Cryptography

Cryptography

- Study of ways to communicate securely and privately in the presence of third parties
- Charles Babbage, Edgar Allan Poe, Alan Turing, and Claude Shannon were all involved in cryptography.

Message to the Class

TSTEPHAAXLISLAESCEMQIYQ

Scytale

Image Source: Wikipedia

Message to the Class

T S T E P H A A X L I S L A E S C E M Q I Y Q
T H I S I
S A S C Y
T A L E Q
E X A M
P L E Q

Early Ciphers

- Substitution Ciphers
  - *Cryptoquip* - Easily Breakable
- Polyalphabetic Ciphers
  - First described by Al-Kindi in the 9th century
  - Later explained by Leon Battista Alberti in 1467

Tabula Recta

	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

Image Source: Wikipedia

Image Source: [Wikipedia]


TOP
SECRET

Encrypting with Enigma

Enigma Machine

- Encoded messages during WWII
- Used several rotors to create a key for encryption
- Board for inputs

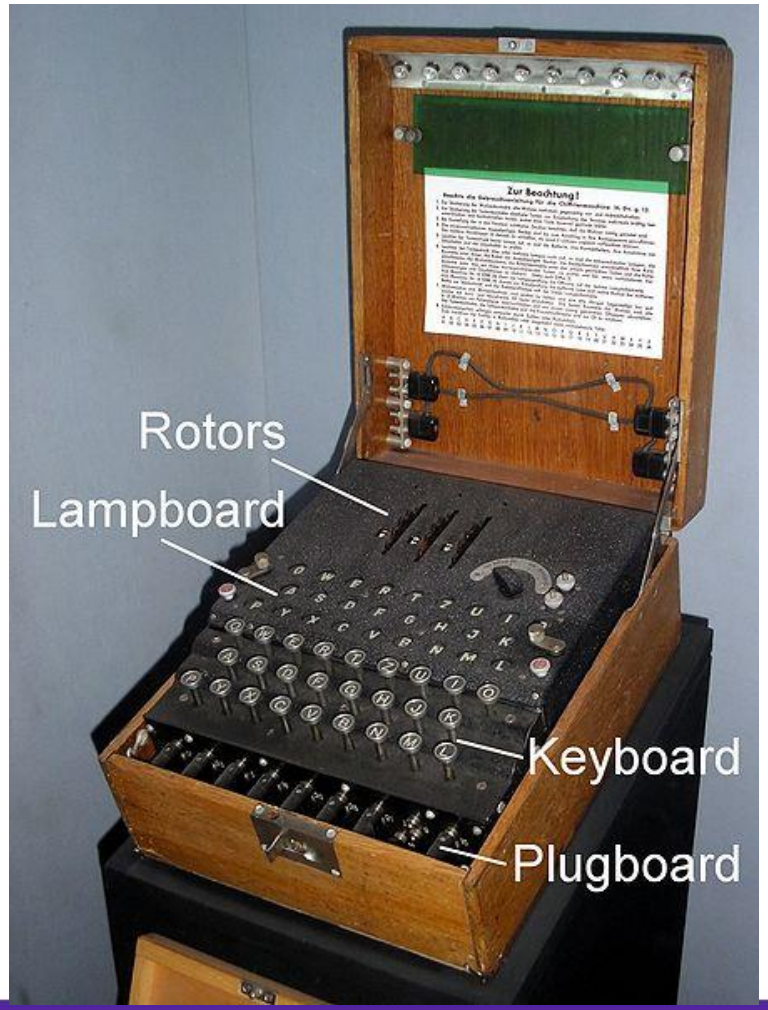


Image Source: Wikipedia

Enigma Machine Rotors

