

La Storia dei Messaggi Segreti fino alle Macchine Crittografiche

Wolfgang J. Irler



The Story from Secret Messages to Cryptographic Machines

Wolfgang J. Irler



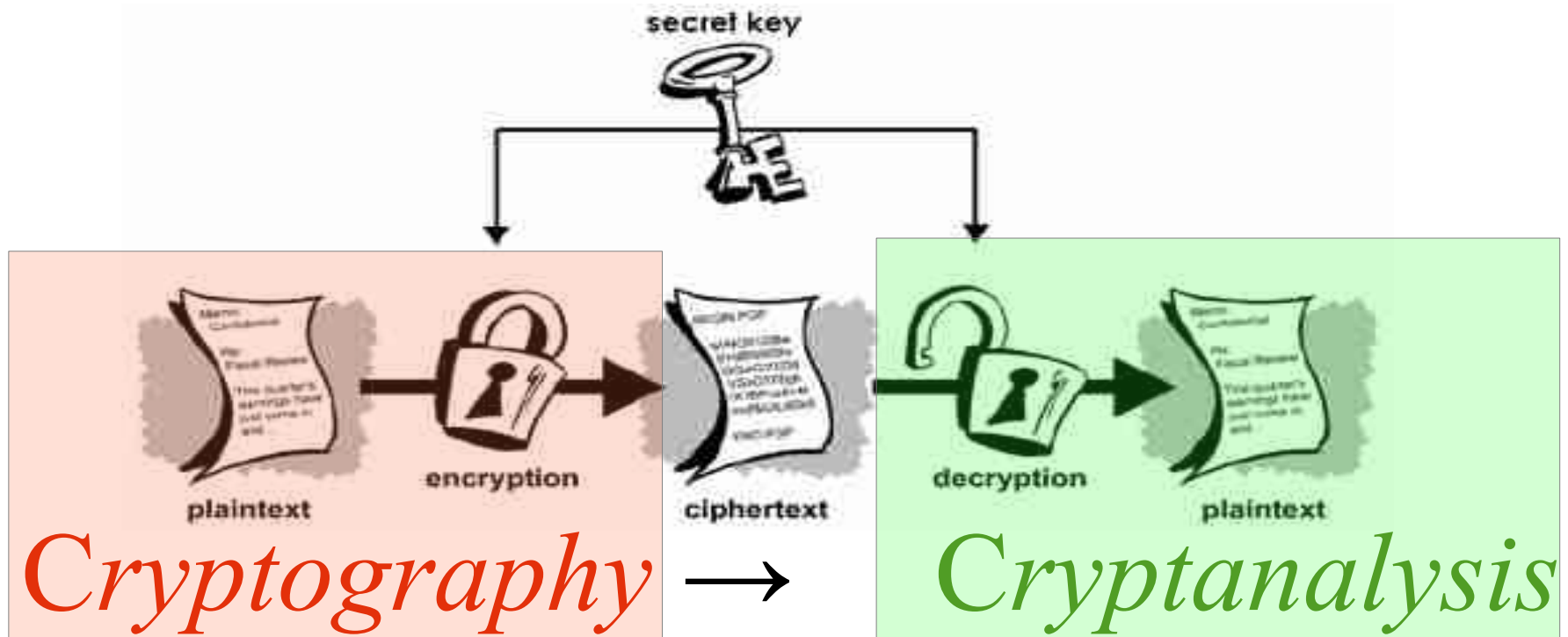
Problem

- Communicate without being understood by others
 - simple – rapid – secure
- via voice, speech
 - rare / strange language
(Navajo codetalker)
- written text
 - **Cryptology**
- non-verbal, images
 - Steganography
- commercial – military
 - telegram - cable – radio – communication
- Internet
 - email, private net, cell-phone



Cryptology

Secret Communication



Cryptography

- protect communication from being read by the wrong people
- Codes and Ciphers that are used to protect communications are Cryptographic Systems
- the application of Codes and Ciphers to messages to make them unreadable is called Encryption of plaintext
secret key + algorithm
- The resulting messages are called Cryptograms
- People who create and use cryptographic systems are called Cryptographers



Cipher systems

- encryption is carried out on **single characters** or **groups of characters** without regard to their meaning

- messages encrypted by a cipher system are **enciphered**
plaintext → **cyphertext**

- Alphabetical permutation / transposition / substitution

- Skytala
- Caesar-cipher
- Leon Battista Alberti
- Trithemius
- Vigenaire
- Polybius - ADFG(V)X



