Knowing the secret of secrets

A super fast time travel through the history of encryption

Code, Crypto & Cipher

What’s the difference?

Code

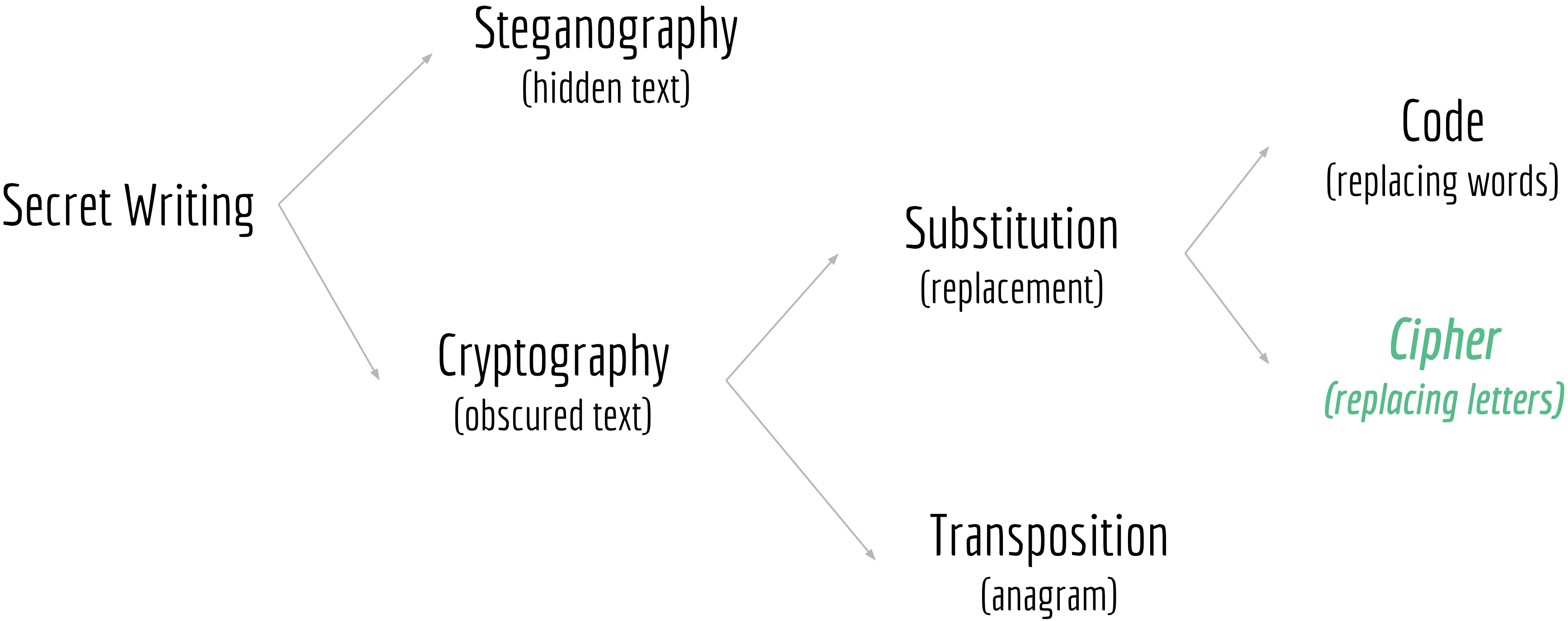
- Replacing entire words and phrases
- “Meet me at the warehouse at 06:00” ➞ “Jupiter”

Cipher (crypto)

- Character level algorithm
- “FROM his shoulder Hiawatha” ➞ “QVPQS OKOIL PUBKJ ZPISF XDW”

Cryptography as a science

Classifications



Secret Writing

Steganography
(hidden text)

Cryptography
(obscured text)

Substitution
(replacement)

