Cursus Cryptografie

MONOALFABEET

16-02-2016

Klassieke systemen

Transpositie
- Route
- Kolom
- Rooster

Monoalfabetisch
- Caesar
- Homofoon
- Monomedinome
- Playfair
- Bifid
- ADFGVX

- Nomenclatuur
- Code
- Encicode

Polyalfabetisch
- Porta
- Vigenère
- Beaufort
- Nihilist
- Progressie
- Autoclaaf
- Wheatstone

- Multiplex
- One-time-pad

Machine
- Hagelin
- Kryha
- Enigma
- Purple

Substitutie

Monoalfabetisch

- letter-voor-letter: Caesar, Monoalfabeet
- digram: Playfair
- meervoudig: Nomenclatuur, Code, Encicode
- gemengd: Monome-dinome, Fractionering

Polyalfabetisch periodiek

- eenvoudig: Porta, Vigenère, Beaufort
- langperiodiek: Hagelin, Enigma
- meer alfabetten: Multiplex

Polyalfabetisch aperiodiek

- Autoclaaf, One-Time-Pad

Nomenclatuur

- oudste voorbeelden ±1400 o.a. stadstaten Italië
- voornamelijk in diplomatiek verkeer gebruikt
- mengsel van letter, digram, trigram, cijfers, symbolen
- vervangers voor letters, digrammen, trigrammen
- homofonen zijn meerdere vervangers voor hetzelfde
- nullen om codebrekers van de wijs te brengen
- letter/cijfer-groepen voor namen, plaatsen, enz.
- paar honderd tot duizenden groepen
- speciale versies voor bepaalde personen

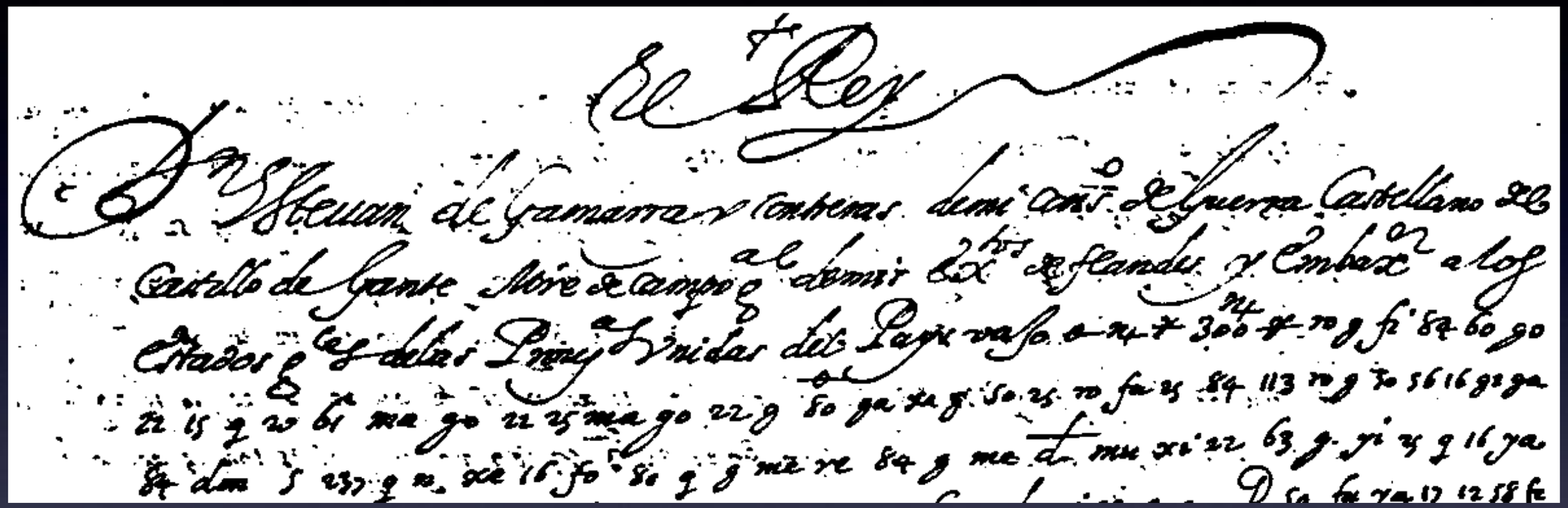
Diplomatieke instructie

El Rey = Philips IV (1605-1665)