	1	2	3	4	5
1	A	B	C	D	E
2	F	G	H	I/J	K
3	L	M	N	O	P
4	Q	R	S	T	U/V
5	W	X	Y	Z	



	A	D	F	G	X
A	w	i	k	p	e
D	d	a	z	y	x
F	v	u	t	s	r
G	q	o	n	m	l
X	h	g	f	c	b



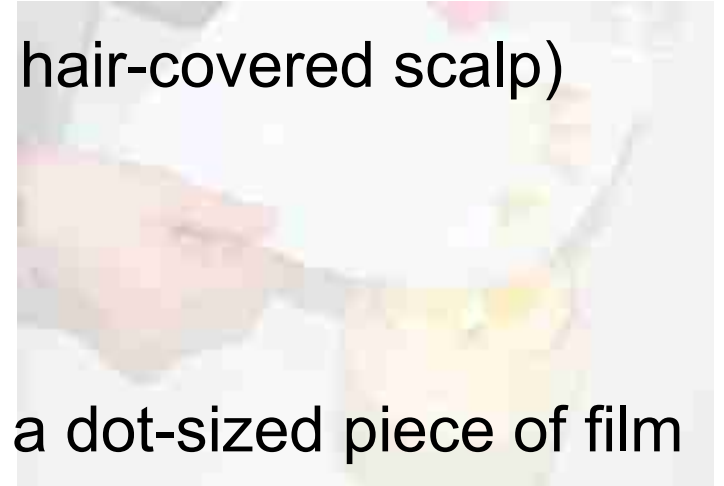
Codes - Codebooks

- concerned with meanings, words or phrases
- messages encrypted by a code system are encoded
- **key** = Codebook
- **algorithm** = search
-
- but: Morse code, binary code, Baudot code, TTY code, program code, punched-card code, etc.

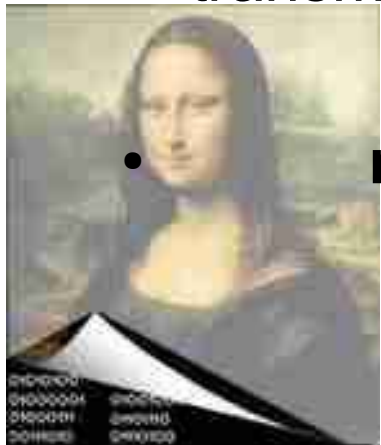


Concealment Systems

- plaintext, but **hidden** (message on the hair-covered scalp)
- **invisible** ink, highlighted letters/words
- **reduce** a message photographically to a dot-sized piece of film
- transmit a message, **compressed** as a burst of noise
- **modify** insignificant color bytes in an unsuspecting image



← **steganography**



Security – Key - Algorithm

Security depends on the
secrecy of the **key**,
not the secrecy of the
algorithm



Classical Cryptography

- Greece – Archilochus (700BC) ➤ Skytale
- Polybios (200BC-120BC) ➤ Polybios-Quadrat
- Julius Caesar (101BC-44BC) ➤ Caesar-Cypher
- Leon Battista Alberti (1404-1472) ➤ disk
- Johannes Trithemius (1462-1516) ➤ Tabula recta
- Blaise de Vigenère (1523-1596) ➤ " with keyword
- Giambattista della Porta (1535-1615) ➤ monoalph. Subst.
- Charles Wheatstone (1802-1875) ➤ 5*5 table
Lyon Playfair (1818-1898)
- Fritz Nebel (1891–1967) ➤ ADF(V)G



Monoalphabetic Systems

- Skytala  Archilochus 700BC → **key** = \emptyset of the rod
Sparta

- Caesar (101BC-44BC)



→ abcdefghijklmnopqrstux
 DEFGHIKLMNOPQRSTUVWXYZABC
key=D(3)

- Leon Battista Alberti (1404-1472)





→ abcdefghijklmnopqrstuvwxyz
 NMLKJIHGFEDCBAZYXWVUTSRQPO
key=n→A



Polyalphabetic Systems: Trithemius - Vigenère

- Tabula recta
- advance alphabet every letter of the plaintext (**no key**)
- help → HFNS
1234
- advance alphabet in order of the **key** = BETA
1234
- help → IIEP
1234

	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
1	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
2	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
3	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
4	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
5	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
	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	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



Giovan Battista della Porta (1535 – 1615)

- DE FVRTIVIS LITERARVM NOTIS VVLGO DE ZIFERIS
- LITERAE CLARIS → key
- Substitute:
on-top with below
below with on top
- key = **AB**: **h**elp ↔ uryc

120 DE FVRT. LIT. NOTIS.

LITERAE SCRIPTI.