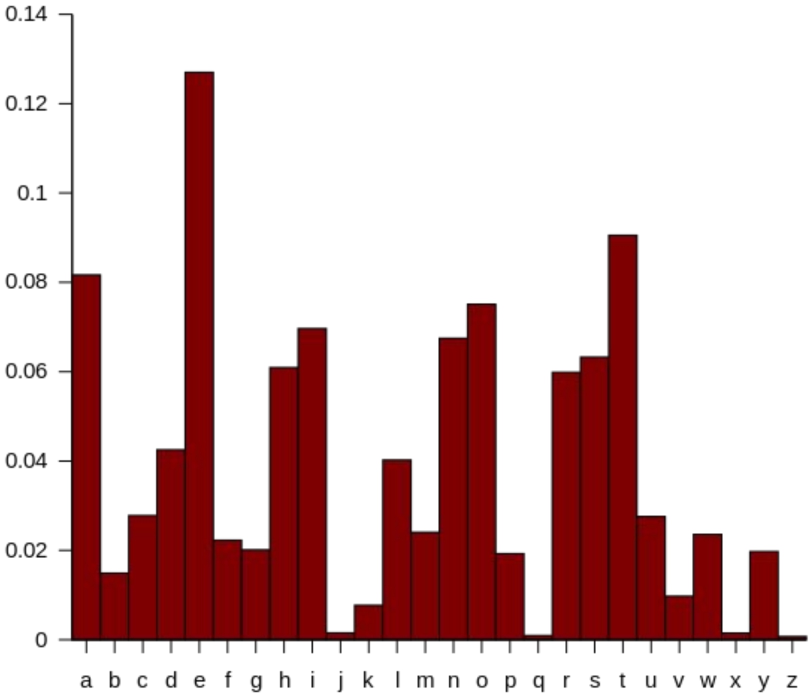
Transposition
(anagram)

Code
(replacing words)

Cipher
(replacing letters)

Short note on Frequency Analysis

- Linguistic features
- Statistical analysis
- Empirical guesswork



Monoalphabetic Substitution Ciphers

Gibberish Level: Beginner

Cesarean Cipher

- Used by Caesar himself

- Single offset alphabet

```
PLAIN:   ABCDEFGHIJKLMNOPQRSTUVWXYZ
CIPHER: TUVWXYZABCDEFGHIJKLMNOPQRS

CLEAR TEXT:      Damn you Brutus
ENCRYPTED TEXT:  WTFG RHN UKNMNL
```

Cesarean Cipher - solution

- Brute force
- Frequency analysis

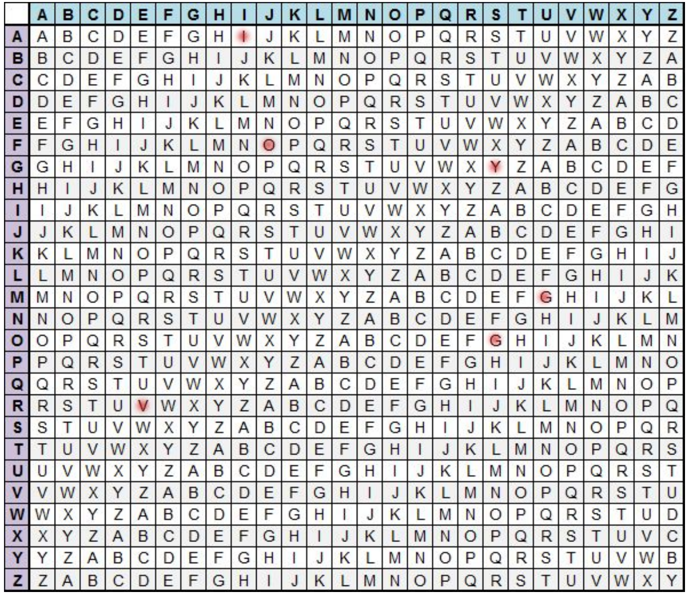
Polyalphabetic Substitution Ciphers

Gibberish Level: Advanced

Vigenère Cipher

- Giovan Battista Bellaso (Blaise de Vigenère)
- “Le chiffre indéchiffrable”
- Multiple offset cipher alphabets

```
TEXT:      Je suis un baguette
KEYWORD:   Fromage
PATTERN:   FR OMAG EF ROMAGEFR
ENCODED:   OV GGIY YS SOSUKXYV
```



	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	D
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	C
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	B
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

