Cryptografie in Cyberspace

21-10-2015

Onderwerpen

- *wat is cryptografie*
- *cryptografie van het verleden*
- *cryptografie van het heden*
- *cryptoanalyse*

meer informatie in syllabus niet-beta via https://staff.fnwi.uva.nl/H.vanderMeer

Wat is Cryptografie

- eenvoudig voorbeeld
- terminologie
- klassieke cryptografie
- openbare sleutel systeem
- quantum cryptografie

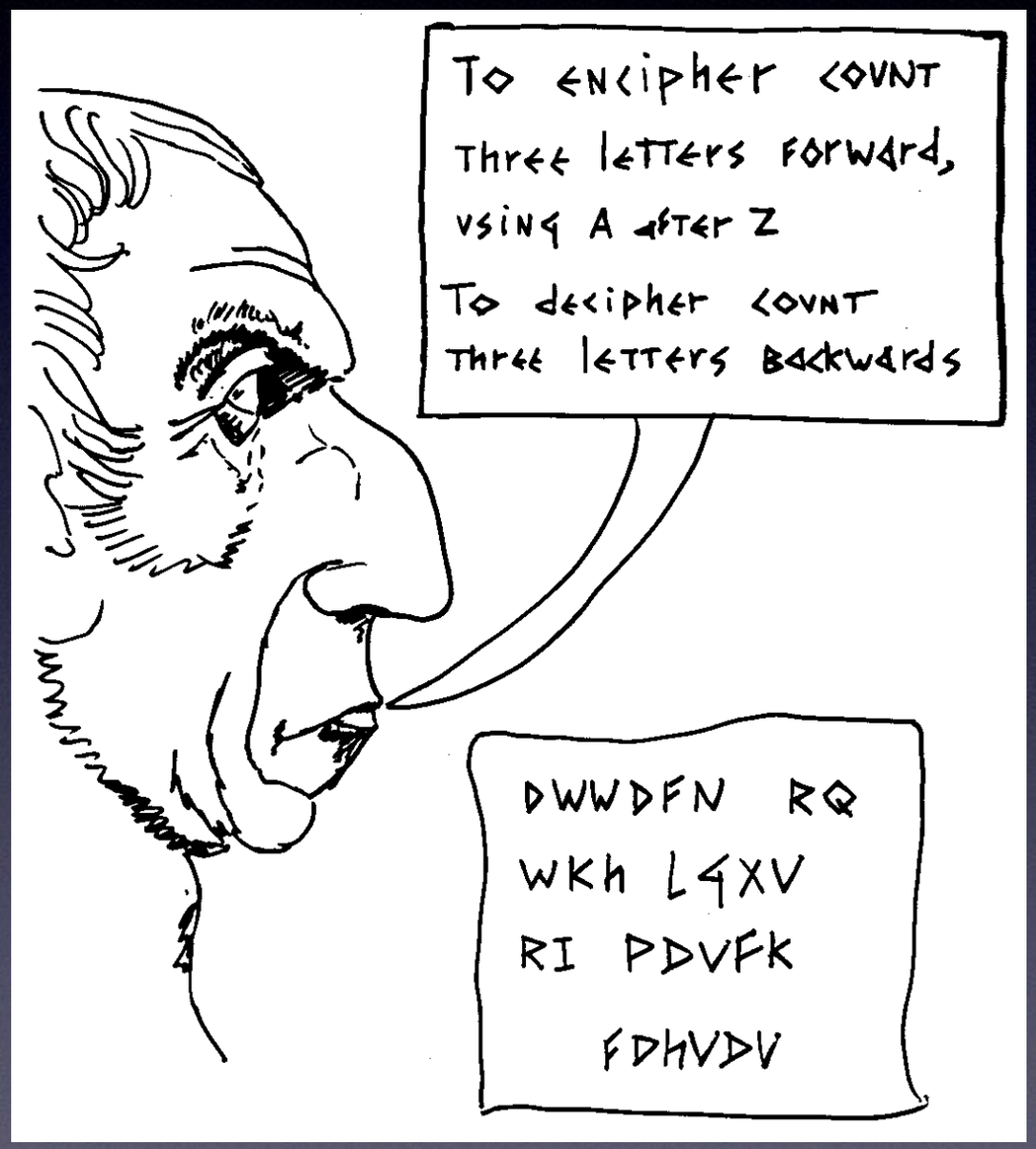
Probleemstelling

Julius Caesar heeft een groot probleem

“Als ik het aanvalsplan verstuur valt het vast en zeker in de handen van die vreselijke Galliërs!”

Wat doen we daaraan?

