How Computers Changed Cryptography

(And Vice Versa)

Erik L. Arneson

What is Cryptology?

cryp•tog•ra•phy (krɪpˈtɒg rə fi)

(n.) the study or the application of the techniques of secret writing, especially code and cipher systems.

crypt·a·nal·y·sis (krĭpˈtə-năl'ĭ-sĭs)

(n.) the analysis and deciphering of cryptographic writings or systems.

Early Cryptography: Substitution Ciphers

A	B	C	D	E	F	G	H	I	J	K	L	M
D	E	F	G	H	I	J	K	L	M	N	O	P

N	O	P	Q	R	S	T	U	V	W	X	Y	Z
Q	R	S	T	U	V	W	X	Y	Z	A	B	C

HELLO MOTHER → KHOOR PRWKHU

Early Cryptanalysis

Al-Kindi, father of Arabic philosophy (9th century CE)

19th Century: Cracking the Vigenère Cipher

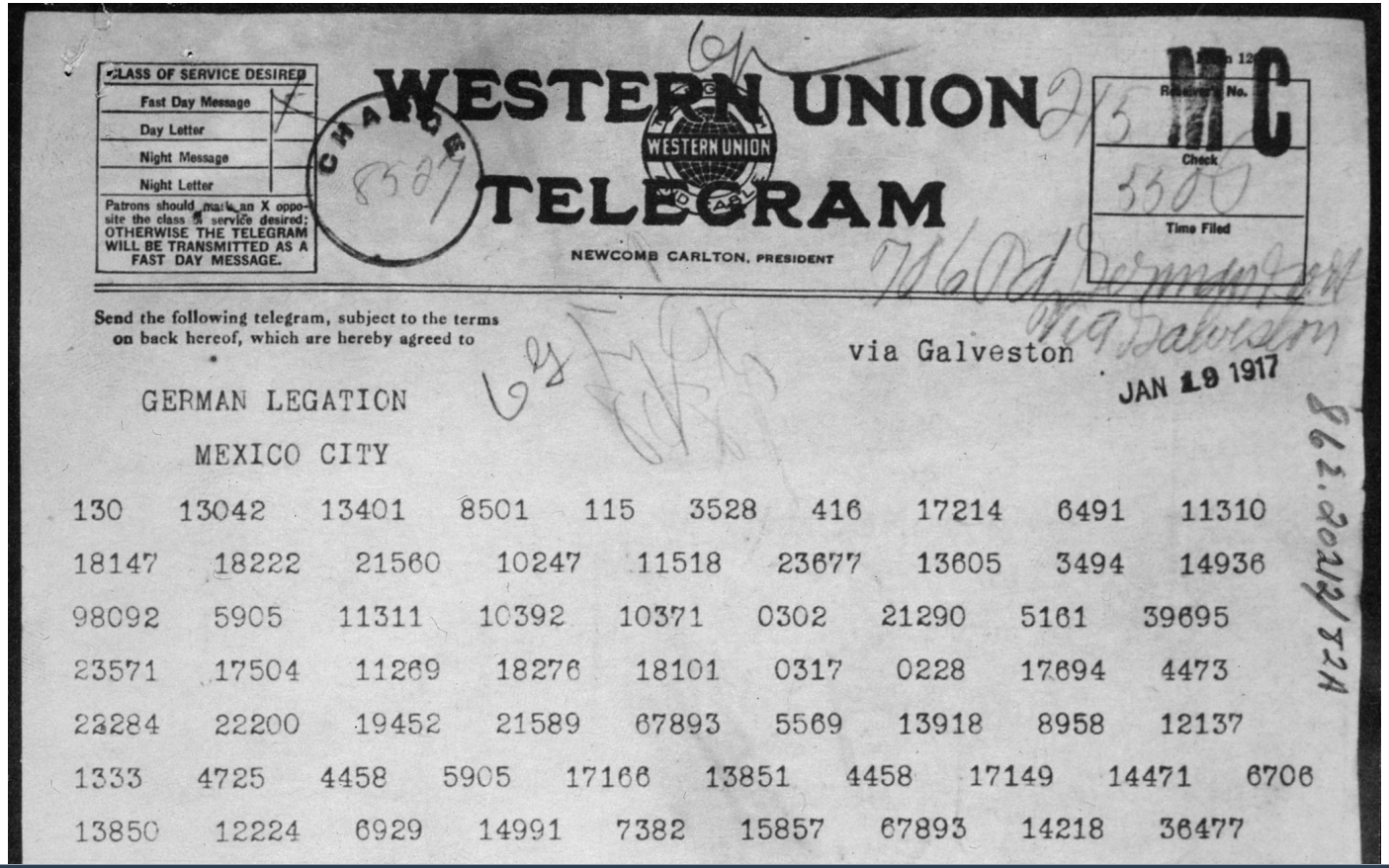
Codes and Codebreaking in World War I

One-Time Pad

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

Playfair Cipher

The Zimmerman Telegram



CLASS OF SERVICE DESIRED
Fast Day Message
Day Letter
Night Message
Night Letter
Patrons should mark an X opposite the class of service desired; OTHERWISE THE TELEGRAM WILL BE TRANSMITTED AS A FAST DAY MESSAGE.

WESTERN UNION TELEGRAM

NEWCOMB CARLTON, PRESIDENT

Receiver's No.
Check
Time Filed

Send the following telegram, subject to the terms on back hereof, which are hereby agreed to