Vigenère Cipher - solution

- Guards against frequency analysis

- Recurring coincidental patterns, *Kasiski* test

  Key: **ABCD**ABCDABCDABCDABCDABCDABCD

  Text: **CRYPTO**ISSHORTFOR**CRYPTO**GRAPHY

  Encrypted: **CSASTP**KVSIQUTGQU**CSASTP**IUAQJB

- **CSASTP** repeats at 16 characters ➞ Key length: 16, 8, **4**, 2, 1

- Find key by guessing and analysing

Enigma

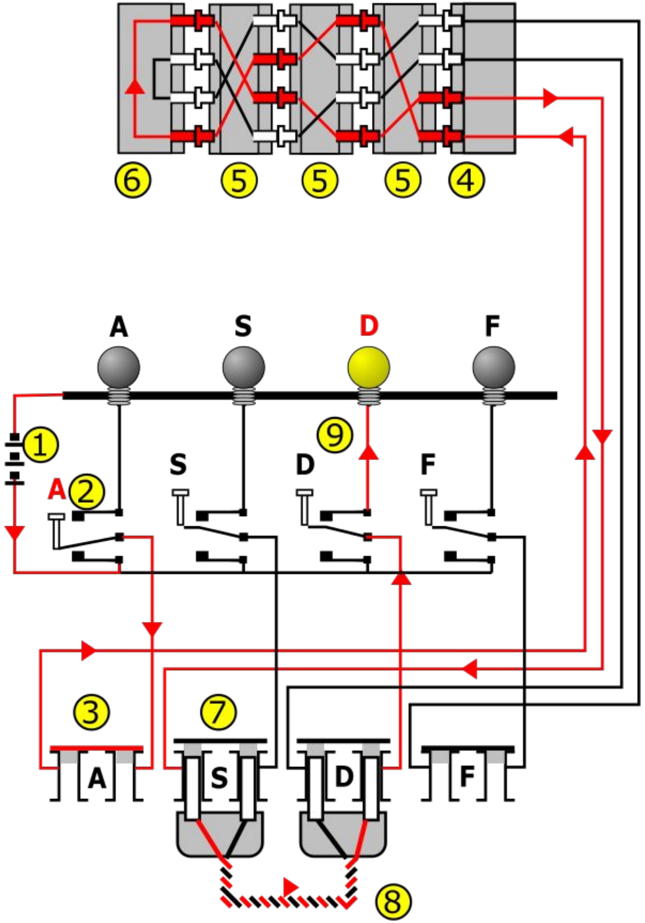
Gibberish level: German

Enigma

- Arthur Scherbius
- Rotating Polyalphabetic Substitution Cipher
- Defeat patterns
- Defeat complexity (“UX”)
- Electro-mechanic automation

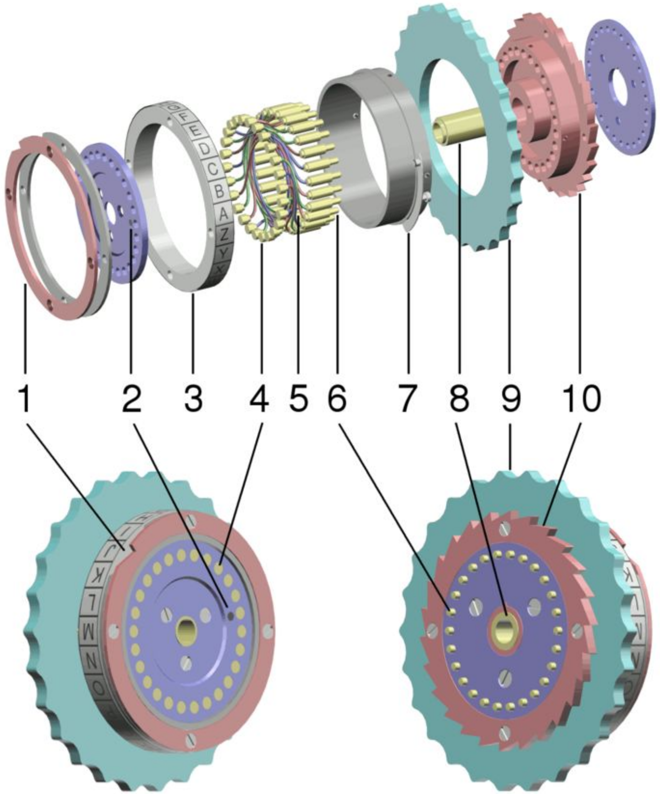
Enigma - wire flow

1. Battery, providing current
2. Letter “A” being pressed on the keyboard
3. Current passing through the plugboard
4. Letter “A” entering the rotor assembly
5. The rotors scrambling the input
6. The reflector returning the current
7. Scrambled letter re-enters the plugboard
8. The signal gets redirected to another wire
9. A light is lit on the display

