La Storia dei Messaggi Segreti

fino alle Macchine Crittografiche

Wolfgang J. Irler

The Story from Secret Messages to Cryptographic Machines

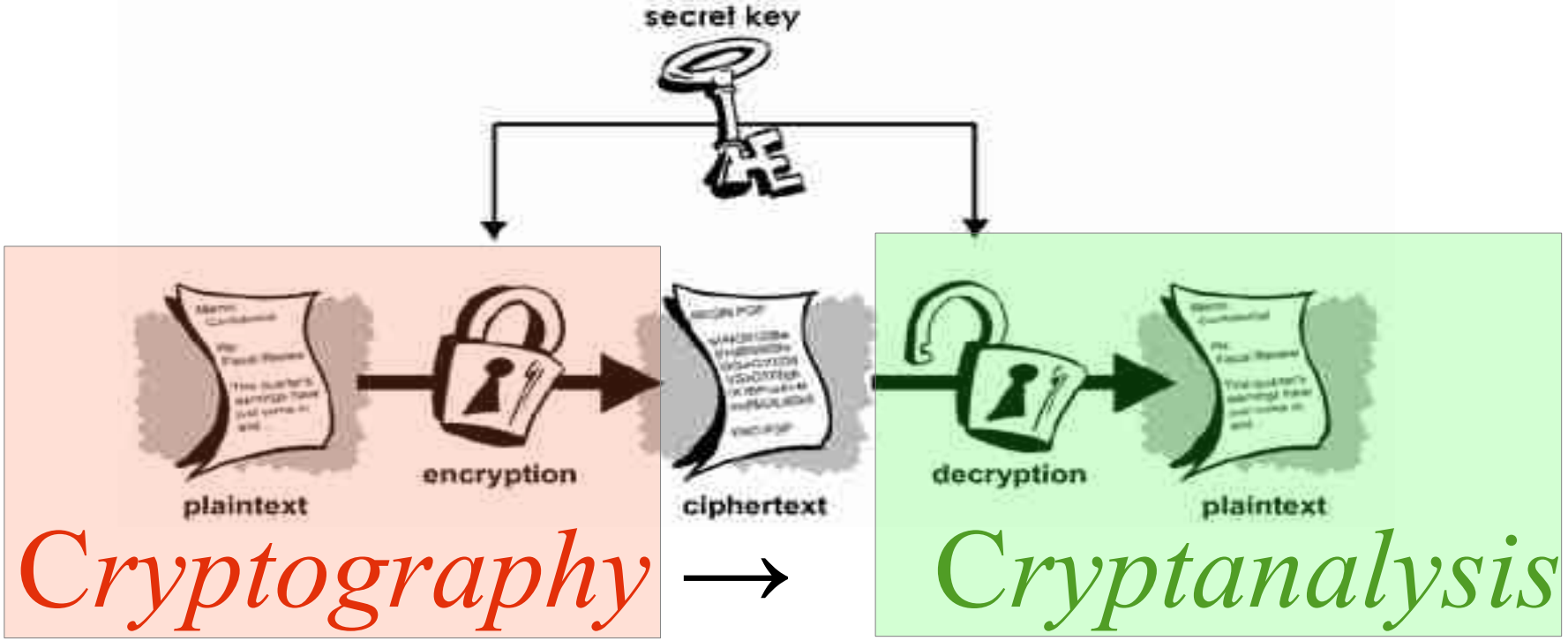
Wolfgang J. Irler

Problem

- Comunicate 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 – comunication
- Internet
  - ➢email, private net, cell-phone

Cryptology

Secret Communication



Cryptography

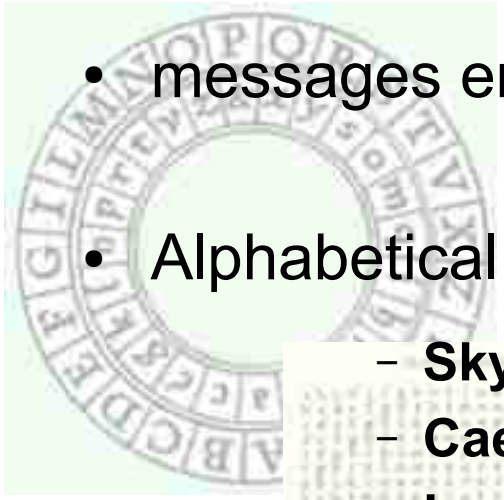
- **protect** communication from being read by the wrong people
- **Codes** and **Ciphers** that are used to protect communications are **Cryptographic Systems**
- the application of Codes and Ciphers to messages to make them unreadable is called **Encryption** of plaintext

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	

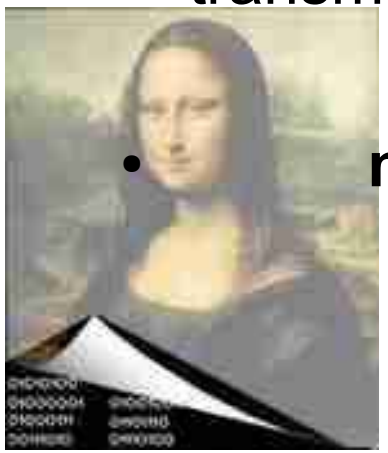
	A	D	F	G	X
A	w	i	k	p	e
D	d	a	z	y	x
F	v	u	t	s	r
G	q	o	n	m	l
X	h	g	f	c	b