Gebruik Cryptografie



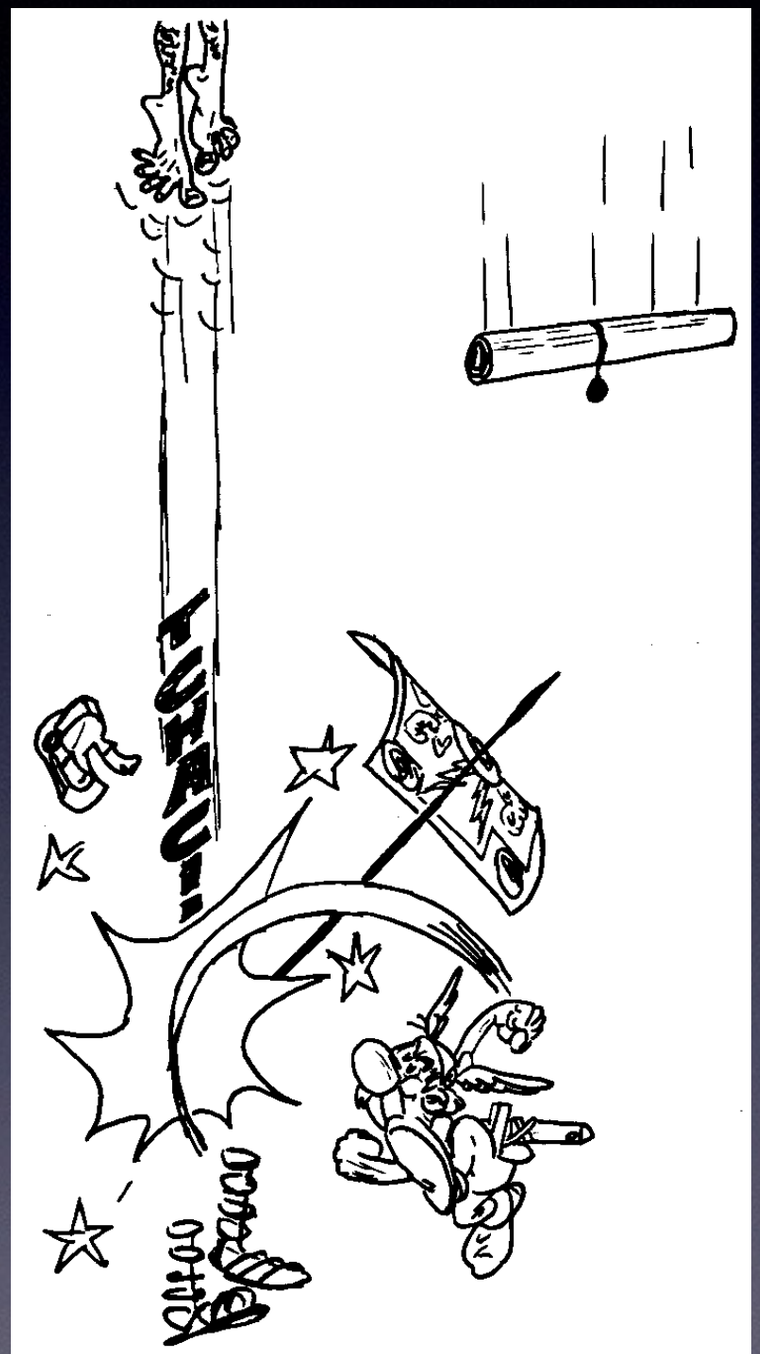
CAESAR *systeem*

vercijferen = 3 plaatsen verder
A→D B→E … X→A

ontcijferen = 3 plaatsen terug
D→A E→B … A→X

sleutel = 3 plaatsen
andere sleutels 1, 2, 4, 5, …

Cryptoanalyse



DWWDFN RQ WKH L4XV RI PDVFK

<VV<EM QP VJ4 KFWU Qh O<TEJ

BUUBDl PO UIF JEVT PG NBSDI

ATTACK ON THE IDUS OF M4R<H

cryptoanalist Cryptanalix

Terminologie

cryptologie = cryptografie + cryptoanalyse

cryptografie = geheim schrijven

κρύπτω = verbergen γραφή = geschrift

klaartekst, cryptogram, cijfertekst

cryptoanalyse = breken geheimschrift

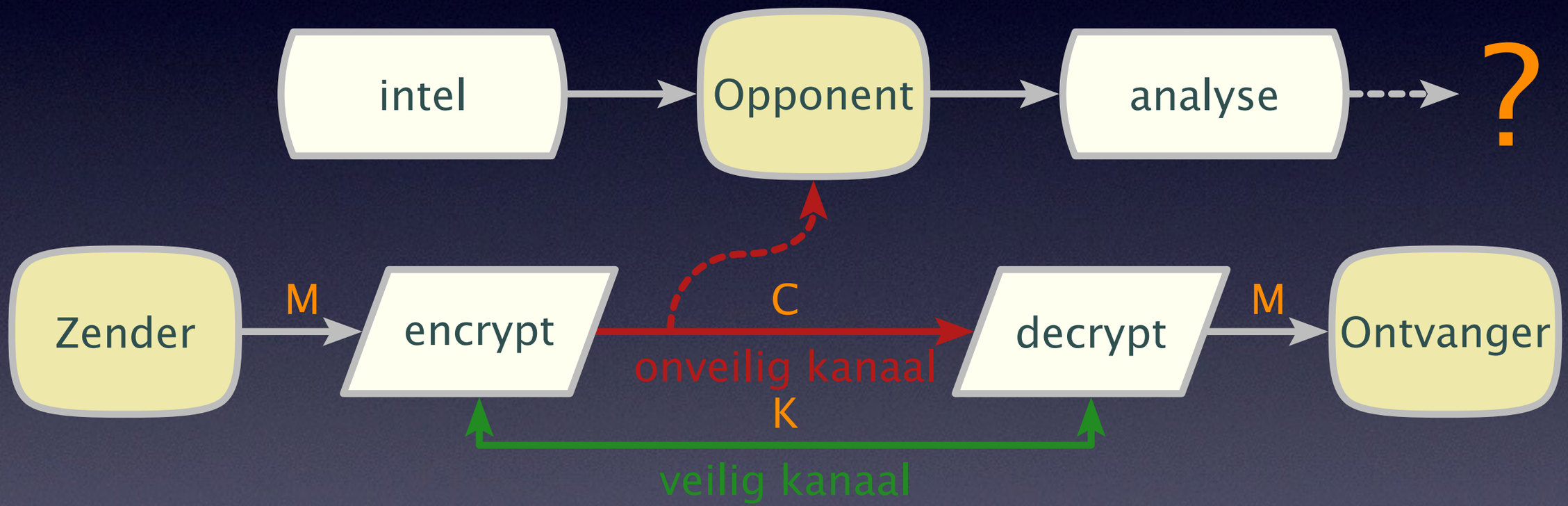
known-plaintext, ciphertext-only, chosen-plaintext

steganografie = verborgen schrijven

στέγω = bedekken

traffic analysis = berichtenverkeersanalyse

Klassieke cryptografie



Regels voor veiligheid

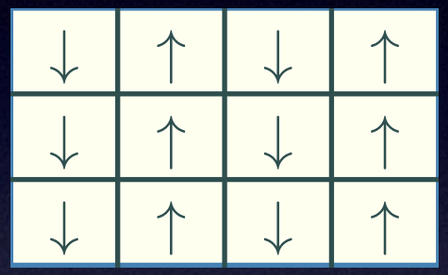
Auguste Kerckhoffs, 1883, La Cryptographie Militaire

Veiligheid berust op geheimhouden van de sleutel
niet op geheimhouden van het geheimschrift

Praktische criteria:
- kosten cryptoanalyse versus waarde geheim
- tijd nodig voor cryptoanalyse versus levensduur geheim

Klassiek cryptosysteem

transpositie



C	R	Y	P
T	O	G	R
A	F	I	E

CTAFORYGIERP

substitutie

```
klaaralfabet  ABCDEFGHIJKLMNOPQRSTUVWXYZ
cijferalfabet DEFGHIJKLMNOPQRSTUVWXYZABC

    VLUCHT POLITIE = YOXFKW SROLWLH
```

- een of beide alfabetten gepermuteerd
- periodiek substitutiepatroon
- niet periodiek substitutiepatroon
- meerdere letters tegelijk vervangen
- woorden en uitdrukkingen vervangen

Staalkaart systemen

Transpositie
- Route
- Kolom
- Rooster

Monoalfabetisch
- Caesar
- Standaard
- Monome-dinome
- Playfair
- Bifid
- ADFGVX
- Nomenclatuur
- Code
- Encicode

Polyalfabetisch
- Porta
- Vigenère
- Beaufort
- Nihilist
- Progressie
- Autoclaaf
- Wheatstone
- Multiplex
- One-time-pad

Machine
- Hagelin
- Kryha
- Enigma
- Purple

enz. enz. enz.

