose using IP^{-1} from Table 7.2; $C = b_{40} b_8 \dots b_{25}$.)

IP							
58	50	42	34	26	18	10	2
60	52	44	36	28	20	12	4
62	54	46	38	30	22	14	6
64	56	48	40	32	24	16	8
57	49	41	33	25	17	9	1
59	51	43	35	27	19	11	3
61	53	45	37	29	21	13	5
63	55	47	39	31	23	15	7

IP^{-1}							
40	8	48	16	56	24	64	32
39	7	47	15	55	23	63	31
38	6	46	14	54	22	62	30
37	5	45	13	53	21	61	29
36	4	44	12	52	20	60	28
35	3	43	11	51	19	59	27
34	2	42	10	50	18	58	26
33	1	41	9	49	17	57	25

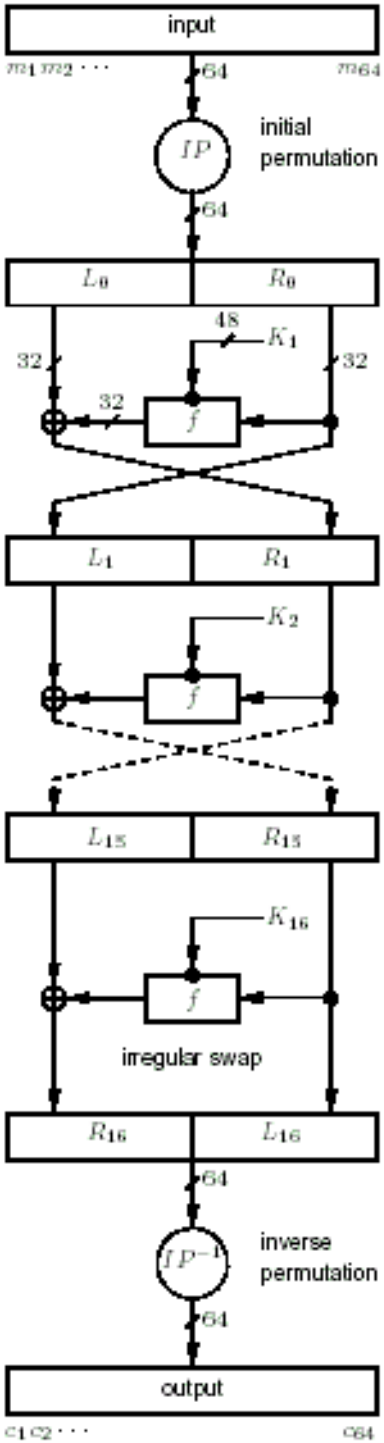
Table 7.2: *DES initial permutation and inverse (IP and IP^{-1}).*

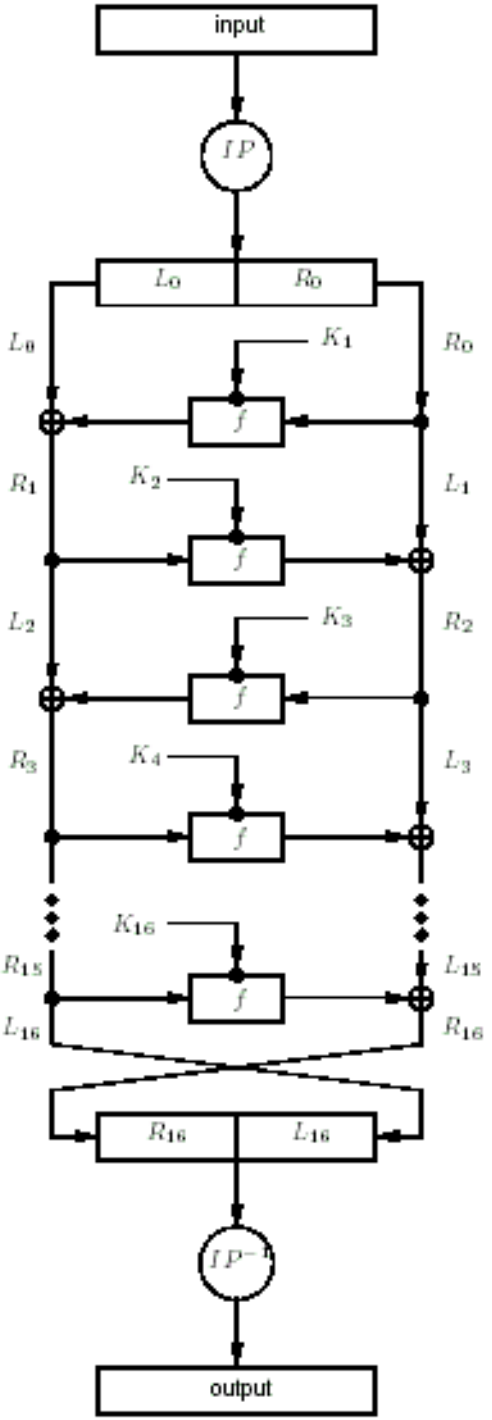
E					
32	1	2	3	4	5
4	5	6	7	8	9
8	9	10	11	12	13
12	13	14	15	16	17
16	17	18	19	20	21
20	21	22	23	24	25
24	25	26	27	28	29
28	29	30	31	32	1