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 unsuspicious 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* Sparta ➔ key = Ø of the rod

- Caesar *(101BC-44BC)*

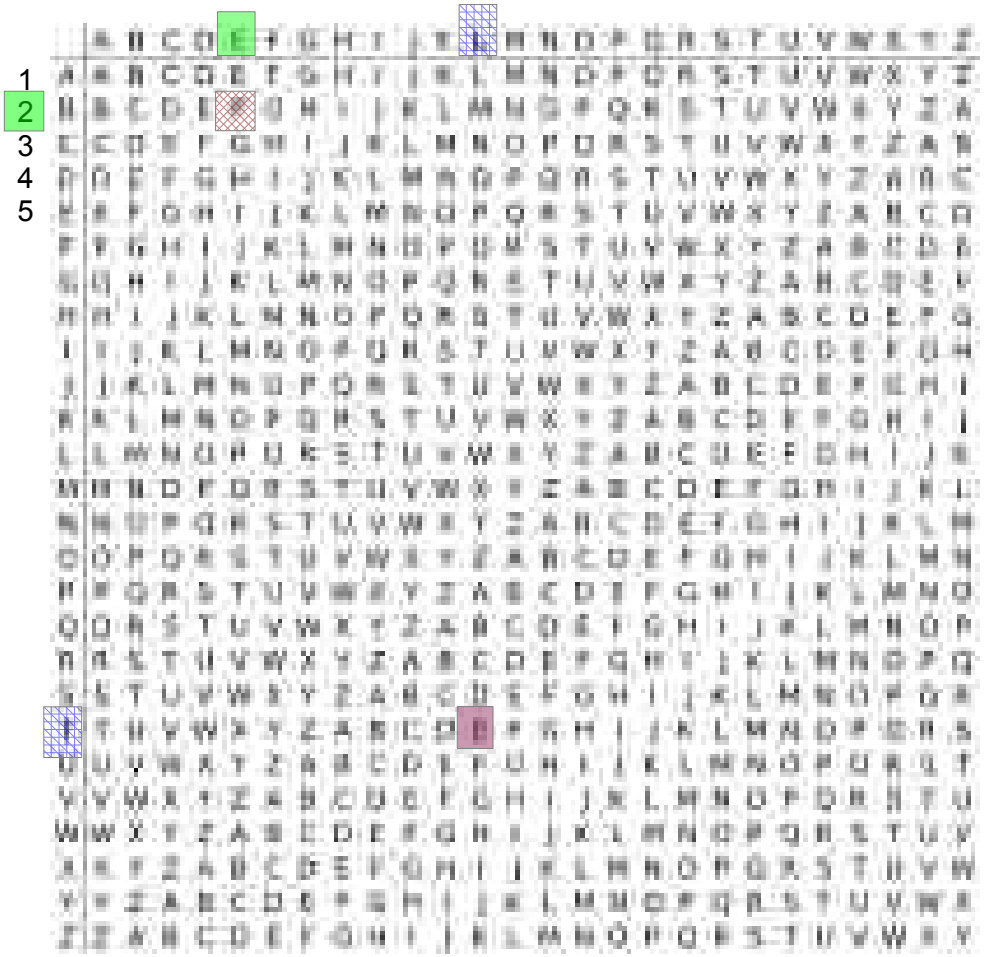
➔ abcdefghiklmnopqrstux
DEFGHIKLMNOPQRSTUXABC
key=D(3)

➔ abcdefghijklmnopqrstuvwxyz
NMLKJIHGFEDCBAZYXWVUTSRQPO
key=n→A

- Leon Battista Alberti *(1404-1472)*

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

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: help ↔ uryc

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

Mixed Monoalphabetic Systems

- Keyword— CRYPTOGRAPHIC

CRYPTOGAHIBDEFJKLMNQSUVWXZ

- Keyword— ARTILLERY

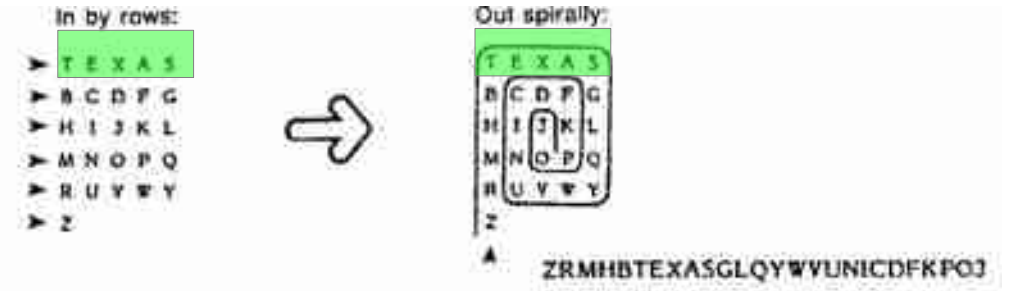
A	R	T	I	L	E	Y
B	C	D	F	G	H	J
K	M	N	O	P	Q	S
U	V	W	X	Z		