Kolomtransposition

sleutel →

2	*5*	*3*	*1*	*6*	*4*
D	E	V	R	A	G
E	N	V	A	N	H
E	T	T	E	N	T
A	M	E	N	Z	Y
N	N	O	G	G	E
H	E	I	M	X	X

←transpositieblok

pt: DE VRAGEN VAN HET TENTAMEN ZIJN NOG GEHEIM XX

ct: RAENG MDEEA NHVVT EOIGH TYEXE NTMNE ANNZG X

cryptoanalyse: splitsing in 6 kolommen is eenvoudig

RAENGM DEEANH VVTEOI GHTYEX ENTMNE ANNZGX

Kolomtranspositie variant

M	*U*	*S*	*K*	*U*	*S*
2	*5*	*3*	*1*	*6*	*4*
D	E	V	R	A	G
E	N	V	A	N	H
E	T	T	E	N	T
A	M	E	N	Z	Y
N	N	O	G	G	E
H	E	I	M		

←transpositieblok niet uitgevuld

```
pt: DE VRAGEN VAN HET TENTAMEN ZIJN NOG GEHEIM
ct: RAENG MDEEA NHVVT EOIGH TYEEN TMNEA NNZG
```

cryptoanalyse: splitsing in 6 kolommen niet eenvoudig

```
RAENG MDEEA? of RAENGM DEEAN? of …??
```

Dubbele transpositie

H	*A*	*R*	*I*	*N*	*G*	*T*	*O*	*N*
3	*1*	*8*	*4*	*5*	*2*	*9*	*7*	*6*
D	E	N	B	R	I	E	L	V
O	O	R	D	E	G	E	U	Z
E	N	G	E	V	A	L	L	E
N	A	L	V	A	N	A	A	R
M	A	D	R	I	D			

L	*E*	*E*	*S*	*B*	*R*	*I*	*L*
5	*2*	*3*	*8*	*1*	*7*	*4*	*6*
E	O	N	A	A	I	G	A
N	D	D	O	E	N	M	B
D	E	V	R	R	E	V	A
I	V	Z	E	R	L	U	L
A	N	R	G	L	D	E	E
L	A						

pt: DEN BRIEL VOOR DE GEUZEN GEVALLEN ALVA NAAR MADRID

ct: AERRL ODEVN ANDVZ RGMVU EENDI ALABA LEINE LDAOR EG

US Army Double Transposition

Monoalfabeet

Vervanging van A–Z door permutatie van A–Z

bijvoorbeeld

```
plaintext  : ABCDEFGHIJKLMNOPQRSTUVWXYZ
ciphertext: SLEUTCONRIMWDFZABGHJKPQVXY
```

PEST → ATHJ

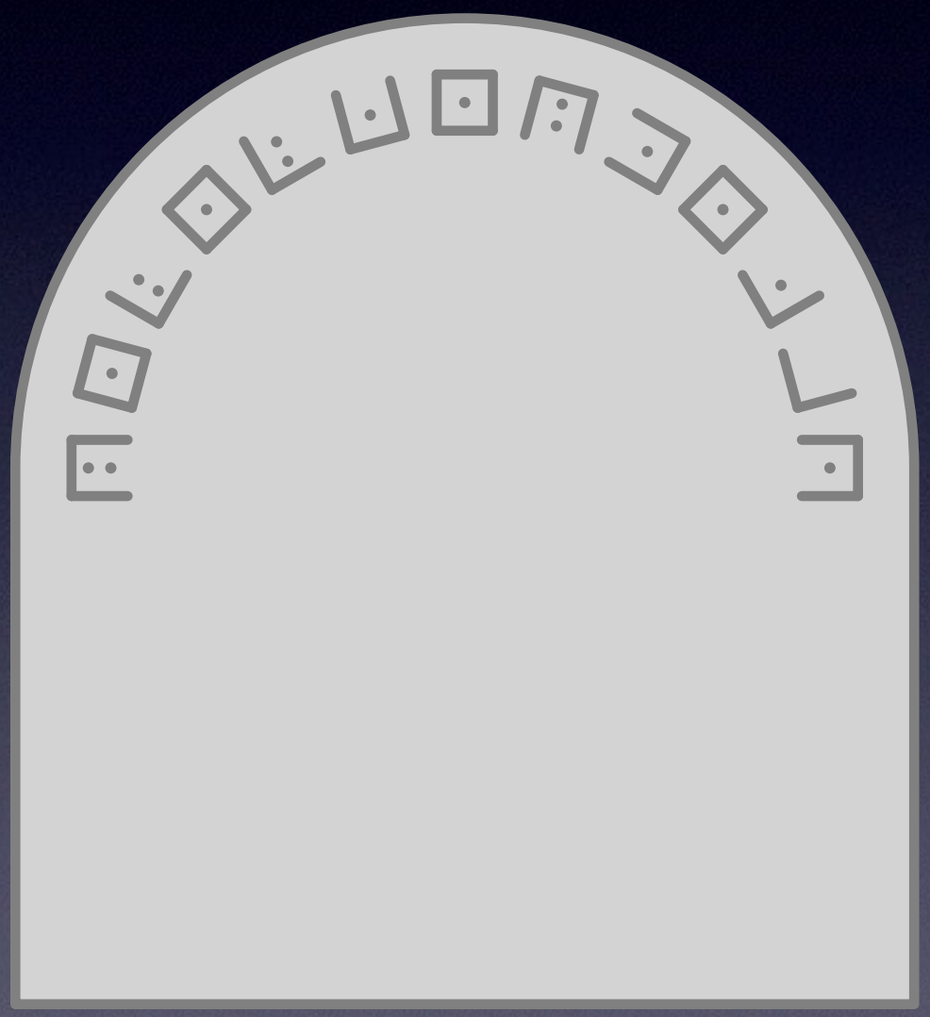
In theorie 26! = 26*x*25*x*…*x*3*x*2 ≈ 4.10^{26} sleutels