via Galveston

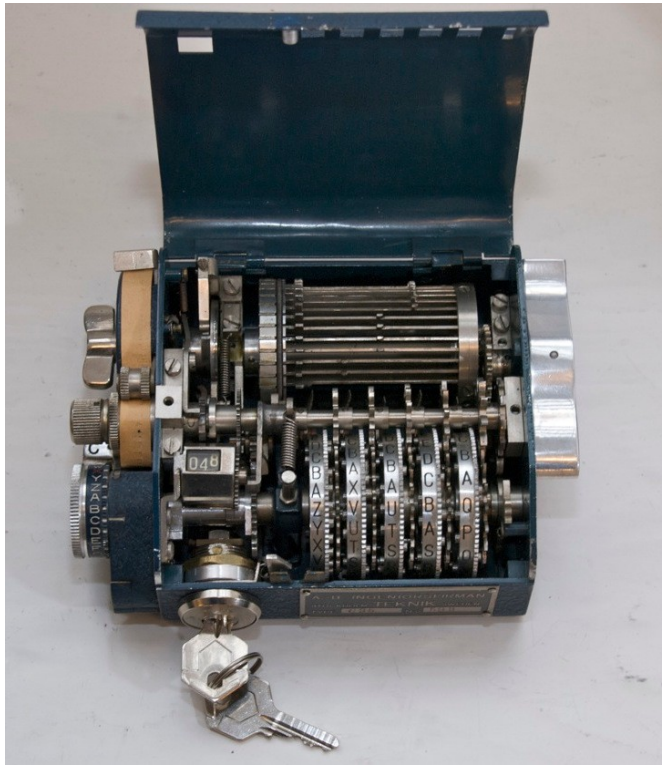
JAN 19 1917

GERMAN LEGATION

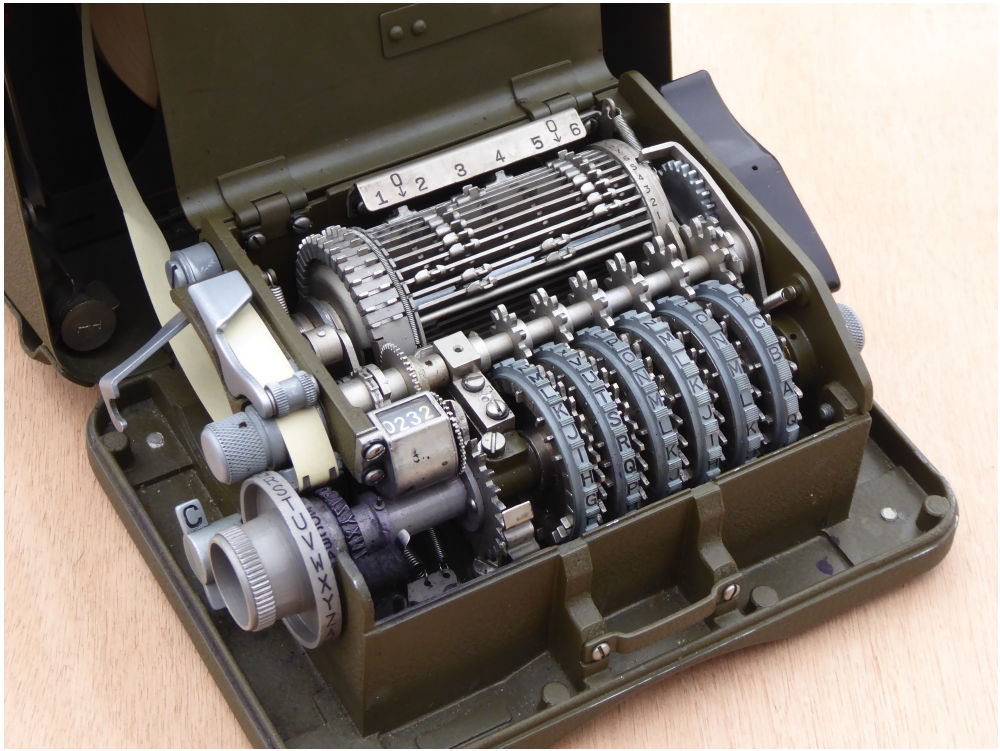
MEXICO CITY

130 13042 13401 8501 115 3528 416 17214 6491 11310
18147 18222 21560 10247 11518 23677 13605 3494 14936
98092 5905 11311 10392 10371 0302 21290 5161 39695
23571 17504 11269 18276 18101 0317 0228 17694 4473
22284 22200 19452 21589 67893 5569 13918 8958 12137
1333 4725 4458 5905 17166 13851 4458 17149 14471 6706