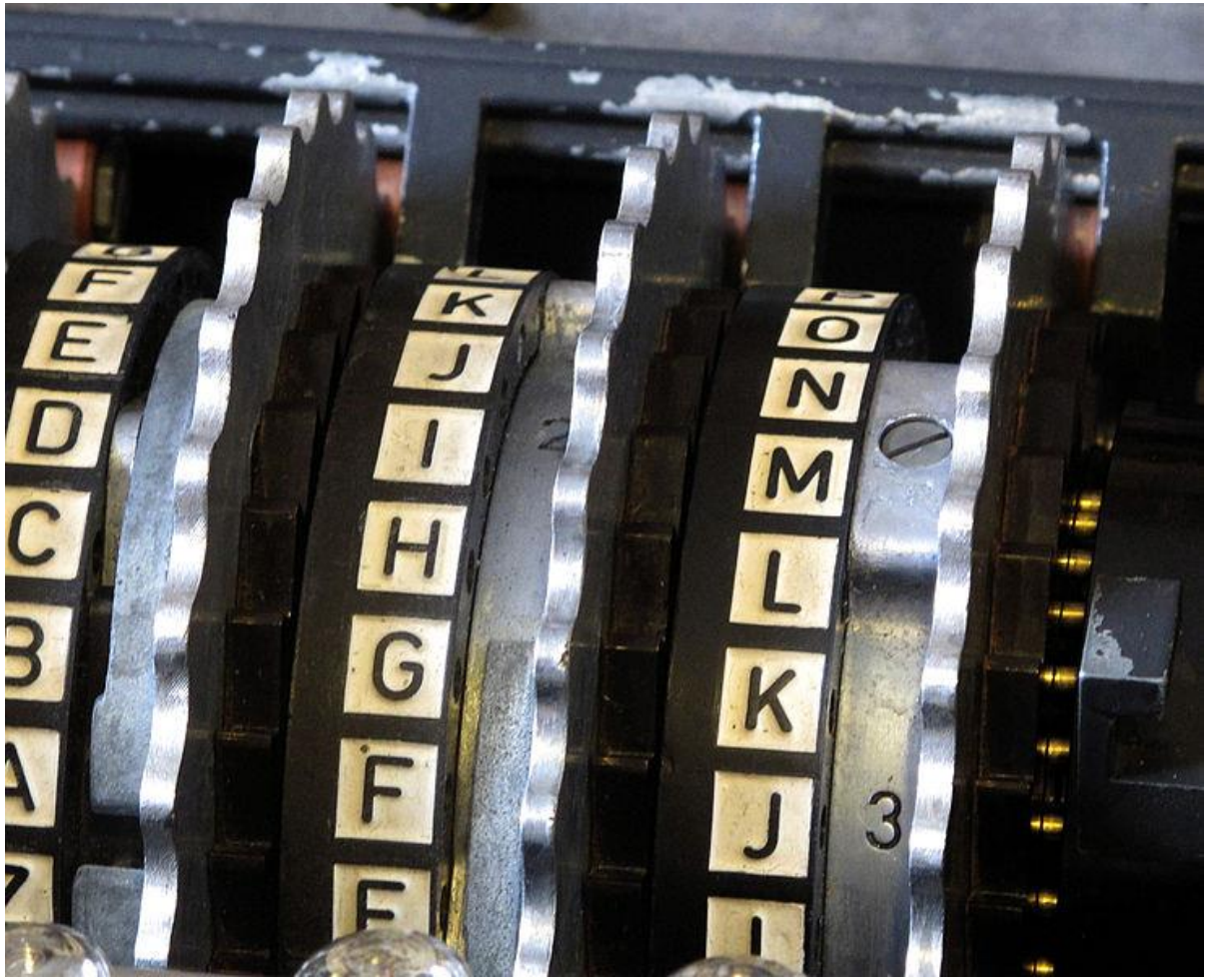


Image Source: Wikipedia

Enigma Machine Rotors

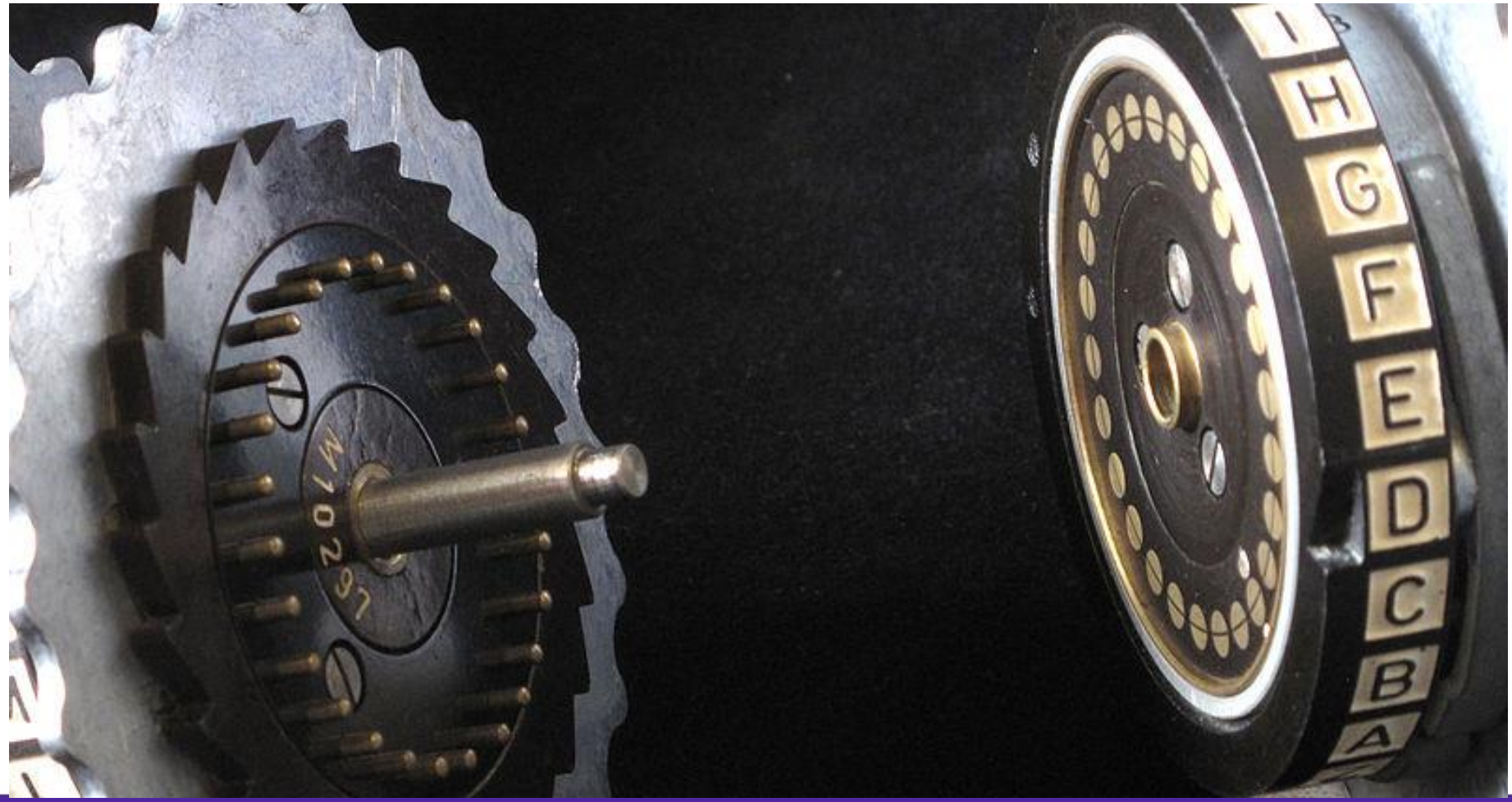


Image Source: Wikipedia

Enigma Machine Ratchet

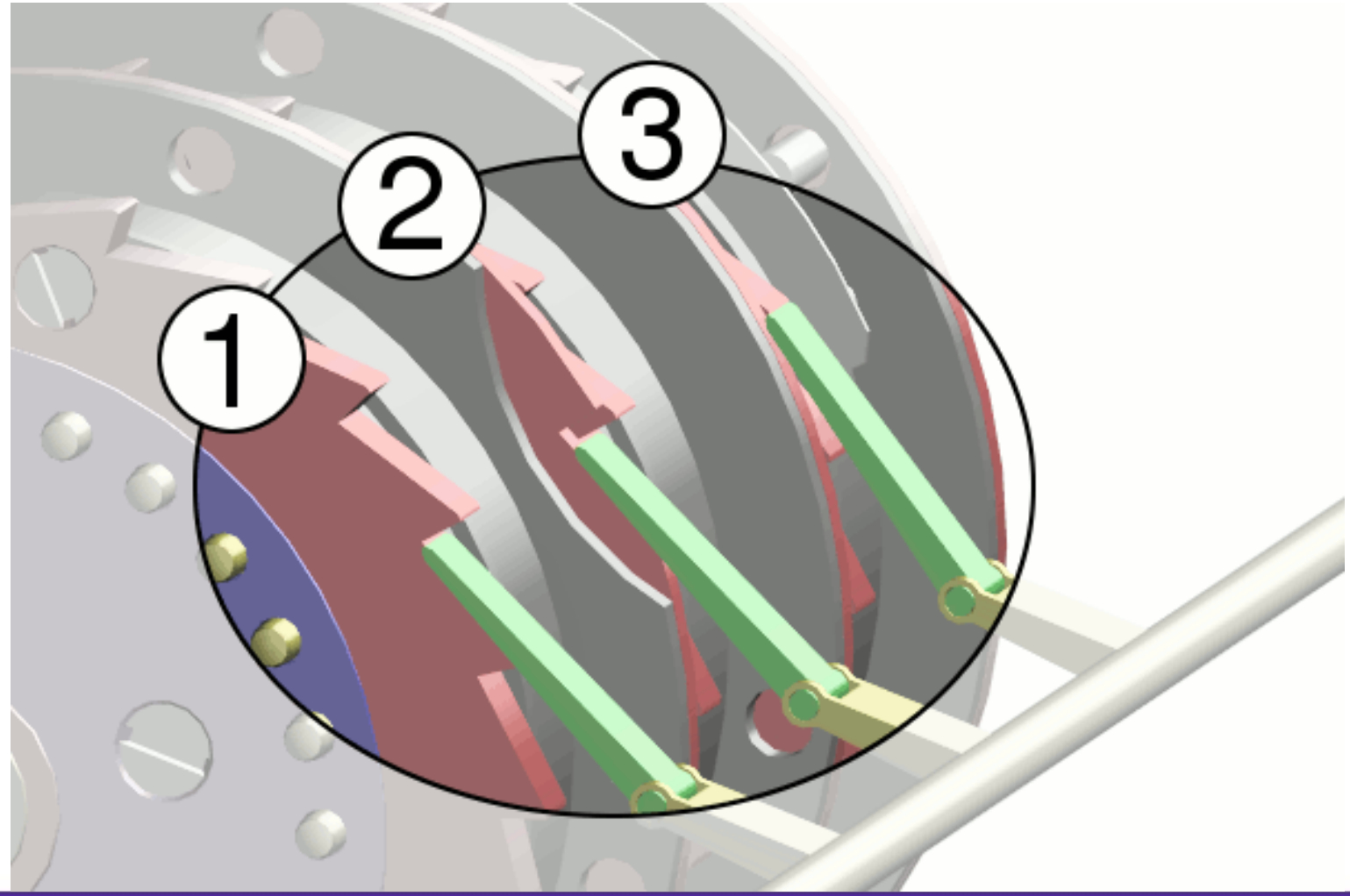


Image Source: Wikipedia

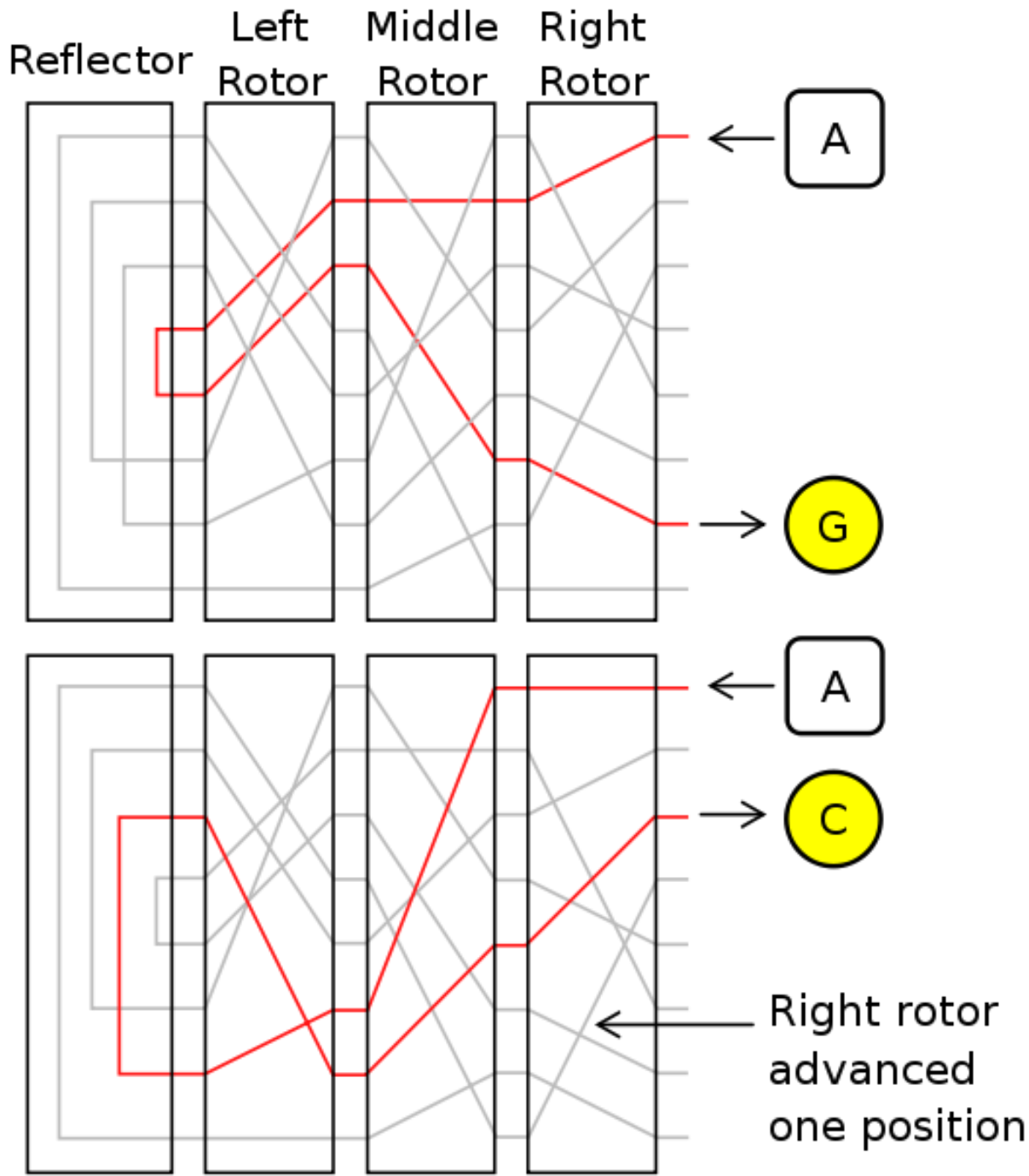


Image Source: Wikipedia

Enigma Machine Plugboard

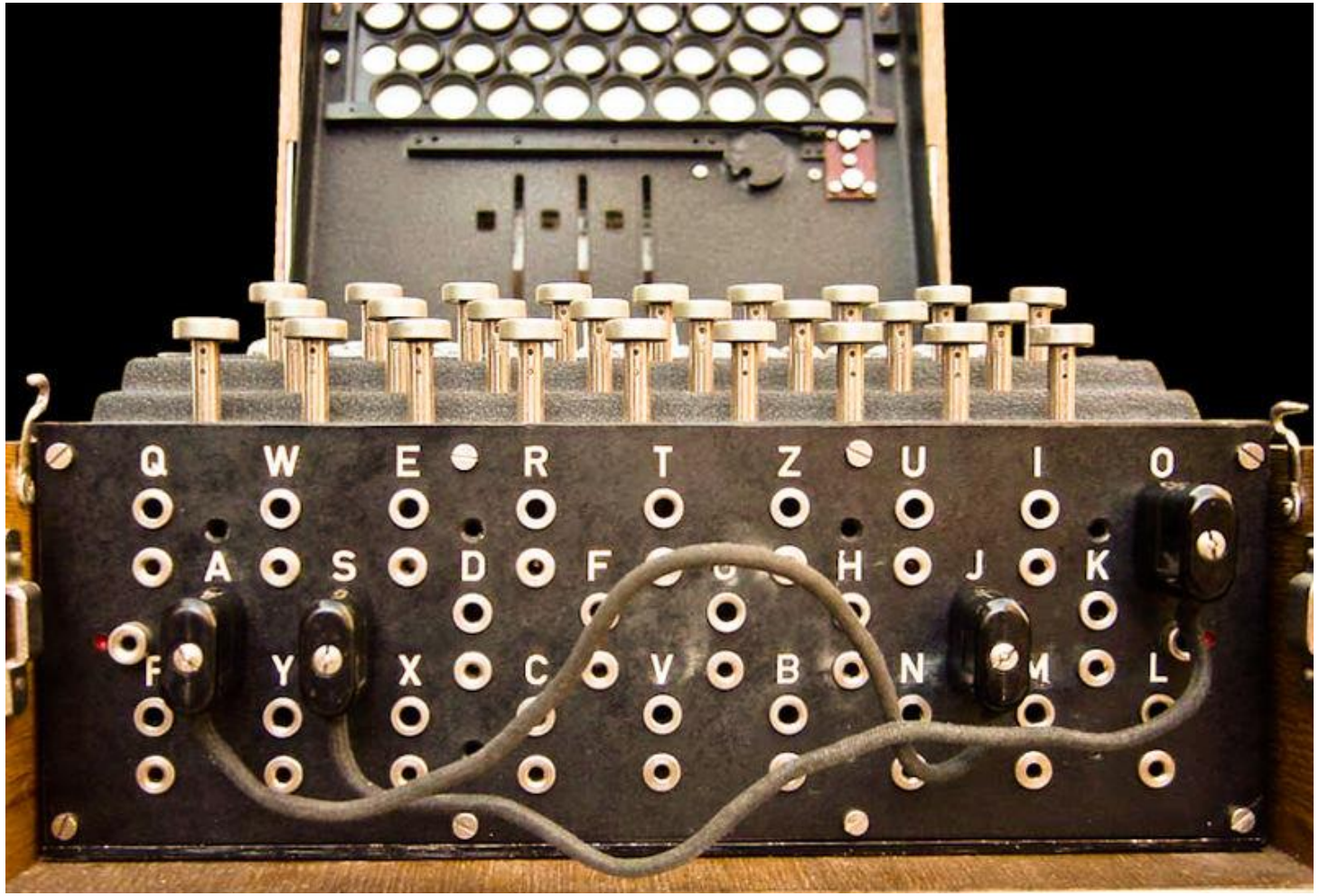


Image Source: Wikipedia

Enigma Key

- Choice and order of rotors
- Initial position of rotors