AB	a	b	c	d	e	f	g	h	i	l	m
CD	n	o	p	q	r	s	t	u	x	y	z
EF	a	b	c	d	e	f	g	h	i	l	m
GH	x	y	z	n	o	p	q	r	f	t	u
IL	a	b	c	d	e	f	g	h	i	l	m
MN	u	x	y	z	n	o	p	q	r	f	t
OP	a	b	c	d	e	f	g	h	i	l	m
QR	f	t	u	x	y	z	n	o	p	q	r
ST	a	b	c	d	e	f	g	h	i	l	m
VX	q	r	f	t	u	x	y	z	n	o	p
YZ	a	b	c	d	e	f	g	h	i	l	m
	o	p	q	r	f	t	u	x	y	z	n

LITERAE CLARIS.

Source: <http://www.mathe.tu-freiberg.de/~hebisch/cafe/kryptographie/dellaporta.html>



Mixed Monoalphabetic Systems

- Keyword— CRYPTOGRAPHIC

CRYPTOGAHIBDEFJKL MNQSUVWXZ

- Keyword— ARTILLERY

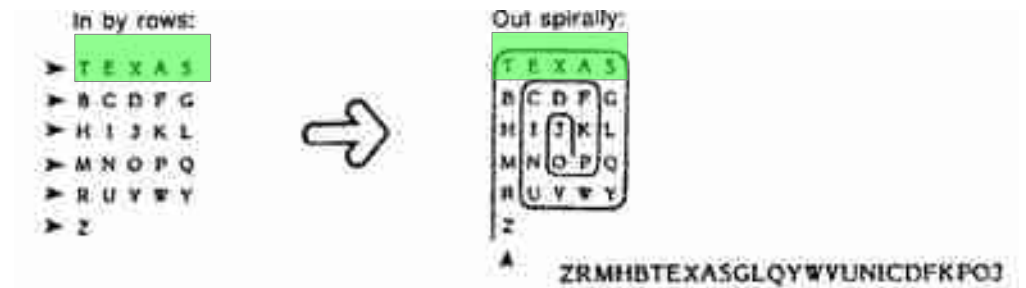
A	R	T	I	L	E	Y
B	C	D	F	G	H	J
K	M	N	O	P	Q	S
U	V	W	X	Z		

- Keyword— CALIFORNIA
order letters

2	1	5	4	3	7	8	6
C	A	L	I	F	O	R	N
B	D	E	G	H	J	K	M
P	Q	S	T	U	V	W	X
Y	Z						

ADQZCBPYFHUIGTLESNMXOJVRKW

- Keyword— TEXAS



Classic Cryptography

- Greece – Archilochus (700BC) ➤ Skytale
- Polybios (200BC-120BC) ➤ Polybios-Quadrat
- Julius Caesar (101BC-44BC) ➤ Caesar-Cypher
- Leon Battista Alberti (1404-1472) ➤ disk
- Johannes Trithemius (1462-1516) ➤ Tabula recta
- Blaise de Vigenère (1523-1596) ➤ " with keyword
- Giambattista della Porta (1535-1615) ➤ monoalph. Subst.
- **Charles Wheatstone** (1802-1875) ➤ 5*5 table
• **Lyon Playfair** (1818-1898)
- Fritz Nebel (1891–1967) ➤ ADF(V)G



Digraphic Playfair Cipher

- 2 Rules:

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

- *rectangular rule*

“the shot heard round the world”

p: **th** es ho th ea **rd** ro un dt he wo rl dx
 c: **QB** CU PQ QB NE **AJ** DT ZU RO CP VQ GM GV

- *encipher right, decipher left and encipher below, decipher above*

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

key = DIGRAPH



Digraphic Substitution Matrix

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

“attack at dawn”

p: **at** **ta** ck at da wn
 c: **PC** **PZ** FN PC CZ AK

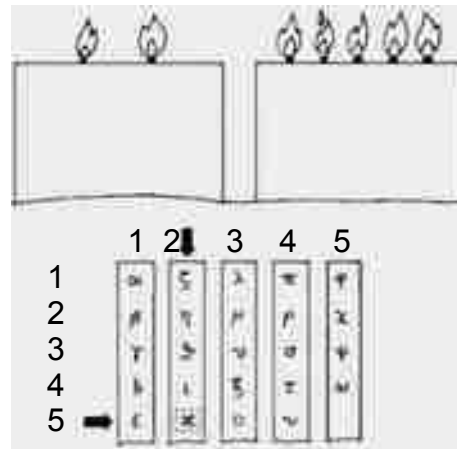


Classic Cryptography

- Greece – Archilochus (700BC) ➤ Skytale
- **Polybios** (200BC-120BC) ➤ Polybios-Quadrat
- Julius Caesar (101BC-44BC) ➤ Caesar-Cypher
- Leon Battista Alberti (1404-1472) ➤ disk
- Johannes Trithemius (1462-1516) ➤ Tabula recta
- Blaise de Vigenère (1523-1596) ➤ " with keyword
- Giambattista della Porta (1535-1615) ➤ monoalph. Subst.
- Charles Wheatstone (1802-1875) ➤ 5*5 table
- Lyon Playfair (1818-1898)
- **Fritz Nebel** (1891–1967) ➤ **ADF(V)G**