datum *Madrid, 27 julio 1658*

- opvolger van Philips III in 1621
- vrede van Munster 1648
- Portugal wordt onafhankelijk
- verliest koloniën aan Engeland
- opstanden Catalonië en Napels

Aanhef



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 …

Aanleiding

In 1658 verovert de Franse generaal Turenne Duinkerken op de Spanjaarden

- Duinkerken wordt al genoemd in 1067
- sinds 1400 zijn er vestingwerken
- aanvoerhaven voor de Spaanse troepen
- basis voor kaapvaart tegen Nederlanders
- herhaaldelijk van eigenaar verwisseld
- evacuatie Engels expeditieleger in mei 1940

Cifra general in 1658

16e eeuw

8-11-1556
18-12-1562
12-7-1564
6-8-1567
26-5-1568
16-7-1571
1572
14-7-1572
21-6-1574
30-5-1575
1580
1582
1587
1585–1588

cifra particular
el duque de Alva
…

17e eeuw

1604
1614-1618
18-8-1647
1-10-1653
16-5-1676
1675-1689
1677-1700
26-3-1690
1691-1692
30-5-1575
1698

Cifra real que aora se usa y vino á principio de Otubre del año 1653

a	b	c	d	e	f	g	h	i	l	m	n
1 9 r	u x	t 2	s n	α 22 o	z y	c 23	m b	11 17 e	d 15	12 p	g f
o	p	q	r	s	t	v	x	y	z	j	
6 8 i	20 21	9 13	4 16	h 25	18 26	19 2 5	27 28	5 ρ	3 14	7 24	

Finales					Nulas		
a ÷	e +	i I	o //	u /	N	0–	F

Numeros			Duplices		
20	21	22	Z	θ	X

na	la	que	80
ne	le	que	81
ni	li	lla	82
no	lo	de	83
nu	lu	de	84

emperador	pez
emperatriz	piz
España	poz
Español	puz
embaxador	[illegible]
embaxada	[illegible]
Elector	[illegible]
esquizaro	100
execucion	101
exercito	102
empresa	103
experiencia	104
esperanza	105

… considerado ▫ el ▫ apretado ▫ estado ▫ en ▫ que ▫ daban ▫ las ▫ cosas ▫ de ▫ Flandes ▫ con ▫ la ▫ perdida ▫ de ▫ Dunquerque ▫ y ▫ suceso ▫ adberso ▫ … ▫ por ▫ la ▫ difficultad ▫ del ▫ paso ▫ de ▫ la ▫ canal ▫ de ▫ Inglaterra …