P			
16	7	20	21
29	12	28	17
1	15	23	26
5	18	31	10
2	8	24	14
32	27	3	9
19	13	30	6
22	11	4	25

Table 7.3: *DES per-round functions: expansion E and permutation P.*

IP = (1 58 55 13 28 40) (2 50 53 29 32 8) (3 42 51 45 27 48)
(4 34 49 61 31 16) (6 18 54 21 30 24) (7 10 52 37 25 64)
(11 44 35 41 59 47) (12 36 33 57 63 15) (14 20 38 17 62 23)
(5 26 56) (9 60 39) (19 46) (22) (43)





$L_i = R_{i-1}$

$R_i = L_{i-1} \oplus f(R_{i-1}, K_i)$

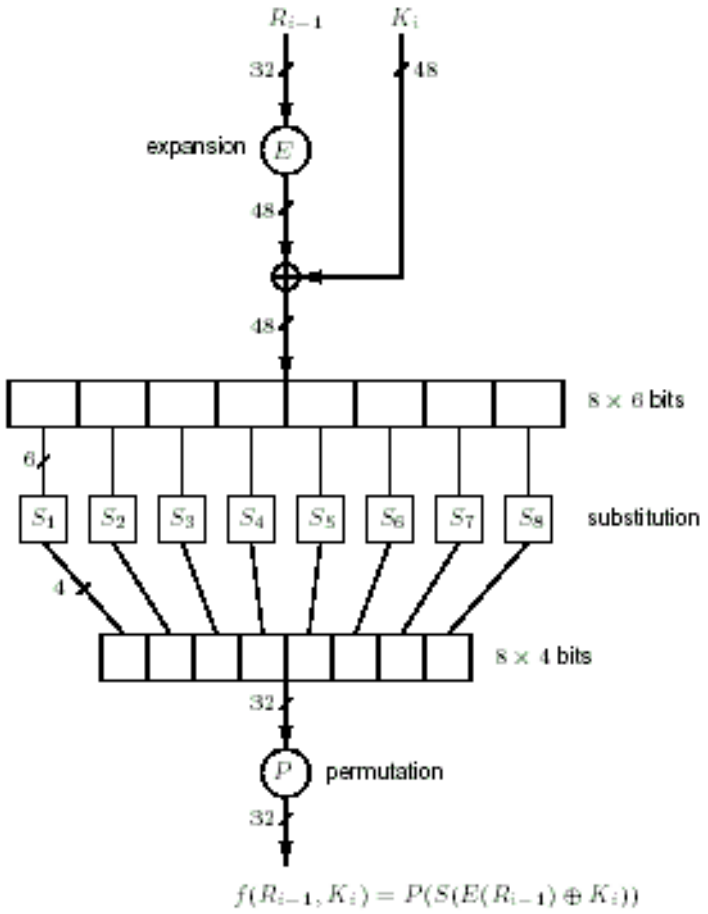


Figure 7.10: DES inner function f.