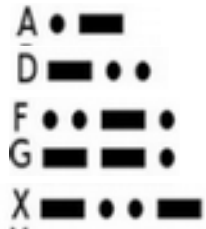


Polybios



ADFG(V)X digraphs

- **ADFGX**



	A	D	F	G	X
A	a	b	c	d	e
D	f	g	h	i/j	k
F	l	m	n	o	p
G	q	r	s	t	u
X	v	w	x	y	z

- **ADFGVX**

	A	D	F	G	V	X
A	q	w	e	r	t	y
D	u	i	o	p	a	s
F	d	f	g	h	j	k
G	l	1	2	3	4	5
V	7	8	6	9	0	z
X	x	c	v	b	n	m



- **h**elp = **D**FAX FAFX

- **h**elp = **F**GAF GADG



Cryptanalysis

- concerned with **solving** the cryptographic systems
- read the text of encrypted messages (**Cryptograms**)
cyphertext → **plaintext**
- recover the Cryptographic Systems used (**Codes** or **Ciphers**)
which system (=algorithm)
which key
- recover the original message for its potential intelligence value
- for future messages in the same or similar systems



Monoalphabetic Cryptanalysis

- monoalphabetic ciphers preserve exactly the **same letter frequencies** as found in **plaintext**:

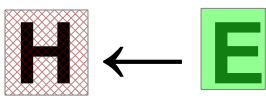


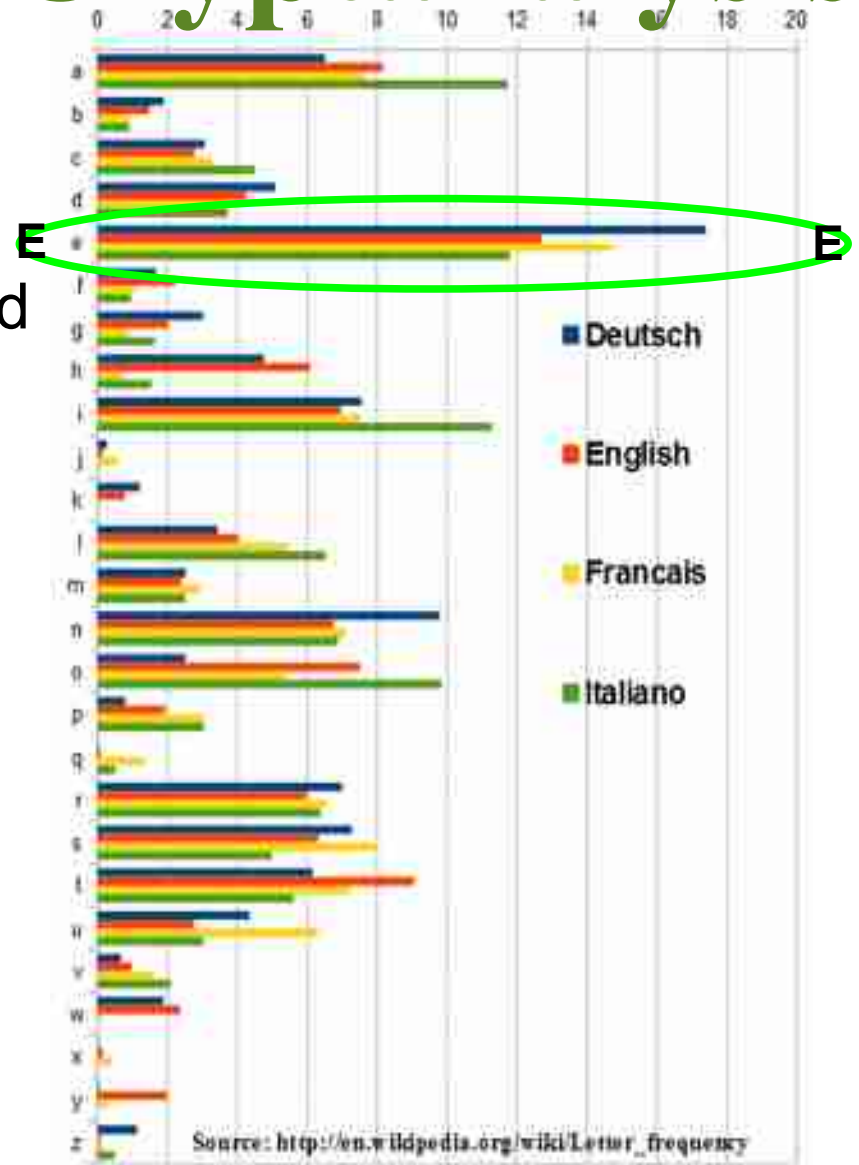
 A B C D E F G H I J K L M N O P Q R S T U V W X Y Z