Monoalfabeet

Vervanging van A–Z door permutatie van A–Z

voorbeeld

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

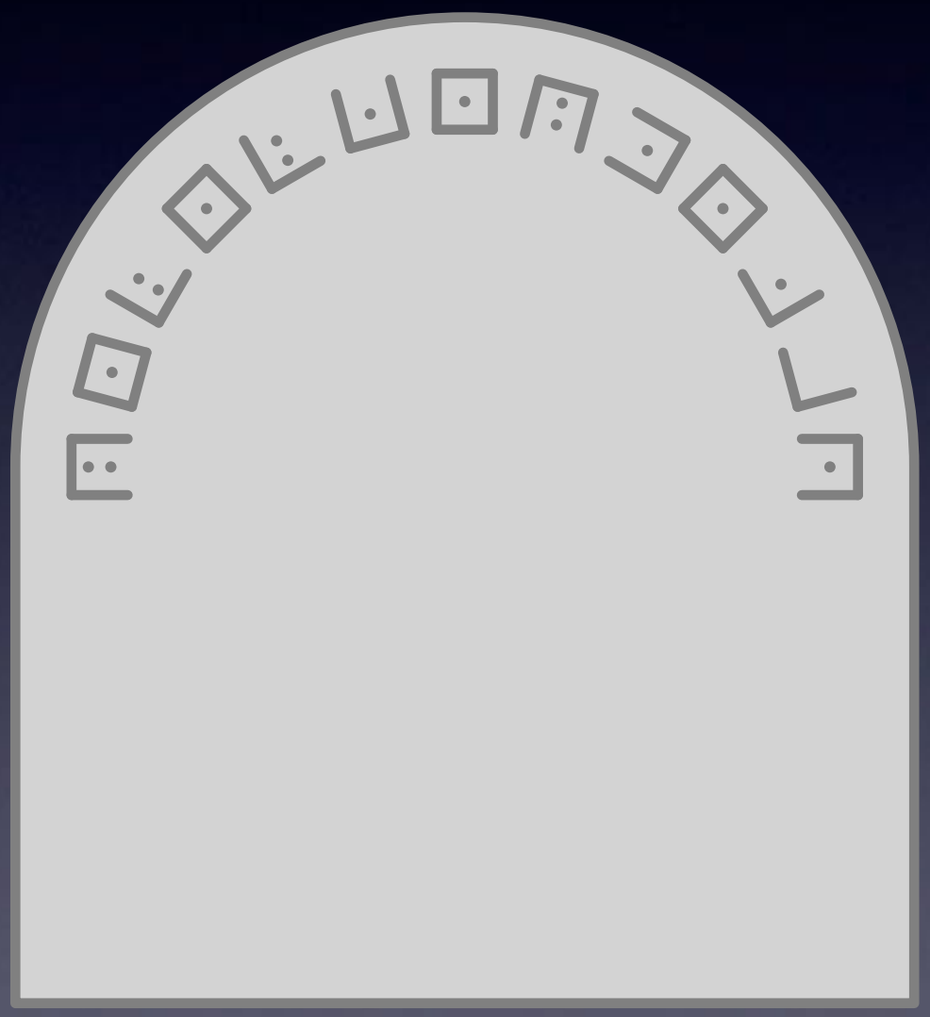
PEST → ATHJ

In theorie 26! sleutels maar veel hebben weinig effect

Caesar-substitutie is eenvoudige letter-opschuiving

Frequentie is gepermuteerde normale distributie
voor Caesar is dit verschoven normale distributie