- Ring setting on rotors
- Plug connections

Enigma Operation

- Set wheels to today's key from codebook
- Operator chooses message key
- Encode message key TWICE to avoid errors
- Set wheels to message key
- Encrypt and send message

Enigma Strengths

- Many factors to the encryption
- Had up to 8 different wheels to choose from by the end of the war
- 150 Trillion different setups from just the plugboard!
- All together, over 158 quintillion

Enigma Weaknesses

- A letter would never encrypt to itself
- Plugboards were reciprocal
- Wheels were not similar enough (could determine which wheels were used)
- Poor policies and procedures

Decrypting with Enigma

Marian Rejewski

- Polish mathematician who worked on the Enigma machine
- 1920s-1930s, Poland was under threat from Germany
- Eventually replicated the German machines

Image Source: Wikipedia

Cracking Enigma

- 1932 - First cracked by Marian Rejewski of Poland
- 1938 - Germany added 2 wheels
- 1939 - Alan Turing creates Bombe
- 1945 - Almost every message deciphered within 2 days

Bombe

- Developed by Alan Turing to simulate enigma machines
- Exploited many of the weaknesses and other facts

Image Source: Wikipedia

Bombe

Impact

"My own conclusion is that it shortened the war by not less than two years and probably by four years … we wouldn't in fact have been able to do the Normandy Landings, even if we had left the Mediterranean aside, until at the earliest 1946, probably a bit later."