- 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

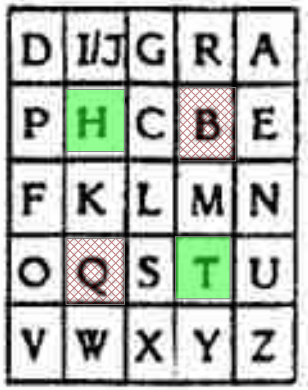


Classic Cryptography

- 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

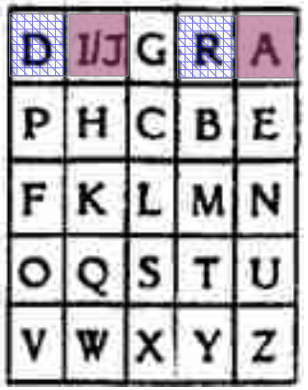
- 2 Rules:



- *rectangular rule* *"the shot heard round the world"*

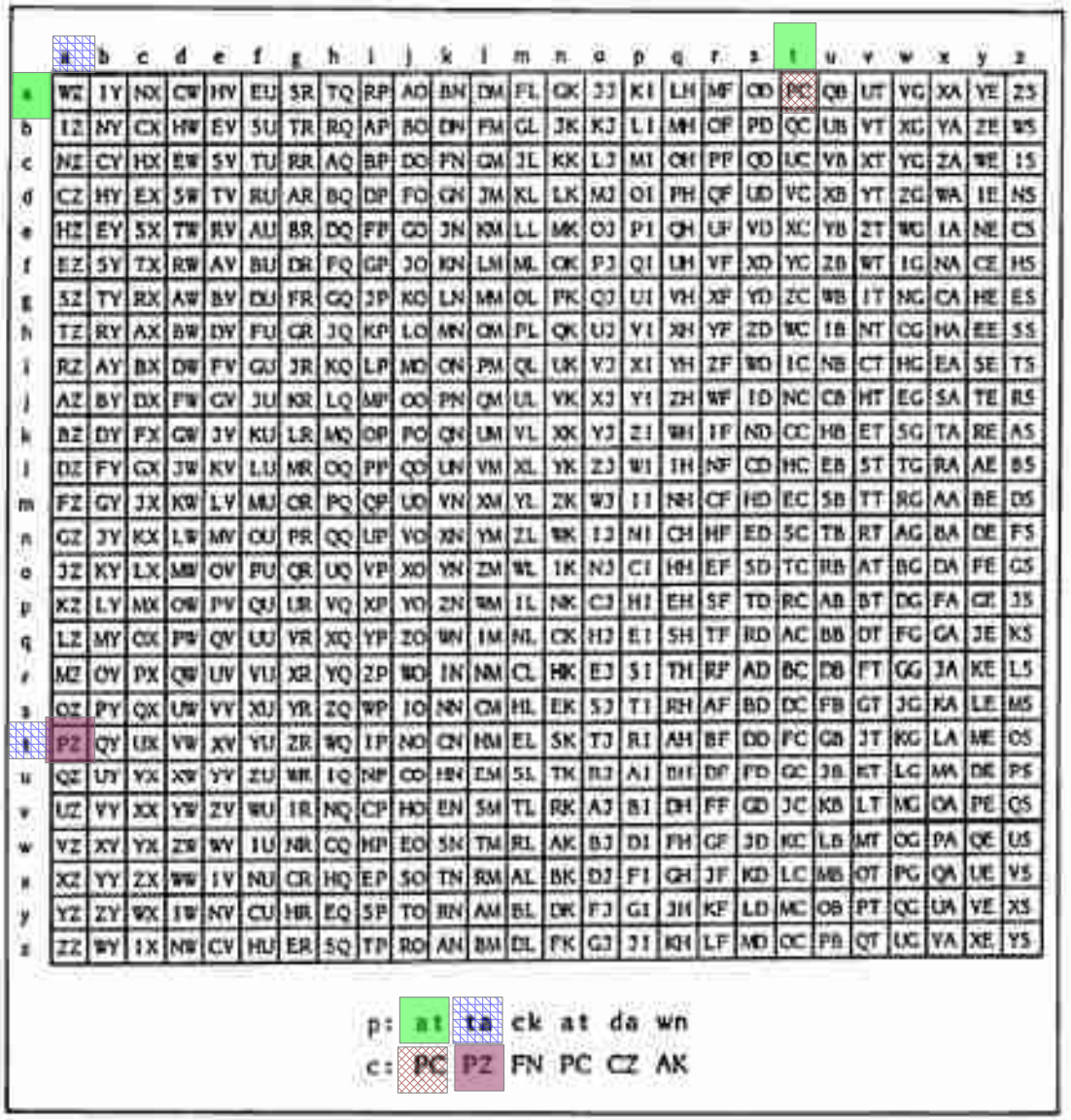
p:	th	es	ho	th	ea	rd	ro	un	dt	he	wo	rl	dx
c:	QB	CU	PQ	QB	NE	AJ	DT	ZU	RO	CP	VQ	GM	GV

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



key = DIGRAPH

Digraphic Substitution Matrix

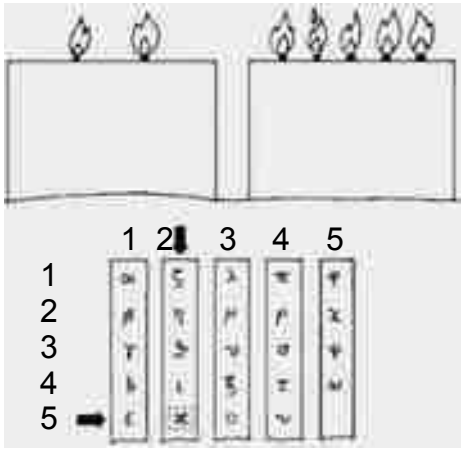


"attack at dawn"