maar veel hebben weinig effect

zoals alleen Q en X verwisselen

cryptoanalist heeft aan 30-60 letters genoeg

Vrijmetselaarsgeheimschrift



Trinity Church, New York

graf van James Leeson † 1794

REMEMBER DEATH

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		

Digram-substitutie

	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*
A	LZ	SW	BH	YJ	YR	WP	BC	FB	FW	XH	DY	MV	KC	UL	CJ	FJ	XW	BR	AD	JP	BJ	PM	JW	IU	OU	DE
B	AJ	GE	KT	AP	TN	VO	GY	CT	JS	OB	YM	MH	WJ	PF	PA	TA	IF	NR	GG	PV	LH	NX	KX	ST	UT	RP
C	LW	KW	DO	QF	JN	LX	DI	TL	DR	RM	SS	HF	RB	QU	UJ	KR	MY	GO	WF	TG	RS	YQ	SC	FI	CR	HK
D	UV	FP	PS	XZ	EV	GR	SV	KF	ZX	WL	RU	WO	YZ	JJ	NJ	VJ	IT	QT	XG	AS	KE	WE	ND	HS	YC	UH
E	AO	CZ	CI	SI	BV	OM	ZO	LE	GD	LB	OI	UK	RC	DK	PZ	YX	KJ	ZT	EM	BS	IZ	XL	RF	WA	YW	EL
F	OC	RI	SP	FY	VH	QE	SE	FC	IK	NZ	RG	LN	TX	NM	SD	JB	UQ	XY	ZG	ML	AV	JC	QM	PQ	AB	ZF
G	MD	VE	FX	MW	OD	PJ	XX	HT	IC	LC	NH	ZD	GC	YY	VP	YA	PC	BE	JF	DS	QK	SX	EQ	ET	YD	JH
H	BT	TK	PR	KY	EC	AN	HZ	SO	YV	MF	ES	YP	FU	AK	NI	SJ	YT	LY	TF	KV	NV	XV	DJ	WX	OO	QB
I	WR	GK	IE	QH	EZ	OY	MU	MT	LA	BP	HA	NM	TJ	QJ	AL	EE	SU	GA	HI	MG	YO	GW	KS	AY	JE	NO
J	VG	ZY	UE	FM	EH	FR	ZW	CA	DN	WD	KD	AU	GP	YS	XM	MR	NC	BQ	HC	NS	NN	ZJ	GJ	VB	RA	TH
K	KQ	UR	VQ	AT	OA	YI	FS	RJ	LT	JD	KI	PG	AC	MI	CD	BG	TZ	PH	OT	WQ	IH	LK	OK	XE	HY	CX
L	YE	VX	GS	VY	IM	HW	HB	JX	NE	ZI	IB	HL	BI	QO	VK	AH	LL	VT	YB	DL	ZC	QI	JA	DH	UY	ZH
M	HU	EW	UC	IJ	UO	SQ	OR	EP	ZE	MX	KL	IQ	TS	QZ	BM	TI	JV	VD	XS	OH	IX	TV	TB	QN	UW	KN
N	LM	CB	SK	EY	PO	FQ	LG	MS	RK	VS	RW	CL	II	RO	ZR	NP	HX	RN	BF	IV	DX	XI	UG	BX	JM	AQ
O	TQ	XN	SH	ZS	WK	OX	WU	HH	MQ	PT	GL	QA	EX	PX	ZB	HJ	VW	SB	PL	DB	NA	CM	UX	IA	JK	LU
P	XD	GM	TC	FG	EJ	FN	WT	NF	OG	QY	DZ	NB	NU	IN	ZV	HM	CS	JU	WV	QG	FH	RQ	TE	DA	GH	AF
Q	YG	DV	EF	HV	TU	HR	LJ	CQ	FK	VC	GF	FZ	ER	XK	NW	XU	VA	ED	MN	UI	RL	GX	WH	WS	TM	OW
R	OS	XR	ID	SG	CY	TY	KG	ZN	YL	KZ	OJ	GU	VF	VR	BD	JO	GV	ZU	FF	WG	XF	GZ	KP	KU	QD	JT
S	RY	GQ	ZZ	HP	CC	HQ	UF	AD	PK	DW	XQ	DU	RH	DC	GN	QR	DM	MK	SF	RZ	MC	FT	BZ	LQ	IO	LO
T	YF	BA	UU	YN	TR	LD	WB	NQ	TW	VN	RD	FA	YU	OP	OQ	LR	FL	JI	JZ	HO	QQ	QC	GI	QW	KH	MA
U	JQ	XO	CH	EA	SY	XJ	IG	PD	ZL	LF	LP	KO	JY	ZP	UD	KA	TD	NG	ZQ	CF	AI	XT	HD	XB	UB	CW
V	XC	EI	BU	VV	AX	DF	MZ	VU	VM	RV	UP	PN	WC	FE	DT	IL	ZM	CU	EK	WZ	OF	LS	BL	IS	XA	BB
W	LI	FO	KM	JR	CV	QP	EG	WN	UA	NT	AG	UN	KK	US	WY	MP	SL	MB	BK	KB	AR	YH	DD	OE	DG	VI
X	AE	FD	ZK	SA	QX	SM	HE	CE	ZA	QV	IY	CN	PY	HN	JG	XP	AZ	UZ	BN	BW	PI	MO	AW	QL	DP	HG
Y	RX	NY	TO	MJ	SR	PE	BO	TT	BY	OV	WM	VZ	GT	CO	JL	GB	SN	NK	OL	PU	EU	RE	PP	RT	AM	CG
Z	ON	ME	IP	PB	WI	EB	LV	PW	EN	VL	NL	AA	QS	WW	RR	SZ	DQ	UM	CP	TP	IW	YK	CK	OZ	FV	IR

niet 1 maar 2 letters tegelijk

sleutels: 676*x*675*x*674*x*…

onthouden ondoenlijk

daarom eenvoudiger schema’s

zoals Playfair

```
pt: NOOIT GEDACHT TOCH GEKREGEN

ct: ZRMQW BSIBH KVOQT LODPH ZODK
```

Periodieke substitutie

Eindige sleutel herhaald gebruikt zoals

Key = $k_1k_2k_3k_4k_5k_6$ 6 = de periode

Vele varianten mogelijk:

- normaal alfabet *Porta, Vigenère*
- teruglopend alfabet *Beaufort*
- gemengd alfabet in verschillende varianten
- sleutelwoord of sleutelzin
- lange sleutel door machine *Hagelin, Enigma*

Vigenère

Blaise de Vigenère
1523–1596
1563 *Traicté des Chiffres*

	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
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
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
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
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
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
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
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
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
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
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
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
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
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
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
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
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
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
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
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
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
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
V	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	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	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	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	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