count letters in **ciphertext**:



 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

- 
- same for mixed monoalphabetic



ZDXWWW EJKAWO FECIFE WSNZIP PXPKIY URMZHI JZTLBC YLGDYJ
 HTSVTV RRYVEG EXNCGA GGOVRE FHZCIB EWLGGR BZXQDQ DGGIAK
 YHJYEQ TDLQTH HBIID RRDYS RBYJFZ AIRCWT UCVYTW YKPMK
 CKHVEX VXYCS WGGAL OUVVOT GCSVY LIRLYE SDDDC PCGVJX
 QXAUIP PXZQIJ JIUWYH COVWMJ UZUJHL DWHPER UBSRUJ HGAAPR
 CRWVHI FRNTQW AJVWRT ACAKRD OZKIIB VIQGBK IJCWHF GTTSSE
 EXFIPJ KICASQ IOUQTP ZSGXGH YTYCTI BAZSTN JKMFXI RERYWE

100% secure: One-Time-Pad

- “long” Vigenère key:
 (key-worm)
 letters from a book page
 telephone book
 printed letter/number list

- **random numbers**
 creation:
 human
 irrational number sequence
 wheels (*periodic!*)
 computer (*pseudo-random*)

process (radioactive decay)

physical entropic information (*systematic bias*)

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

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



Quasi-One-Time-Pad

- machine-created bit-stream ciphers (Lorenz Schlüsselzusatz Siemens-Geheimschreiber)
wheels with prime-number teeth (“Tunny”)



- **key** = seed setting

- encryption: binary adding: plaintext+bit-sequence:
- decryption: xor-ing the ciphertext

XOR Truth Table		
Input		Output
p	q	
0	0	0
0	1	1
1	0	1
1	1	0

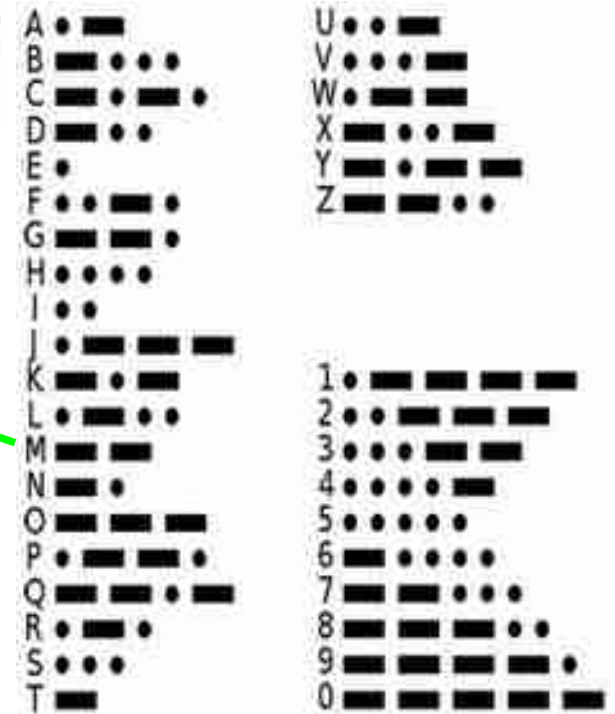
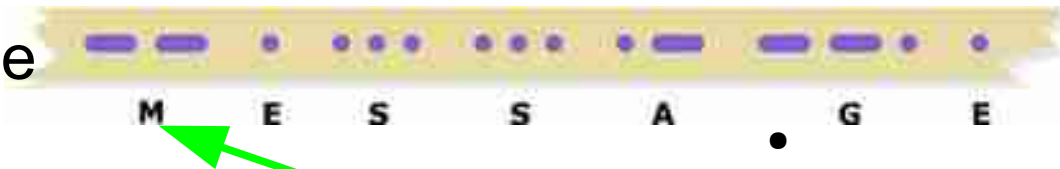
$$p \oplus q = (p \vee q) \wedge \neg(p \wedge q)$$