Classic Cryptography

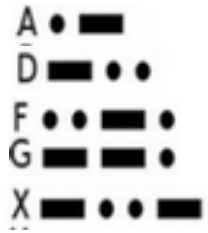
- Greece – Archilochus *(700BC)* ➢Skytale
- **Polybios** *(200BC-120BC)* ➢Polybios-Quadrat
- Julius Caesar *(101BC-44BC)* ➢Caesar-Cypher
- Leon Battista Alberti *(1404-1472)* ➢disk
- Johannes Trithemius *(1462-1516)* ➢Tabula recta
- Blaise de Vigenère *(1523-1596)* ➢ " with keyword
- Giambattista della 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

	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

- **ADFGVX**

- help = DFAX FAFX
- help = FGAF 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

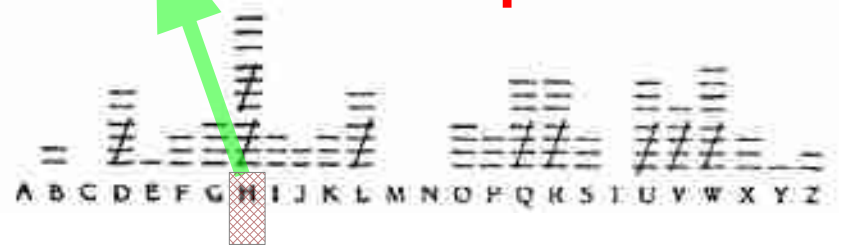
- recover the original message for its potential intelligence value

- for future messages in the same or similar systems

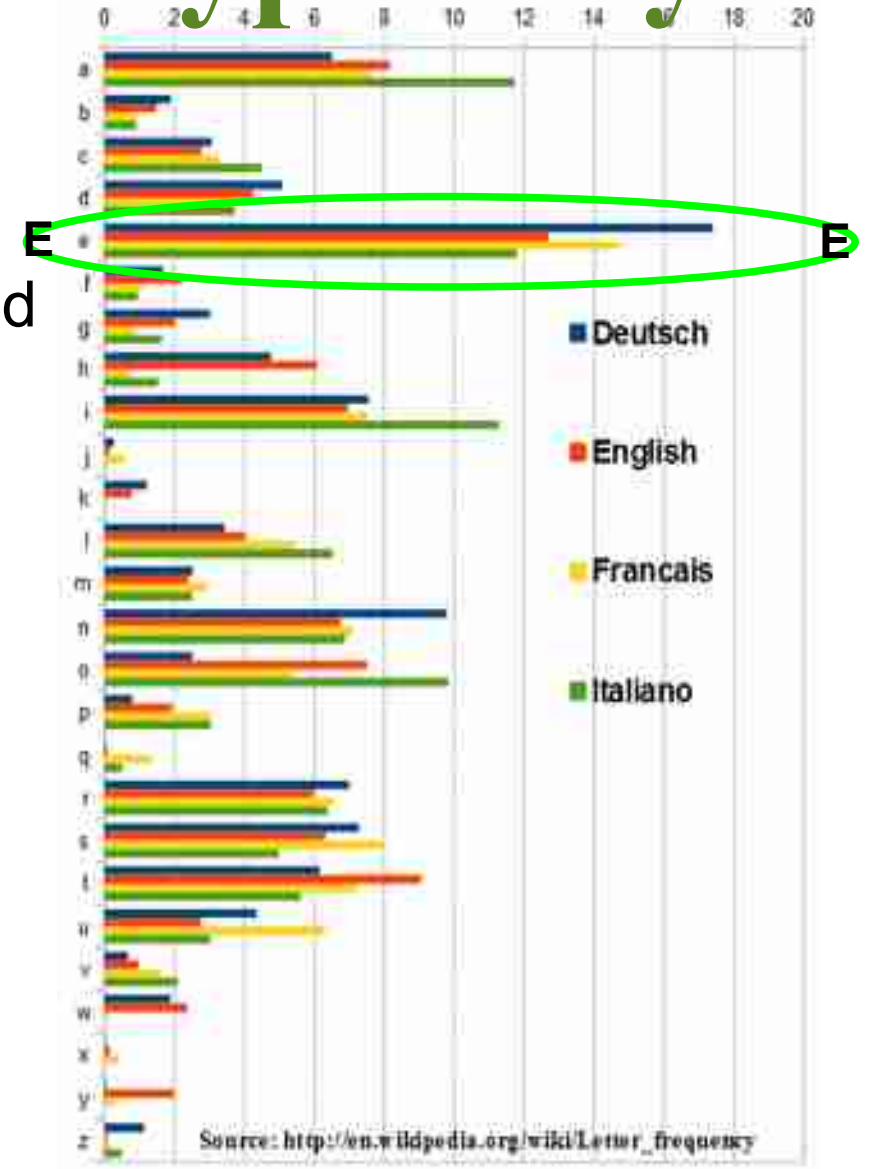
Monoalphabetic Cryptanalysis

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

count letters in **ciphertext**:



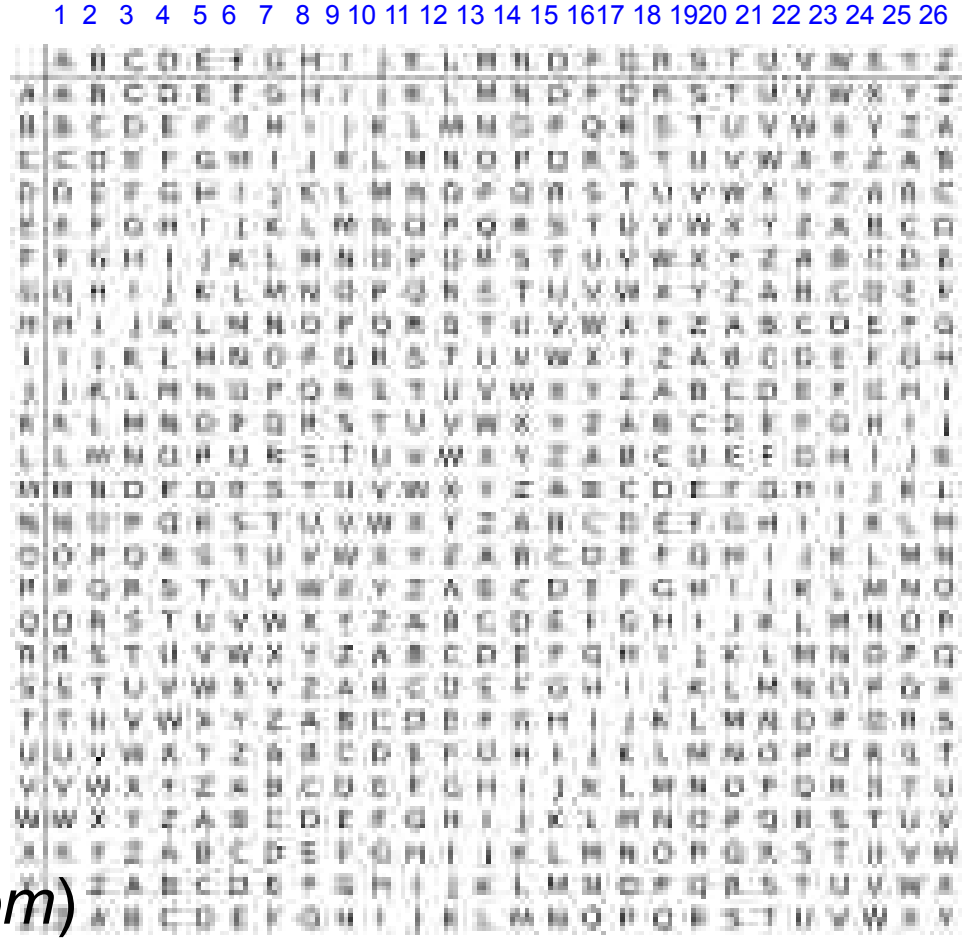
- **H** ← **E**
- same for mixed monoalphabetic



ZDXWWW EJKAWO FECIFE WSNZIP PXPKIY URMZHI JZTLBC YLGDYJ
HTSVTV RRYYEG EXNCGA GGQVRF FHZCIB EWLGGR BZXQDQ DGGIAK
YHJYEQ TDL QT H BI I ER DY S RBYJFZ AIRCWI UCVXTW VKPQMK
CKHVEX VXY CS W G A OUV VQ GC V LI BLYE S 8D DC CGVJX
QXAUIP PXZQIJ JIUWYH COVWMJ UZOJHL 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*)

Quasi-One-Time-Pad

- machine-created bit-stream ciphers (Lorenz Schlüsselzusatz Siemens-Geheimschreiber)

  wheels with prime-number teeth ("Tunny")

- key = seed setting

- encription: binary adding: plaintext+bit-sequence:
- decription: xor-ing the ciphertext

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

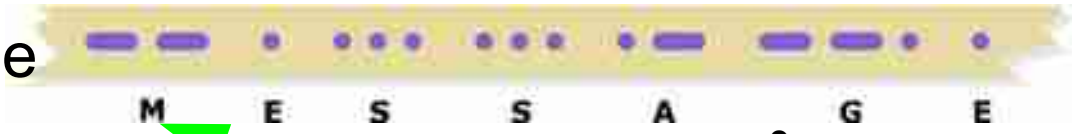
XOR Truth Table

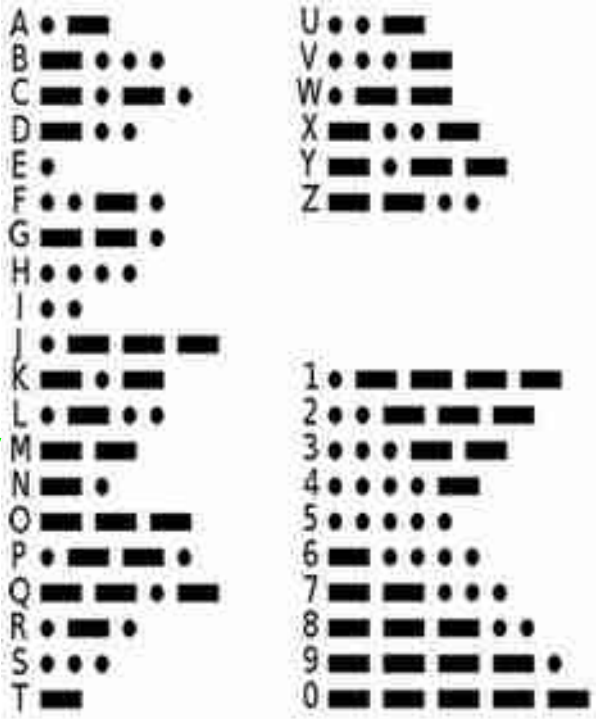
Input		Output
p	q	
0	0	0
0	1	1
1	0	1
1	1	0