vercijfer: sleutel M → S ↓ = E

ontcijfer: sleutel M → E ↑ = S

One-Time-Pad

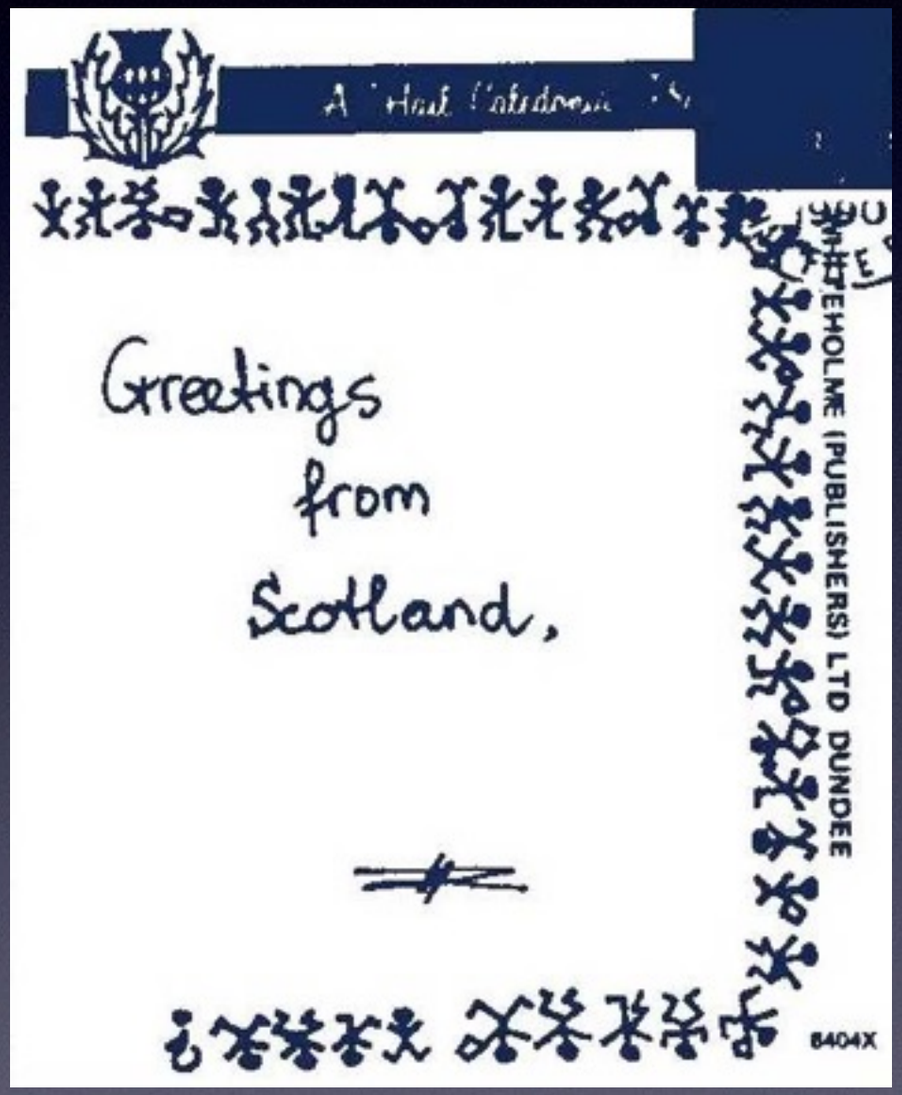
sleutel + klaartekst → cryptogram

- oneindig lange willekeurige éénmalige sleutel nodig
- voordeel: absoluut onbreekbaar
- nadeel: éénmalig gebruik dus veel sleutel nodig
- hergebruik sleutel: kwetsbaar VENONA -break KGB-cipher

sleutelproductie met

- radioactief verval, electronische ruis
- loterij
- pseudorandom generator (niet meer onbreekbaar!!)

Echte cryptografie



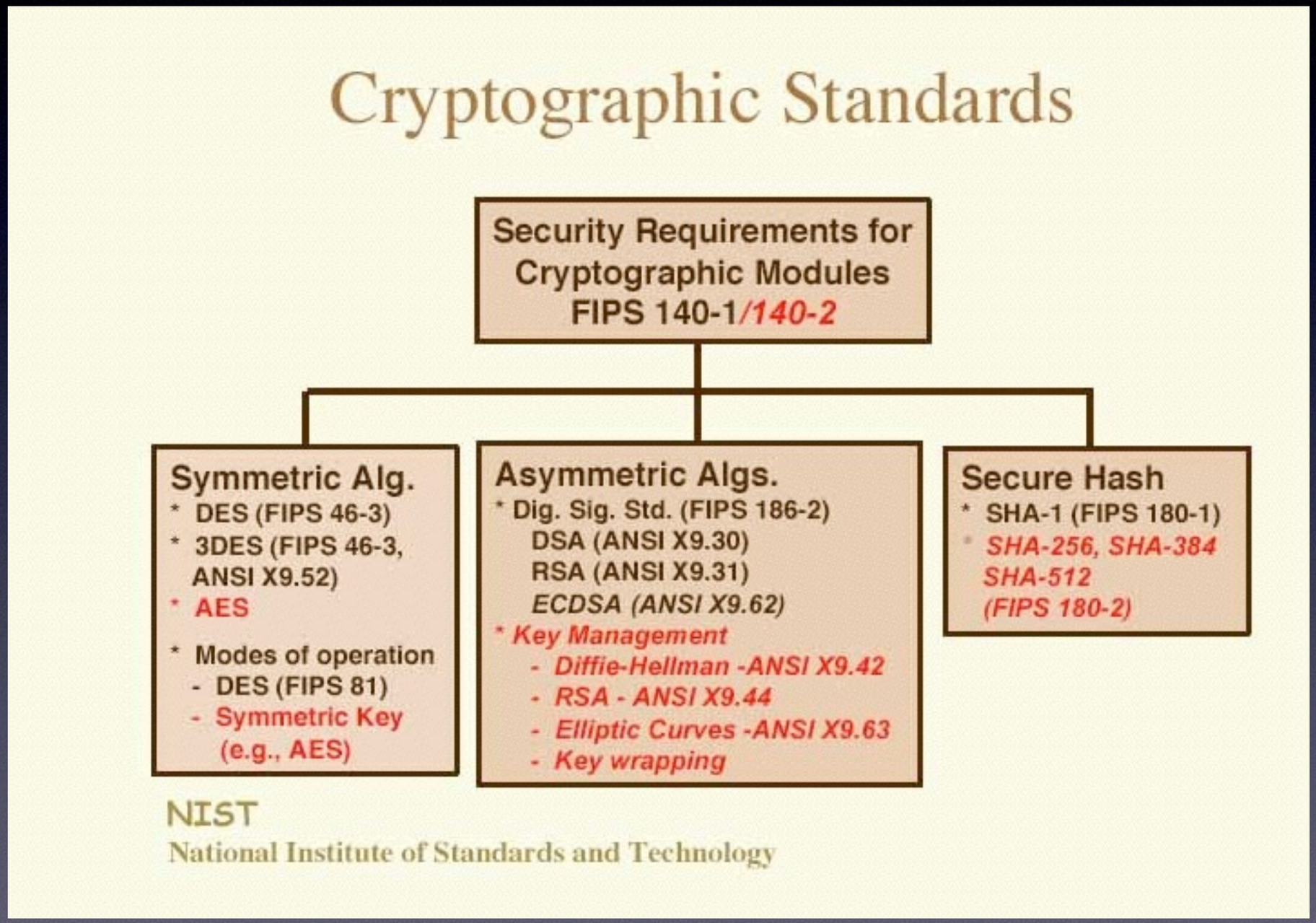
Diplomatieke instructie

El Rey = Philips IV (1605-1665)

datum *Madrid, 27 julio 1658*

Don Estevan de Gamarray contreras demi ans del juerra Castellano al castillo de Gante Sire de campo general demis exitos de flandes y embaxer al estados generales de las Provincias Unidas del Pays vajo …