Vrijmetselaars



Trinity Church, New York
graf van James Leeson † 1794

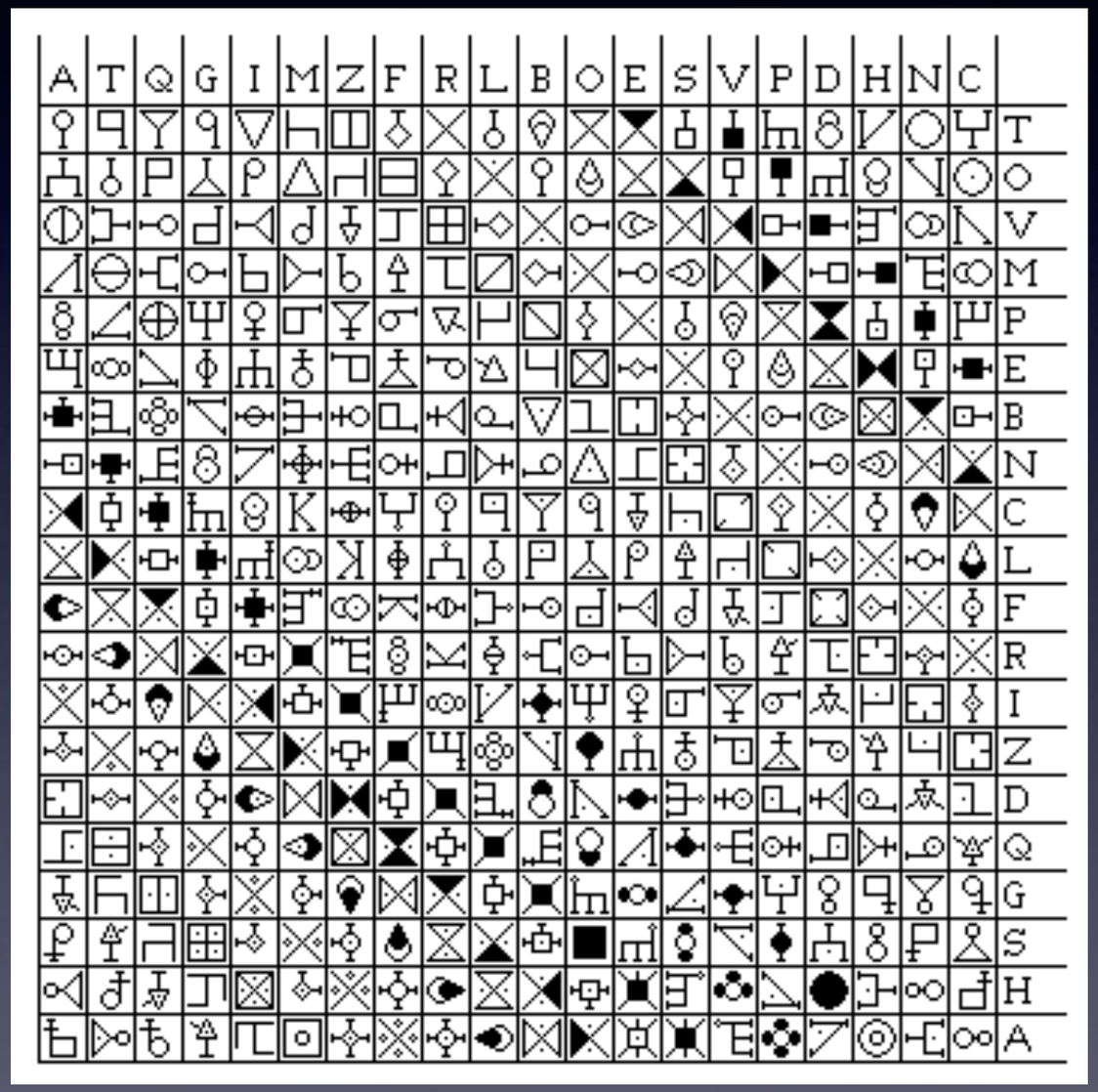
REMEMBER DEATH

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



digram-tabel van
Giovanni Battista della Porta

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