- cracked by COLOSSUS

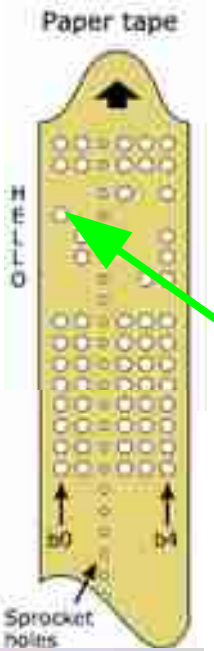
Transmission Codes

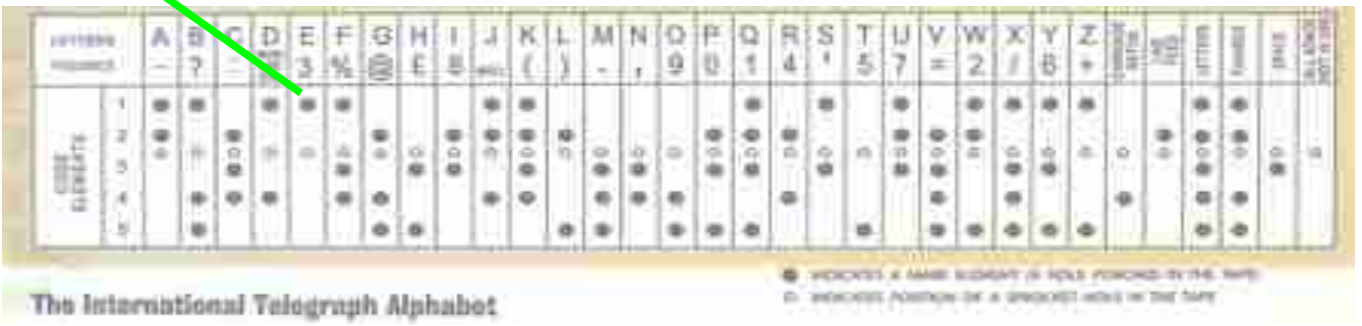
- Morse





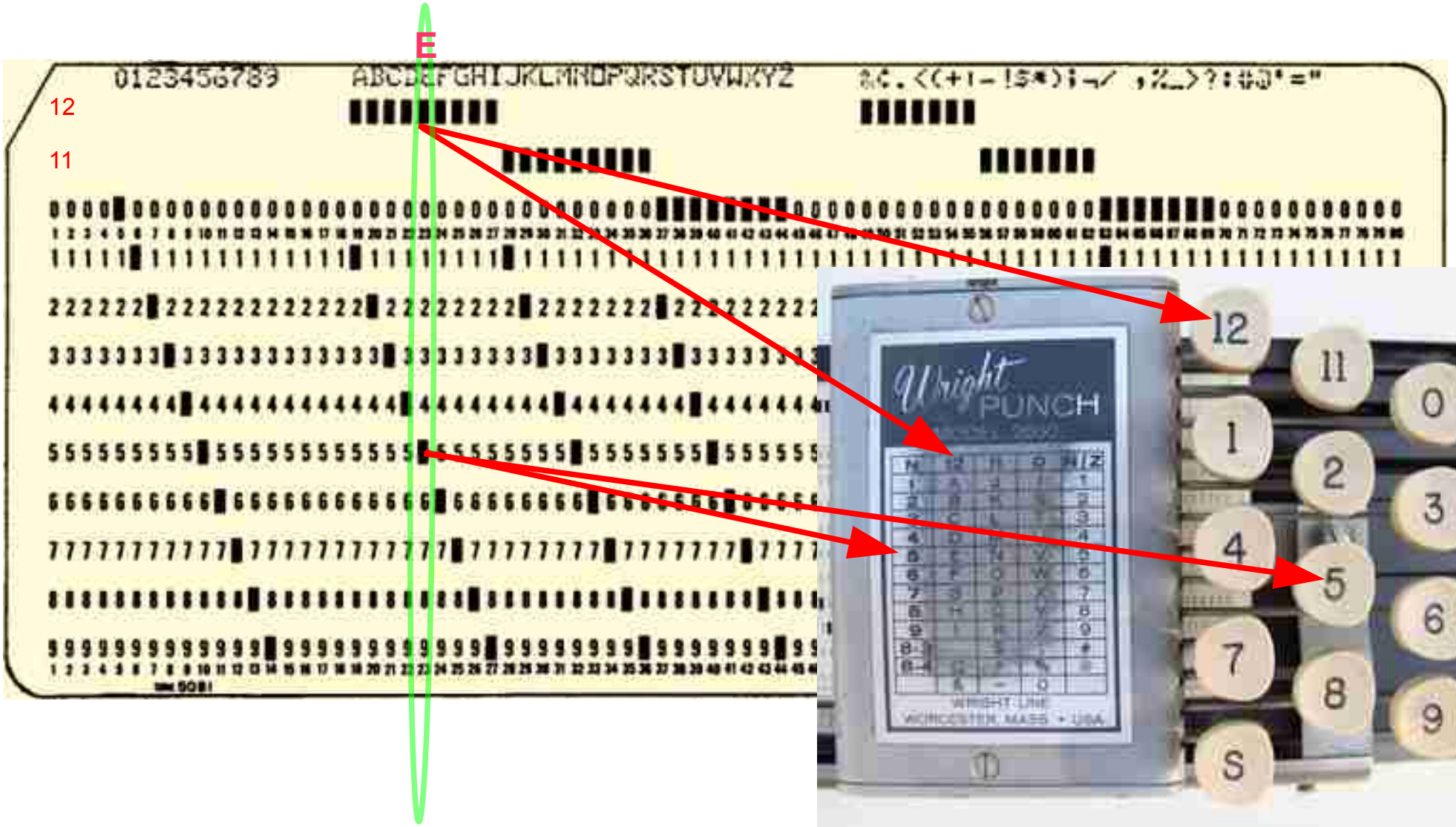
- Baudot
- Murray



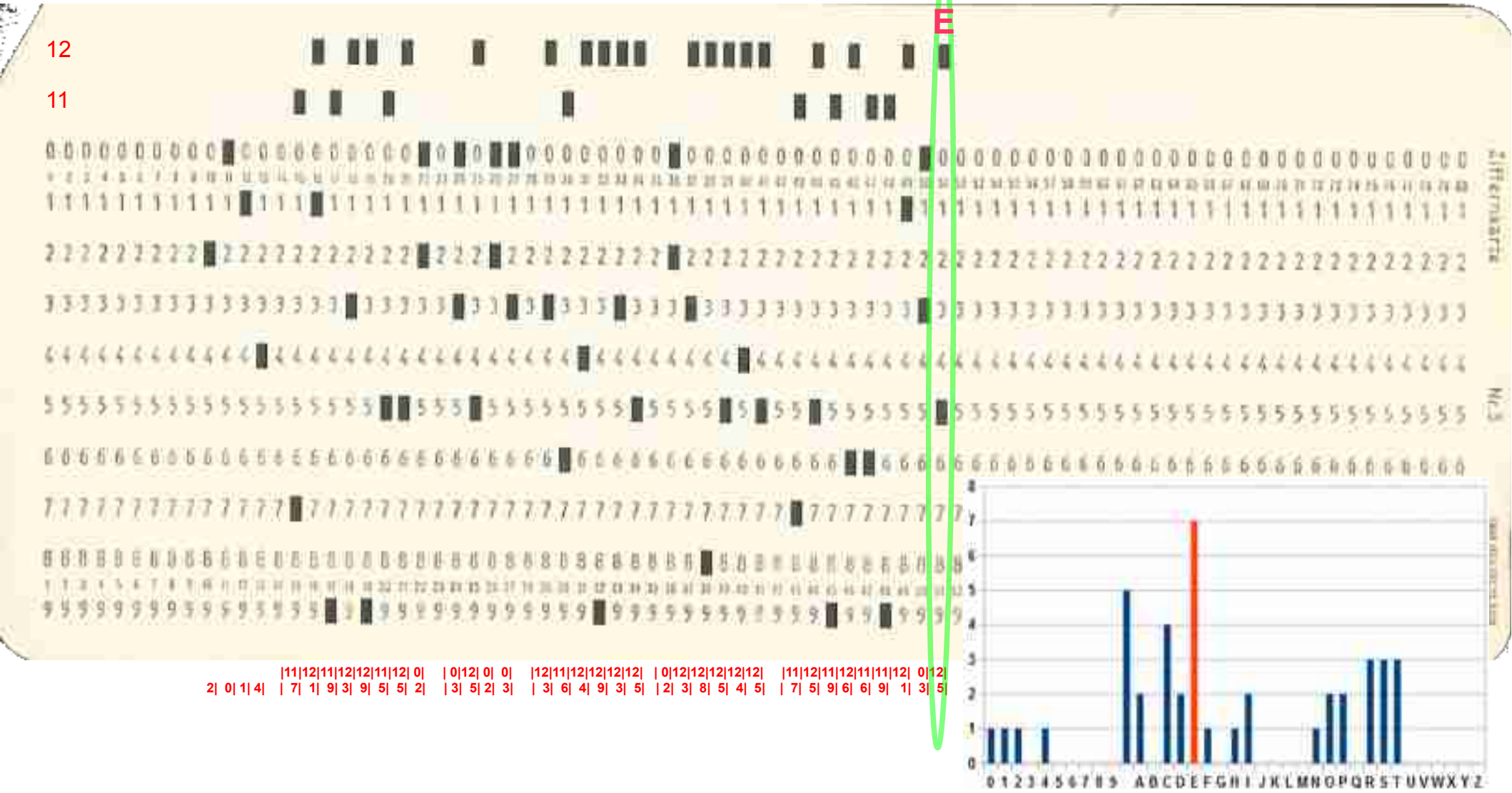


Source: http://en.wikipedia.org/wiki/Baudot_code

Punched Card Code



Quiz: decode the card



From the disk to the rotor

- Alberti

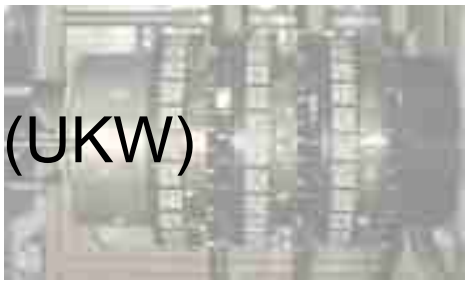
➢ monoalphabetic disk

- Jefferson

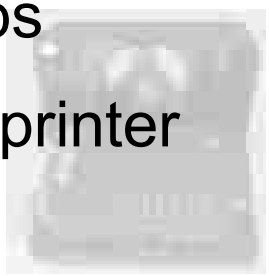
➢ polyalphabetic roll

- Eduard H. **Hebern** (US)
- Hugo A. Koch (NL)
- **Arthur Scherbius (DE)**
- Arvid G. Damm (SE)
- **Boris C.W. Hagelin**
  (SE-US-CH: Crypto AG)