- cracked by COLOSSUS

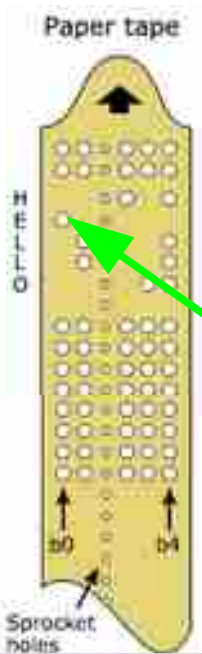


Transmission Codes

- Morse



- Baudot
- Murray



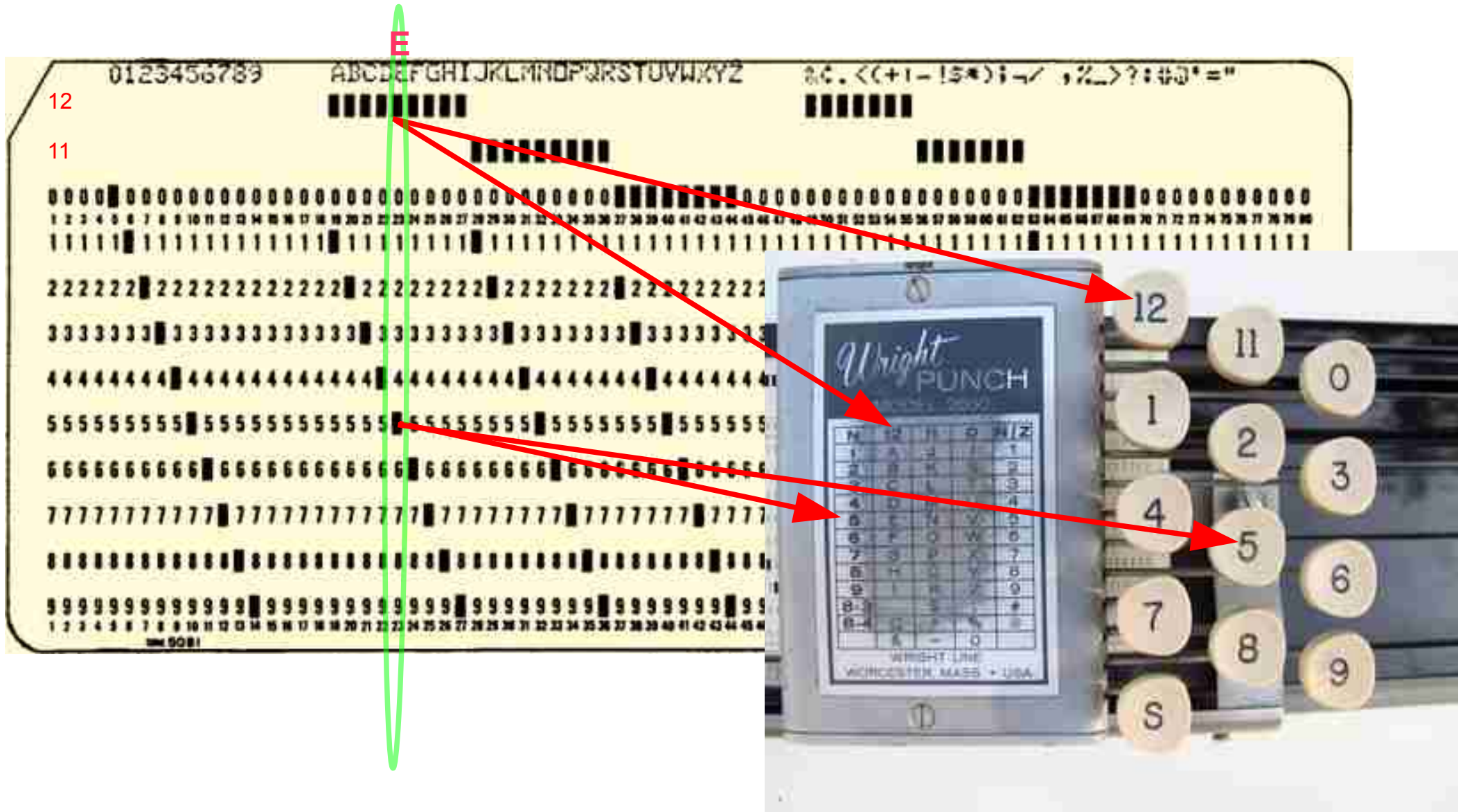
Letter	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	Blank	Stop	Letter	Number	Blank	Not a digit			
1																																			
2																																			
3																																			
4																																			
5																																			
6																																			
7																																			
8																																			
9																																			
0																																			