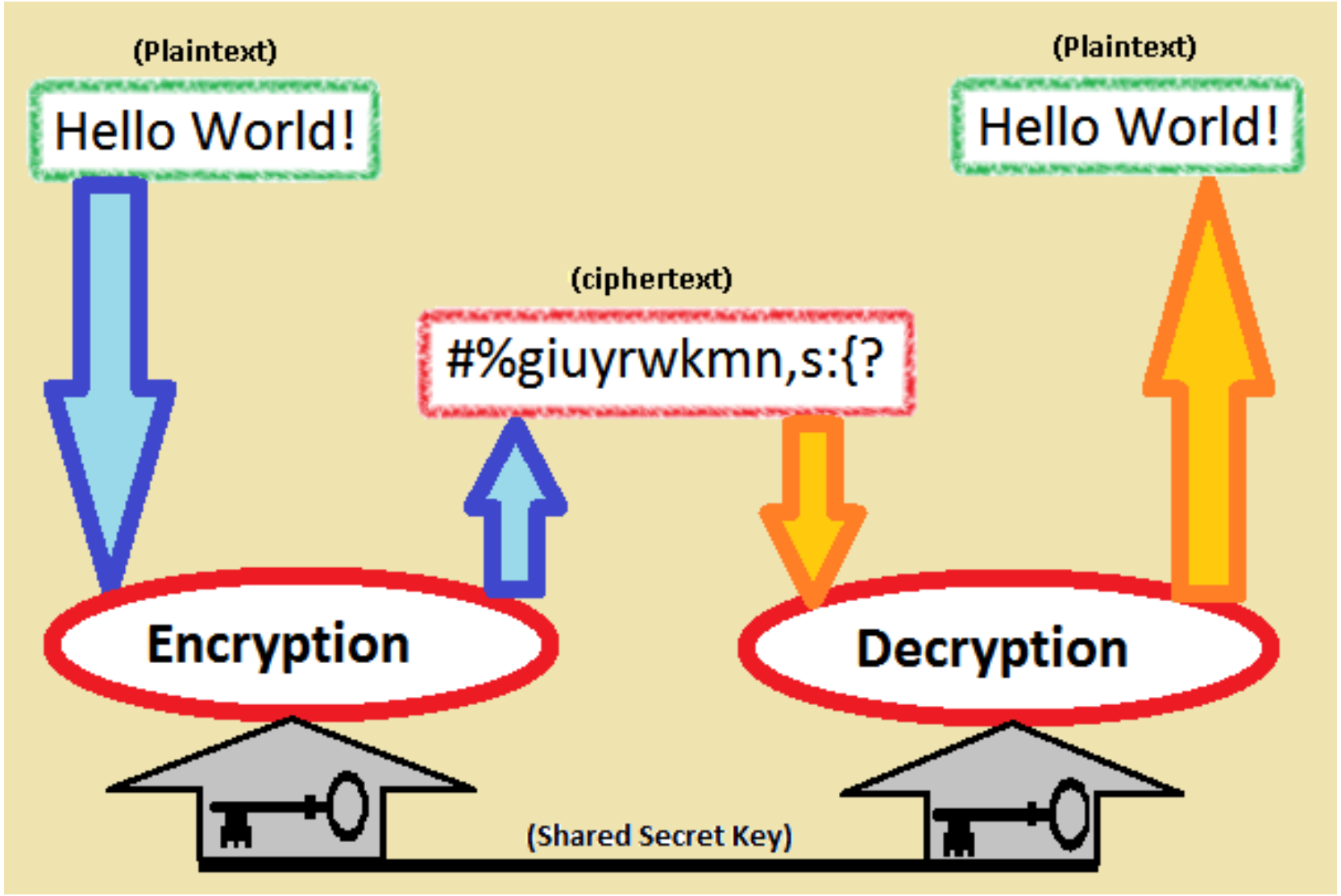
-Sir Harry Hinsley
British Intelligence Historian