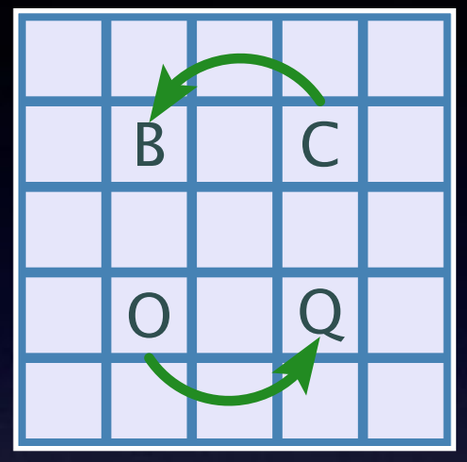
AA–ZZ geeft 676! sleutels

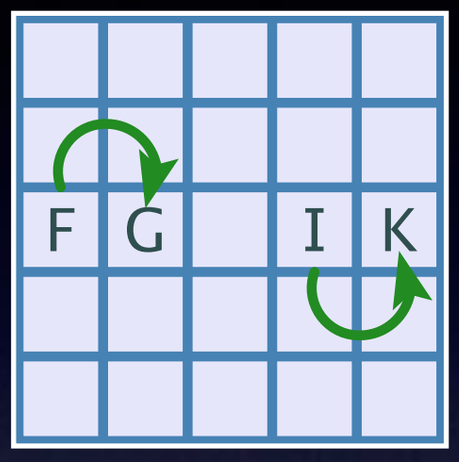
onthouden ondoenlijk

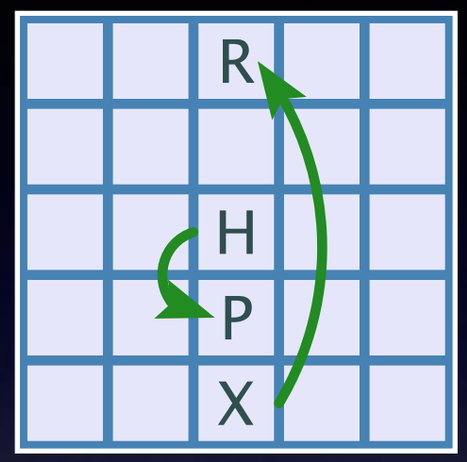
eenvoudiger schema's bijvoorbeeld de Playfair (Wheatstone, baron Playfair)

```
pt: NOOIT GEDACHT TOCH GEKREGEN
ct: ZRMQW BSIBH KVOQT LODPH ZODK
```