Moderne Cryptografie



Blokgeheimschrift

64-bits klaartekst → 64-bits cijfertekst = blok van 64 bits lang

56-bits sleutel → $2^{10} \approx 1000$ → $2^{56} \approx 64\ 000\ 000\ 000\ 000\ 000$

Theoretisch $2^{64}!$ vercijfersleutels voor 64-bits blok vercijfering mogelijk

→ alle mogelijke onderlinge verwisselingen van alle blokken

blok van 2 bits, $2^2 = 4$ waarden, $4! = 4x3x2x1 = 24$ sleutels

klaar →	sleutel-1	sleutel-2	sleutel-3	…	sleutel-24
↓	↓	↓	↓	…	↓
0	0	1	2	…	3
1	1	2	3	…	2
2	2	3	0	…	1
3	3	0	1	…	0

Meestal véél minder benut: 56-bits sleutel, 64 bits blok → $2^{56} << 2^{64}!$

Valkuilen

Sleutels waarbij vercijfering geen effect: fixed point

2-maal vercijferen geeft klaartekst terug: zwakke sleutel

Naief gebruik: zichtbare struktuur

… en nog veel meer …

Valkuilen

geheimschrift *veilig en goed implementeren* is haast nog moeilijker dan een geheimschrift maken

Western Digital self-encrypting hard drives riddled with security flaws

Encrypted data is often easily recovered, in some cases with no password required.

by **Dan Goodin** - Oct 21, 2015 12:50am CEST

Share Tweet 62

Electronic Code Book

```
* MYSTERY PROGRAM                                                    00000010
* D.E.KNUTH                                                          00000020
* THE ART OF COMPUTER PROGRAMMING, VOL I                             00000030
* EXERCISE 1.3.2 # 8                                                00000040
PRINTER   EQU   18                                                  00000050
BUF       ORIG  *+3000                                              00000060
1H        ENT1  1                                                   00000070
          ENT2  0                                                   00000080
          LDX   4F                                                  00000090
2H        ENT3  0,1                                                 00000100
```

ECB

```
\BKF<&bm/qKI5¨Uz}eKxbR.H\8KxbR.H\8KxbR.H\8KxbR.H\8KxbR.H\8KxbR.HlH[)rb?X
\BK=pw<s+m AbR.H\8KxbR.H\8KxbR.H\8KxbR.H\8KxbR.H\8KxbR.H\8KxbR.HlH[)rb@X
\BKM+w.i/lKH)RQw*h!M(%.x/grK$ [q+_Wx9¨ZH&8KxbR.H\8KxbR.H\8KxbR.HlH[)rbAX
\BK>;w`k&kpxs`AVn8NxzR.H\8KxbR.H\8KxbR.H\8KxbR.H\8KxbR.H\8KxbR.HlH[)rbBX
\h}B1'Sz\8K>4(.H\IcxbR.H\8KxbR.H\8KxbR.H\8KxbR.H\8KxbR.H\8KxbR.HlH[)rbCX
\Z!?bR.H\8KH5{UH\BV,rb>H\8KxbR.H\8KxbR.H\8KxbR.H\8KxbR.H\8KxbR.HlH[)rbDX
\IsxbR.H\8K>1'?H\IKxbR.H\8KxbR.H\8KxbR.H\8KxbR.H\8KxbR.H\8KxbR.HlH[)rbEX
\8KxbR.H\8K>1'@H\HKxbR.H\8KxbR.H\8KxbR.H\8KxbR.H\8KxbR.H\8KxbR.HlH[)rbFX
\8KxbR.H\8KE'+.H\LqxbR.H\8KxbR.H\8KxbR.H\8KxbR.H\8KxbR.H\8KxbR.HlH[)rbGX
\JsxbR.H\8K>1'AH\HW*bR.H\8KxbR.H\8KxbR.H\8KxbR.H\8KxbR.H\8KxbR.HlH[)rc>X
```

Remedie tegen structuur:
Cipher Block Chaining = ketting rijgen

Cipher Block Chaining

ECB

```
\BKF<&bm/qKI5¨Uz}eKxbR.H\8KxbR.H\8KxbR.H\8KxbR.H\8KxbR.H\8KxbR.H1H[)rb?X
\BK=pw<s+m AbR.H\8KxbR.H\8KxbR.H\8KxbR.H\8KxbR.H\8KxbR.H\8KxbR.H1H[)rb@X
\BKM+w.i/lKH)RQw*h!M(%.x/grK$ [q+_Wx9¨ZH&8KxbR.H\8KxbR.H\8KxbR.H1H[)rbAX
\BK>;w`k&kpxs`AVn8NxzR.H\8KxbR.H\8KxbR.H\8KxbR.H\8KxbR.H\8KxbR.H1H[)rbBX
\h}B1'Sz\8K>4(.H\IcxbR.H\8KxbR.H\8KxbR.H\8KxbR.H\8KxbR.H\8KxbR.H1H[)rbCX
\Z!?bR.H\8KH5{UH\BV,rb>H\8KxbR.H\8KxbR.H\8KxbR.H\8KxbR.H\8KxbR.H1H[)rbDX
\IsxbR.H\8K>1'?H\IKxbR.H\8KxbR.H\8KxbR.H\8KxbR.H\8KxbR.H\8KxbR.H1H[)rbEX
\8KxbR.H\8K>1'@H\HKxbR.H\8KxbR.H\8KxbR.H\8KxbR.H\8KxbR.H\8KxbR.H1H[)rbFX
\8KxbR.H\8KE'+.H\LqxbR.H\8KxbR.H\8KxbR.H\8KxbR.H\8KxbR.H\8KxbR.H1H[)rbGX
\JsxbR.H\8K>1'AH\HW*bR.H\8KxbR.H\8KxbR.H\8KxbR.H\8KxbR.H\8KxbR.H1H[)rc>X
```

Effect van block chaining:

CBC

```
\BKF<&bm,T7OqHX)JZ#It;'qG3nbw.UZDkZ{z!$CADF5}sR,>|2N!f!t;U}g$YO]H>y17\/V
E!enHtkjp/&PKg:SmgqiNZh<j@]#QM7%gxI<T@emdQ5UW34Va*!nZ&b?^bl(]x1(kKhQp{q!
h.T?<4@+8;@(e'2CbDau.L`\2LtaRl\n]Llz,/WW$%X4/¨&@!]DM2tT)}6Of5g#q+ ,OHjdj
(awn$#evNm)(8$Gm]FwASvuVZ cZViD?WWOsY\r(TO;-\OApQh'F_BoYNAr_b5>B[*n)u8!;
X3-kG_tVUkxJ{(C?RU|c zq(O.h|¨m@pLfT6%`nYI?@O(S=BFw,h+Fk+CPw¨.9:sP9sKA<}l
M45+D/LUJl!syKB>GOw@-N!'D(cYOAOoA`Or34}X>9;,6'LA;q'E9yz*8Jr^<lIrE3n(Oo.k
B|#ARb\T?Un $*<=<?Z9'|j&9wFR*o9n6P2k-bgW3)}%OU6@Oai>3Hd)-:UW6;3q:#Q!I>xj
7[=:L1GS44)x}X(<1|t2!KV%.U`K$>%m+.Ld'1SV(f8}*$¨?%?$7-vP(¨woPOi p/`kyClei
,9W3F_4R)qCxm+b;&^U2p}1$#7AKsp_l o-dvc.U|Hx}yV\>y!d7|I+'vYPP <Yo$BLy3?Ah
!-`362oQ}eLqgYQ:zND<jL #w'OUm?Nkt_{np2|Tq8g(s%K=npSAvwy&kI?ZyjHnx2;$-n'g
```

AES

12 september 1997 NIST start opvolging DES uit 1975

AES = Advanced Encryption Standard

ongeclassificeerd en publiek algoritme

overal zonder royalties beschikbaar

symmetrisch 128 bits blokgeheimschrift

keuze voor sleutel uit 128, 192, 256 bits

efficiënte implementatie in smartcards

wedstrijd met deelnemers uit alle delen van de wereld

Winnaar is Rijndael

twee Belgen: Vincent Rijmen en Joan Daemen

Algebra als basis wiskunde dus!

Keuze blok/sleutel uit 128/192/256 bits

Aparte vercijferstap vóór eigenlijke vercijfering

Afhankelijk sleutellengte 10/12/14 ronden uitvoeren

Snelle vercijfering in smartcards met weinig geheugen

Cryptoanalyse nog niet gelukt

Rijndael schema

stap	startronden	slotronde
1	ByteSub	ByteSub
2	ShiftRow	ShiftRow
3	MixColumn	AddRoundKey
4	AddRoundKey	

ByteSub = monoalfabetische substitutie van 256 bytes
ShiftRow en MixColumn = combineren van aantal bytes
AddRoundKey = combineren met veranderende subsleutels

Basisoperaties

b_0	b_4	b_8	b_{12}
b_1	b_5	b_9	b_{13}
b_2	b_6	b_{10}	b_{14}
b_3	b_7	b_{11}	b_{15}

ByteSub

b_0	b_4	b_8	b_{12}
b_1	b_5	b_9	b_{13}
b_2	b_6	b_{10}	b_{14}
b_3	b_7	b_{11}	b_{15}

ShiftRow

b_0	b_4	b_8	b_{12}
b_1	b_5	b_9	b_{13}
b_2	b_6	b_{10}	b_{14}
b_3	b_7	b_{11}	b_{15}

MixColumn

ByteSub

b_0	b_4	b_8	b_{12}
b_1	b_5	b_9	b_{13}
b_2	b_6	b_{10}	b_{14}
b_3	b_7	b_{11}	b_{15}

ShiftRow

b_0	b_4	b_8	b_{12}
b_5	b_9	b_{13}	b_1
b_{10}	b_{14}	b_2	b_6
b_{15}	b_3	b_7	b_{11}

MixColumn

b_0	b_4	b_8	b_{12}
b_5	b_9	b_{13}	b_1
b_{10}	b_{14}	b_2	b_6
b_{15}	b_3	b_7	b_{11}

AddRoundKey

128 bits sleutel verbruikt 1408 subsleutel-bytes

door slimme berekening “on the fly”

combinatie van sleutel en data:

met speciale bit voor bit optelling

$0 + 0 = 1 + 1$ en $1 + 0 = 0 + 1 = 1$

voorbeeld: 1100 + 1010 = 0110

PublicKey systeem

Aragorn
K1-paar

Boromir
K2-paar

Arwen
K3-paar

Publickey in gebruik

in: public key Arwen

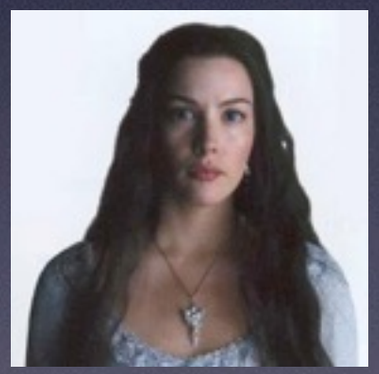
uit: secret key Arwen

Geheimhouding

Maar is dit Aragorn?

in: secret key Aragorn

uit: public key Aragorn



Authentiseren

Ja! dit is Aragorn!

Trapdoor functies

- oneway functie
  eenvoudig *uitrekenen* maar moeilijk *terugrekenen*
  voorbeeld: *kwadrateren* eenvoudig, *worteltrekken* moeilijk
- trapdoor oneway functie
  moeilijk terugrekenen - maar eenvoudig m.b.v. *extra* informatie

klassificatie van benodigde rekentijd naar probleemgrootte

- eenvoudig: groeit langzaam als probleem groter wordt
- ondoenlijk: groeit razendsnel als probleem groter wordt
- alle sleutels proberen wordt explosief moeilijker als het aantal sleutels groter wordt

leverancier valluik-functies is *getaltheorie o.a. factoriseren*
(=ontbinden in factoren 15 = 3 x 5)

Getaltheorie een klein beetje maar

we rekenen alleen met positieve gehele getallen

niet alle getallen maar slechts tot een zeker maximum

en als antwoord groter is dan het maximum - wat dan?