Claude Shannon

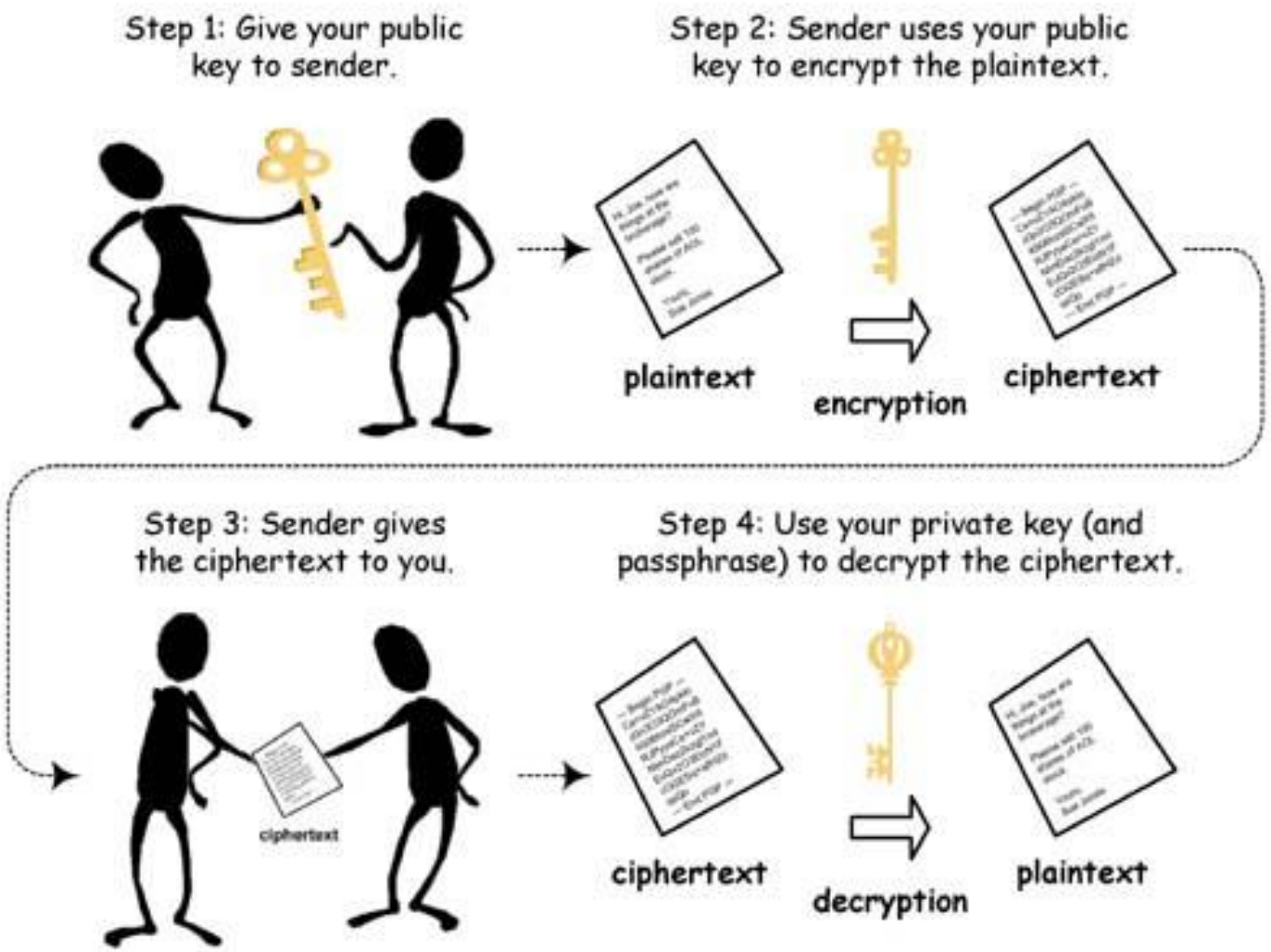
The Father of Information Theory

Image Source: Wikipedia

Symmetric Key Encryption



Public Key Encryption



Source: Askamathematician.com

Key Encryption

RSA Encryption

- Developed in 1977
- Named for the 3 creators (Ron Rivest, Adi Shamir, Leonard Adleman)
- Uses the product of 2 large prime numbers to generate a key
- Key strength depends on the difficulty of factoring large numbers

RSA Example

- Choose 2 distinct prime numbers p and q
- Compute their product $n = pq$
- Compute the totient t of n: $t = (p - 1)(q - 1)$

RSA Example

- Choose any number *e* less than *t* that is **coprime** to *t* (they share no common factors but 1)
- Calculate *d* as the **modular multiplicative inverse** of *e* (mod *t*)
  $e * x = 1 \pmod{t}$

RSA Keys

- Public Key : (n, e)
- Encode: $c = m^e \pmod{n}$

- Private Key : (n, d)
- Decode: $m = c^d \pmod{n}$