Playfair







STRANDBAL CO → BQ FI → GK HX → PR

Verdubbelde letter AAB … → AX AB … → RY TC …

Alf Mongé, Signal Corps Bulletin 1936

`BUFDA GNPOX IHOQY TKVQM PMBYD AAEQZ`

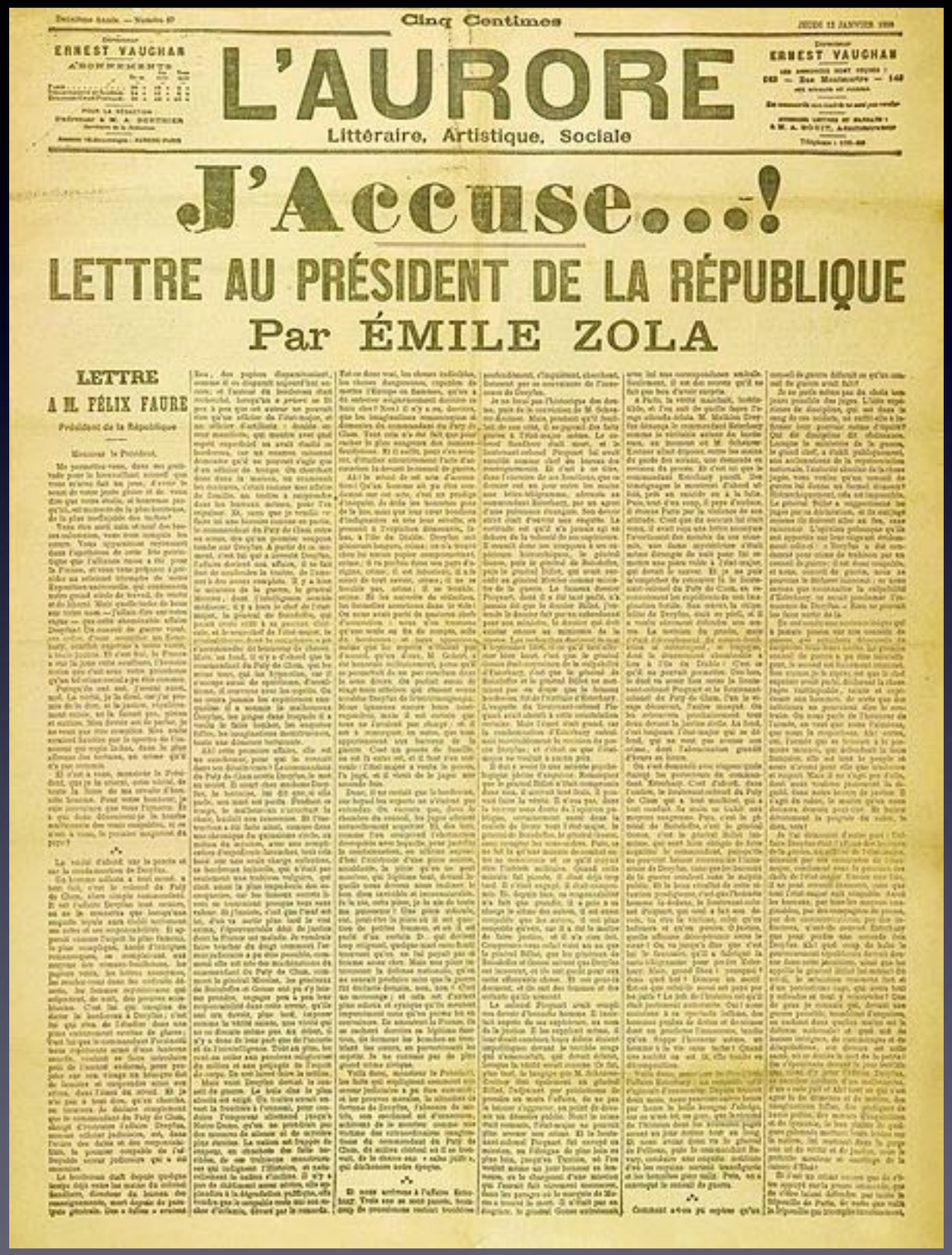
do let author know if you succeed

Code

Alfred Dreyfus verdacht als verrader in Franse generale staf

De werkelijke verrader blijkt veel later Ferdinand Esterhazy

Codeboek



Cinq Centimes

ERNEST VAUCHAN

L'AURORE

Littéraire, Artistique, Sociale

J'Accuse...!

LETTRE AU PRÉSIDENT DE LA RÉPUBLIQUE

Par ÉMILE ZOLA

LETTRE
A M. FÉLIX FAURE
Président de la République

arrestatie Dreyfus in 1894

veroordeling voor hoogverraad

verbannen naar Duivelseiland

Panizzardi, militair attaché van Italië stuurt telegram in Baravelli code foutief vertaald door geheime dienst

Emile Zola pamflet “J’accuse” eerherstel pas in 1906

One part code

Baravelli handelscode – deel van pagina 75

7500 Raziocinio
7501 Razionale
7502 Razza
7503 Di buona razza
7504 Di cattiva razza
7505 Il Re di
7506 S.M. il Re
7507 Reagire, Reagente
7508 Reagito
7509 Realista, Reale
…

7550 Reggimento Bersaglieri
7551 Reggimento Cavalleria
7552 Reggimento Linea
7553 Reggio Calabria
7574 Reggio d'Emilia
7555 Regia
7556 Regia cointeressata
7557 Regime
7558 Passato regime
7559 Sotto il regime
…

Two part code

Loopgraafcode uit de Eerste Wereldoorlog			
About to advance	BY	AF	Enemy machine gun fire
Ammunition exhausted	FB	AG	Gas is being released
Are advancing	PX	AP	Stretcher bearers needed
At	SX	AV	Recall working party
Attack failed	BM	AW	Casualties heavy
Attack successful	PF	AX	Using gas shells
Barrage wanted	XF	AZ	Relief completed
Be ready to attack	ZF	BJ	Situation serious

Encicode

```
Attack failed ammunition exhausted klaartekst
8971 1290 onvercijferde code
4481 0925 additief
2352 1115 vercijferde code = encicode
```

Optellen en aftrekken
zonder carry

About to advance	3256
Ammunition exhausted	1290
Are advancing	0032
At	9983
Attack failed	8971
Attack successful	4225
Barrage wanted	0283