The International Telegraph Alphabet

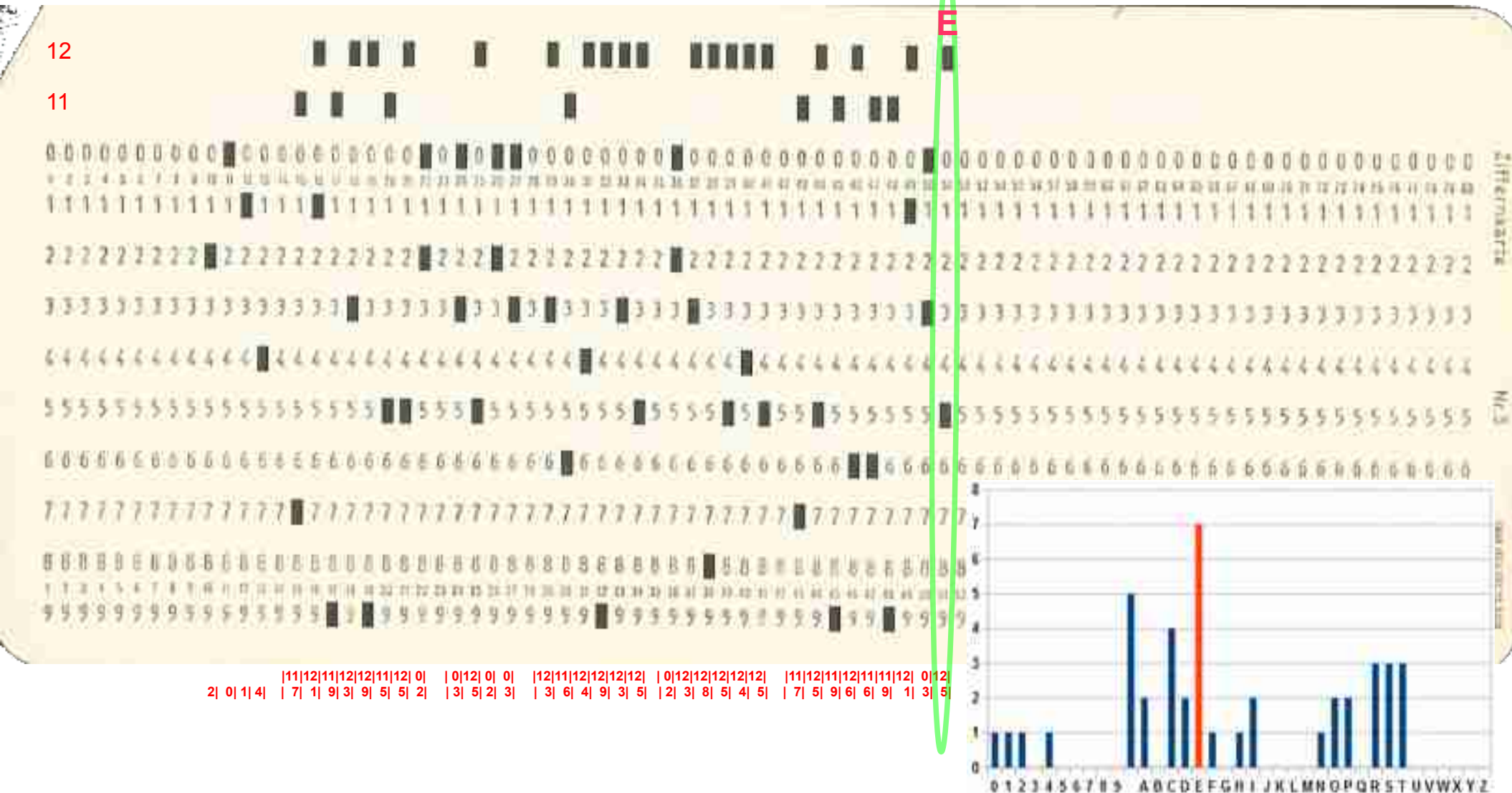
Source: http://en.wikipedia.org/wiki/Baudot_code



Punched Card Code



Quiz: decode the card



From the disk to the rotor

- Alberti



- monoalphabetic disk

- Jefferson



- polyalphabetic roll



- Eduard H. Hebern (US)

- 5 rotors connected by current

- Hugo A. Koch (NL)

- rotors - lamps

- Arthur Scherbius (DE)