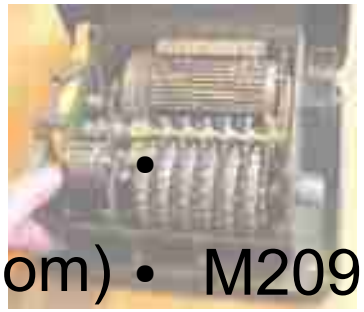
➢ 5 rotors connected by current
➢ rotors - lamps
➢ with reflector (UKW)

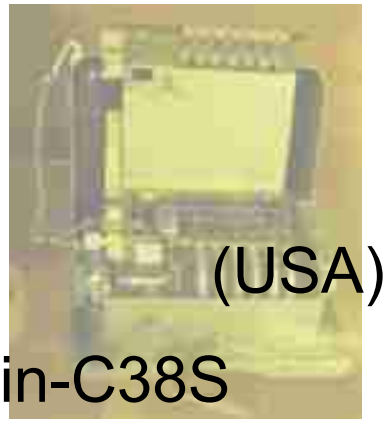


➢ lamps
➢ printer



Cryptographic Machines



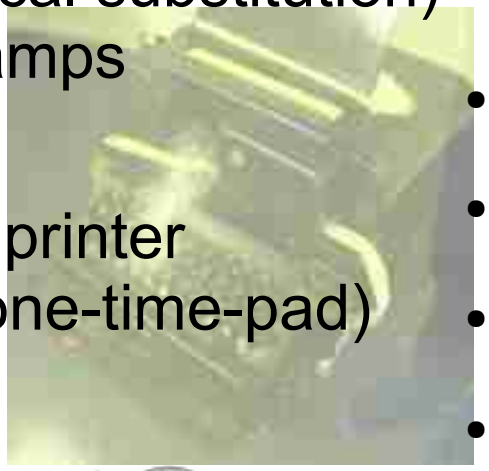


- rotor-setting:
- pin-wheel-key (pseudo-random)

  printed tape
- code-card-key (pseudo-random)
- keyboard:

  (non reciprocal substitution)

  output lamps

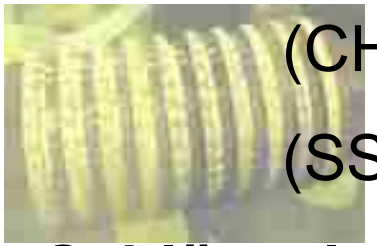


  teletype printer

  (pseudo one-time-pad)

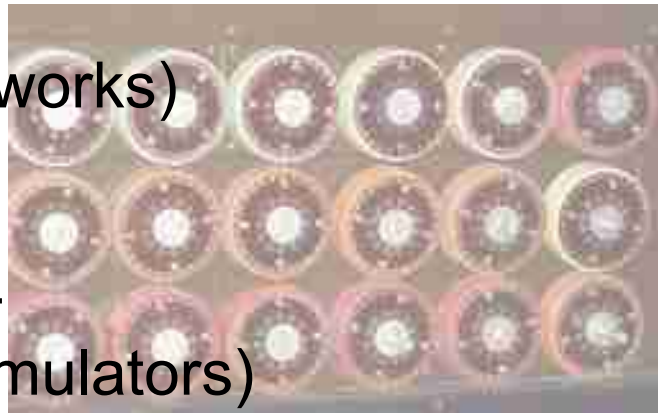
-
- M209 (USA)
- Hagelin-C38S
-

-
- **Enigma** (DE)
- Nema (CH)



- Fialka (SSSR)
- **Lorenz Schlüsselzusatz**
- **Siemens T-52** (DE)

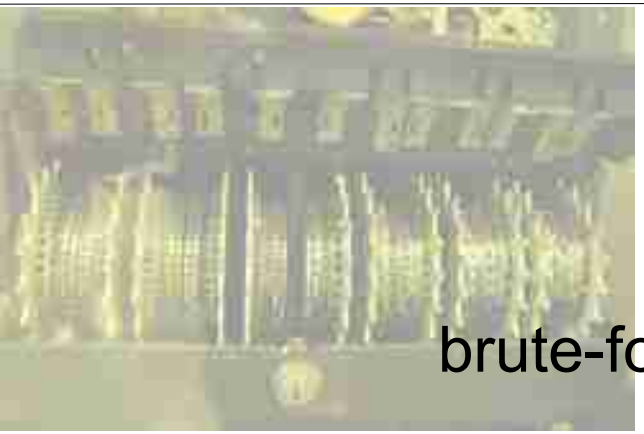
Bletchley-Park Cryptanalysis



- **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