doe dan een modulo reductie

voorbeeld 100 getallen 0…99 en niet meer

stel uitkomst van een berekening is 317

bewaar alleen de rest van 317 gedeeld door 100

het antwoord is 17 de rest van 317:100

we noteren dit als 317 modulo 100 = 17

Getallen in publickey

stel alleen getallen 0 t/m 99 dus modulo 100 rekenen

verwijder alle getallen die factor met 100 gemeen hebben

blijft over 1, 3, 7, 11, … want geen factor 2 en/of 5

waarom? dat geeft een goede verzameling getallen

handig is nu: niet modulo 100 maar modulo priemgetal

waarom? dan alle getallen 1, 2, 3,…, priem-1 present

doe er vervolgens de 0 bij:

resultaat is een fijne verzameling om mee te werken

publickey-systemen rekenen met zo’n verzameling

RivestShamirAdleman 1978

geheime systeeminformatie

p en *q* twee priemgetallen

d speciaal gekozen getal

vercijferen

M tot macht *e* modulo *n* = *C*

ontcijferen

*C t*ot macht *d* modulo *n* = *M*

openbare systeeminformatie

product *n* = *p* x *q*

getal *e* zo berekend dat

e x *d* = *1* mod *(p-1)(q-1)*

vercijfer-mechanisme is machtsverheffen

maak *n* meer dan 300 cijfers

p en *q* uit *n* uitrekenen is dan hels moeilijk

gevaar:
p,q,d,e onzorgvuldig gekozen

Voorbeeld RSA

Kies RSA parameters

1. p = 47 en q = 59 → n = 2773
2. (p-1)(q-1) = 46.58 = 2668
3. kies d = 157 en ggd(2668,157) → e = 17 (grootste gemene deler)
   want ed = 17.157 = 1 modulo 2668

Codeerschema spatie = 00, A = 01, B = 02, …

Vercijfering

```
   I T  S    A L  L    G R  E E  K    T O    M  E
M: 0920 1900 0112 1200 0718 0505 1100 2015 0013 0500
C: 0948 2342 1084 1444 2663 2390 0778 0774 0219 1655
```

0920^{17} modulo 2773 = 0948 ↔ 0948^{157} modulo 2773 = 0920

Factoriseren

# cijfers	schatting 1985	realisering
100	1 jaar	
125	100 jaar	1994: RSA-129
150	10.000 jaar	1999: RSA-155
175	700.000 jaar	2003: RSA-176
200	30 miljoen jaar	2005: RSA-200
225	1 miljard jaar	2009: RSA-232
250	60 miljard jaar	quantum computer?

Priemgetallen

hoeveel priemgetallen in [2 .. 100] cijfers?
bij benadering ongeveer # = 100 / ln 100
van 100 cijfers? #(100) - #(99) ≈ 4.10^{97}
gemiddelde afstand priemgetallen ≈ ln 100
bij 100 cijfers ± 230, bij 150 cijfers ± 345

Gauss 1777–1855

voor RSA minstens n = 1024 bits → p,q elk ± 150 cijfers
nu al beter is neem 4096 bits, 512 bits al onveilig

priemgetallen zijn niet allemaal gelijkwaardig:
zogenaamd sterk priemgetal nodig

Priemgetal vinden - hoe?

deterministisch AKS = Agrawal-Kayal-Saxena algoritme

probabilistisch Solovay-Strassen algoritme

1. kies een getal *a* om ermee te testen of *n* priemgetal is
   a heet een getuige voor *n* is een priemgetal
2. voer de test uit
   twee mogelijke uitkomsten:
   getuige *a* zegt dat *n* niet priem = betrouwbaar
   leugenaar *a* zegt dat *n* wel priem = onbetrouwbaar
3. leugenaar heeft 50% kans → na 20 testen < 0.0001%

Quantumcryptografie

Quantummechanica bepaalt gedrag elementaire deeltjes

Zoals de onzekerheidsrelatie van Heisenberg:
plaats en snelheid deeltje niet tegelijkertijd exact te meten

Gebruik: meting beïnvloedt toestand van het deeltje

Realisatie cryptografie met polarisatie van één foton

Quantum bit-transport

bits:	1	0	1	1	0	1	1
verzonden:							
meting:							
ontvangst:	1	0	0	1	0	1	1
verificatie:							
resultaat:	1	0			0	1	1

Cryptoanalyse

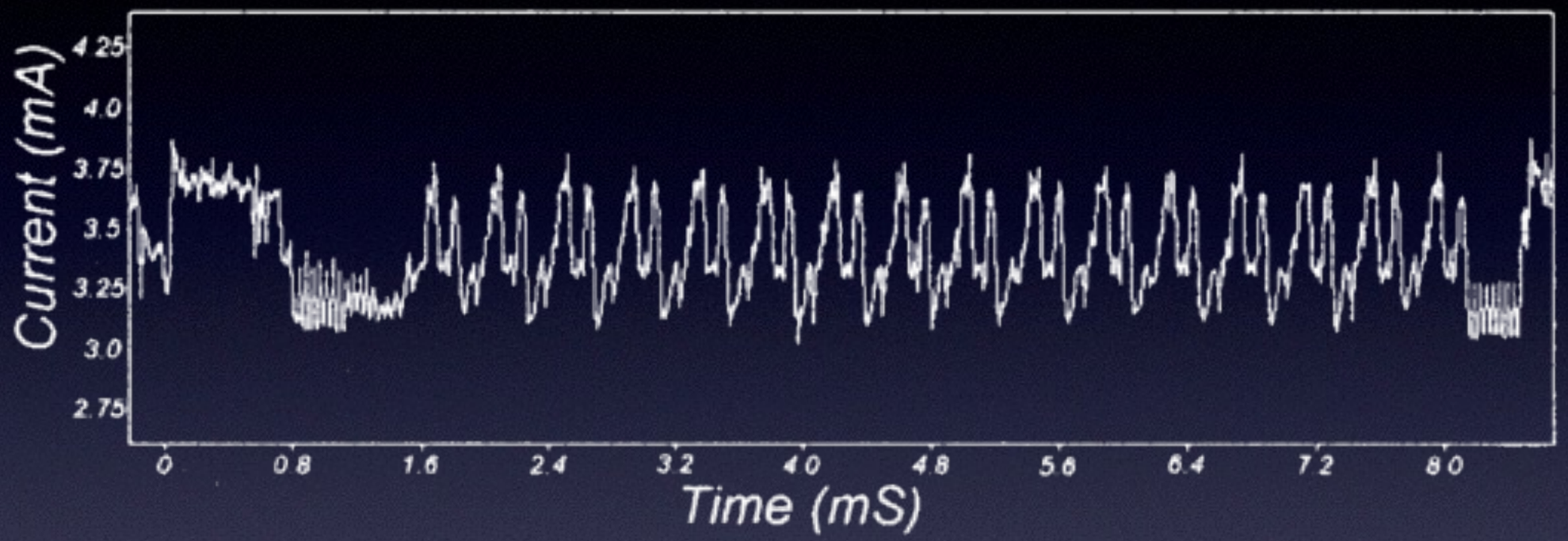
- brute force = uitputtend zoeken
  in software
  special purpose hardware

- side channel analyse = fysische methoden benutten

- time memory tradeoff = berekeningen vooraf maken

- individuele methoden tegen zwakke punten systeem

Side Channel Analyse



stroomverbruik toont processor acties

foutinjectie geeft verschillende uitkomsten

timing analyse door verschil in processor instructies

Cryptografie in Cyberspace

The END

21-10-2015