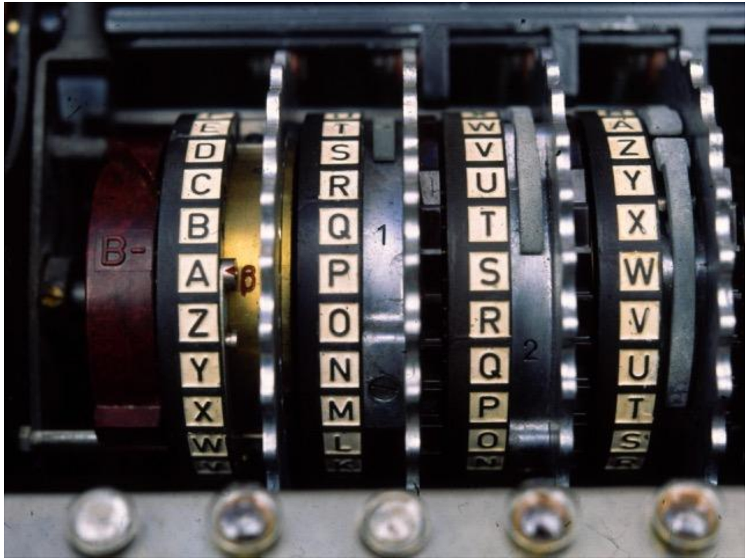


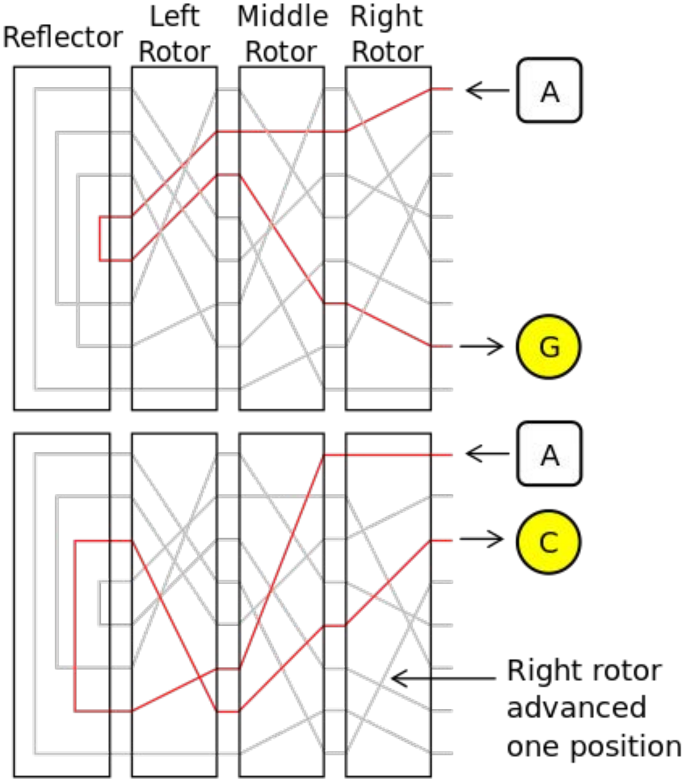
Enigma - the rotor

1. Notched ring (transfer rotation)
2. Reference point for “A”
3. Alphabet ring
4. Connector pads
5. Connectors “scrambling” the alphabet
6. Wire pins
7. Offset configuration lever
8. Rotation axle
9. Offset configuration wheel
10. Rotation ratchet wheel



Enigma - rotor assembly





Enigma - configuration

```
B III IV I AXL (YF) (ZH)
```

- Reflector “B”
- Rotors “III”, “IV” and “I”
- Initial offset of rotors “A”, “X”, “L” respectively (reflector excluded)
- Switch “Y” with “F” and “Z” with “H” on the plugboard

Enigma - what went wrong?

- Virtually no visible patterns
- 3 of 5 rotors + 10 plugs ➝ ***158 962 555 217 826 360 000*** configurations
- Secret intelligence and external hints
- Repetition and association (keywords, weather reports, “personal style”)
- Polish mathematician Marian Rejewski, “bomby”

Asymmetric ciphers

Gibberish level: Outer space

Solving the practical issues

- Key distribution
- Verify origin
- Whitfield Diffie & Martin Hellman formalized an idea
- Ronald Rivest, Adi Shamir & Leonard Adleman provided an implementation

It doesn’t end here...

- Significant computation effort
- RSA exposes plenty of attack vectors of its own
- Political attention and legislation
  (the peculiar case of PGP)