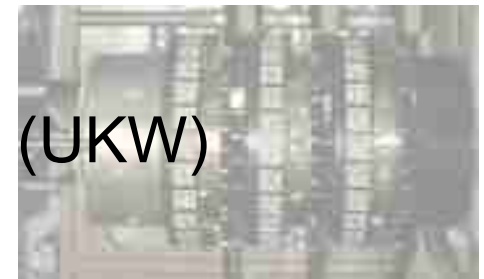
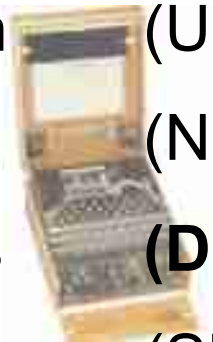
- with reflector (UKW)

- Arvid G. Damm (SE)

- lamps

- Boris C.W. Hagelin
(SE-US-CH: Crypto AG)

- printer



Cryptographic Machines

- rotor-setting:

- pin-wheel-key (pseudo-random)



- M209 (USA)



- Hagelin-C38S

printed tape

- code-card-key (pseudo-random)

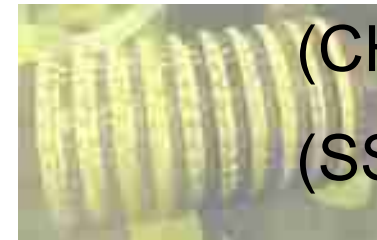
- keyboard:



- **Enigma** (DE)

(non reciprocal substitution)
output lamps

- Nema (CH)

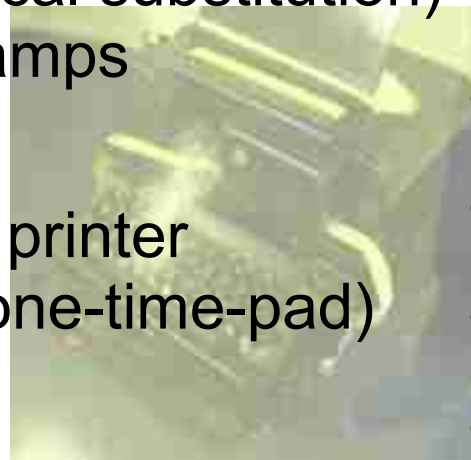


- Fialka (SSSR)

teletype printer
(pseudo one-time-pad)

- **Lorenz Schlüsselzusatz**

- **Siemens T-52** (DE)



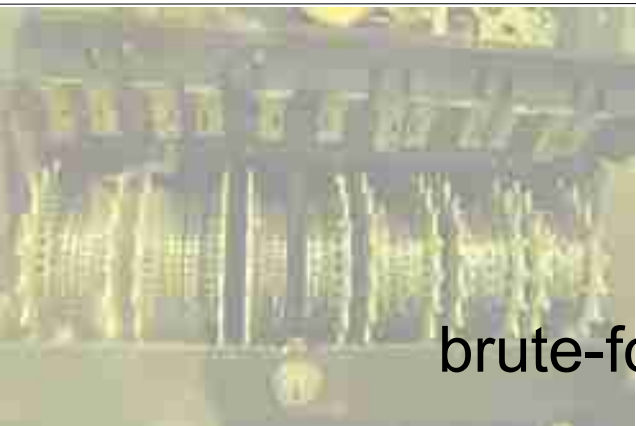
Bletchley-Park Cryptanalysis



- **Enigma** (25 models, 50 radio-networks)
 - Polish Bombe
 - Turing Bombe:
crib (word/phrase)→**menu**+
brute-force attack (36 Enigma-simulators)
→ **daily key**

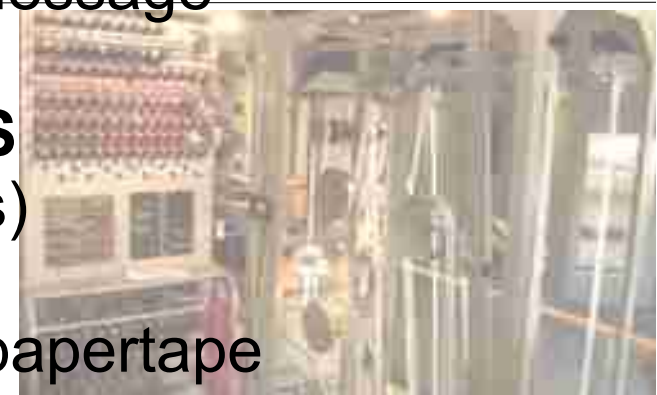


non reciprocal substitution → Italian message: only “LLLLLLL...”
→ NO “L” in message



- **Lorenz-SZ-40** (Tunny)
cracked by **COLOSSUS**
1700 valves (vacuum tubes)

brute-force **xor-ing** plaintext + crib-papertape



thanks – grazie – danke

Wolfgang J. Irler