row	column number															
	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15
S_1																
0	14	4	13	1	2	15	11	8	3	10	6	12	5	9	0	7
1	0	15	7	4	14	2	13	1	10	6	12	11	9	5	3	8
2	4	1	14	8	13	6	2	11	15	12	9	7	3	10	5	0
3	15	12	8	2	4	9	1	7	5	11	3	14	10	0	6	13
S_2																
0	15	1	8	14	6	11	3	4	9	7	2	13	12	0	5	10
1	3	13	4	7	15	2	8	14	12	0	1	10	6	9	11	5
2	0	14	7	11	10	4	13	1	5	8	12	6	9	3	2	15
3	13	8	10	1	3	15	4	2	11	6	7	12	0	5	14	9
S_3																
0	10	0	9	14	6	3	15	5	1	13	12	7	11	4	2	8
1	13	7	0	9	3	4	6	10	2	8	5	14	12	11	15	1
2	13	6	4	9	8	15	3	0	11	1	2	12	5	10	14	7
3	1	10	13	0	6	9	8	7	4	15	14	3	11	5	2	12
S_4																
0	7	13	14	3	0	6	9	10	1	2	8	5	11	12	4	15
1	13	8	11	5	6	15	0	3	4	7	2	12	1	10	14	9
2	10	6	9	0	12	11	7	13	15	1	3	14	5	2	8	4
3	3	15	0	6	10	1	13	8	9	4	5	11	12	7	2	14
S_5																
0	2	12	4	1	7	10	11	6	8	5	3	15	13	0	14	9
1	14	11	2	12	4	7	13	1	5	0	15	10	3	9	8	6
2	4	2	1	11	10	13	7	8	15	9	12	5	6	3	0	14
3	11	8	12	7	1	14	2	13	6	15	0	9	10	4	5	3
S_6																
0	12	1	10	15	9	2	6	8	0	13	3	4	14	7	5	11
1	10	15	4	2	7	12	9	5	6	1	13	14	0	11	3	8
2	9	14	15	5	2	8	12	3	7	0	4	10	1	13	11	6
3	4	3	2	12	9	5	15	10	11	14	1	7	6	0	8	13
S_7																
0	4	11	2	14	15	0	8	13	3	12	9	7	5	10	6	1
1	13	0	11	7	4	9	1	10	14	3	5	12	2	15	8	6
2	1	4	11	13	12	3	7	14	10	15	6	8	0	5	9	2
3	6	11	13	8	1	4	10	7	9	5	0	15	14	2	3	12
S_8																
0	13	2	8	4	6	15	11	1	10	9	3	14	5	0	12	7
1	1	15	13	8	10	3	7	4	12	5	6	11	0	14	9	2
2	7	11	4	1	9	12	14	2	0	6	10	13	15	3	5	8
3	2	1	14	7	4	10	8	13	15	12	9	0	3	5	6	11

Table 7.8: DES S-boxes.

7.83 Algorithm DES key schedule

INPUT: 64-bit key $K = k_1 \ldots k_{64}$ (including 8 odd-parity bits).
OUTPUT: sixteen 48-bit keys K_i, $1 \leq i \leq 16$.

1. Define v_i, $1 \leq i \leq 16$ as follows: $v_i = 1$ for $i \in \{1, 2, 9, 16\}$; $v_i = 2$ otherwise. (These are left-shift values for 28-bit circular rotations below.)
2. $T \leftarrow \text{PC1}(K)$; represent T as 28-bit halves (C_0, D_0). (Use PC1 in Table 7.4 to select bits from K: $C_0 = k_{57}k_{49} \ldots k_{36}$, $D_0 = k_{63}k_{55} \ldots k_4$.)
3. For i from 1 to 16, compute K_i as follows: $C_i \leftarrow (C_{i-1} \hookleftarrow v_i)$, $D_i \leftarrow (D_{i-1} \hookleftarrow v_i)$, $K_i \leftarrow \text{PC2}(C_i, D_i)$. (Use PC2 in Table 7.4 to select 48 bits from the concatenation $b_1 b_2 \ldots b_{56}$ of C_i and D_i: $K_i = b_{14} b_{17} \ldots b_{32}$. '$\hookleftarrow$' denotes left circular shift.)

PC1						
57	49	41	33	25	17	9
1	58	50	42	34	26	18
10	2	59	51	43	35	27
19	11	3	60	52	44	36
above for C_i; below for D_i						
63	55	47	39	31	23	15
7	62	54	46	38	30	22
14	6	61	53	45	37	29
21	13	5	28	20	12	4

PC2					
14	17	11	24	1	5
3	28	15	6	21	10
23	19	12	4	26	8
16	7	27	20	13	2
41	52	31	37	47	55
30	40	51	45	33	48
44	49	39	56	34	53
46	42	50	36	29	32

Table 7.4: DES key schedule bit selections (PC1 and PC2).