13850 12224 6929 14991 7382 15857 67893 14218 36477

Early Mechanical Ciphers

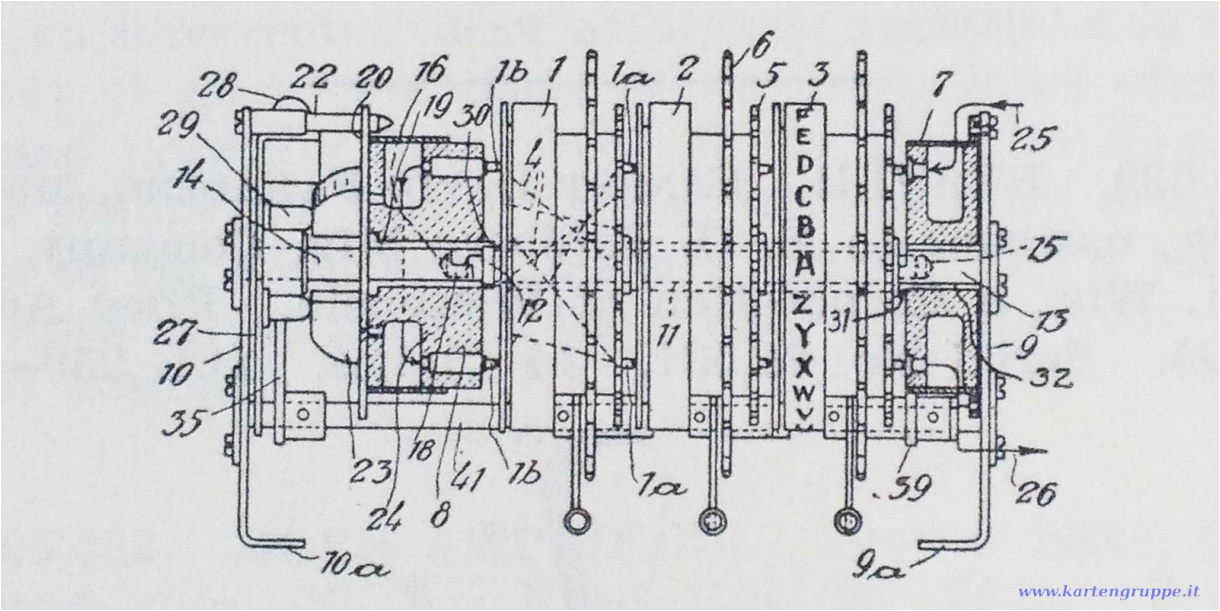


C-35 Cipher Machine



M-209 Cipher Machine

1918: Enter the Enigma



Enigma patent drawing

The Difficulty of the Enigma

Each of 3 scramblers in one of 26 positions (26 × 26 × 26)	17,576
Scrambler arrangement order (3 × 2 × 1)	6
Plugboard swapping with 3 cables	100,391,791,5000
Total no. of keys	**10,586,916,764,424,000**

Biuro Szyfrów Cracks the Enigma

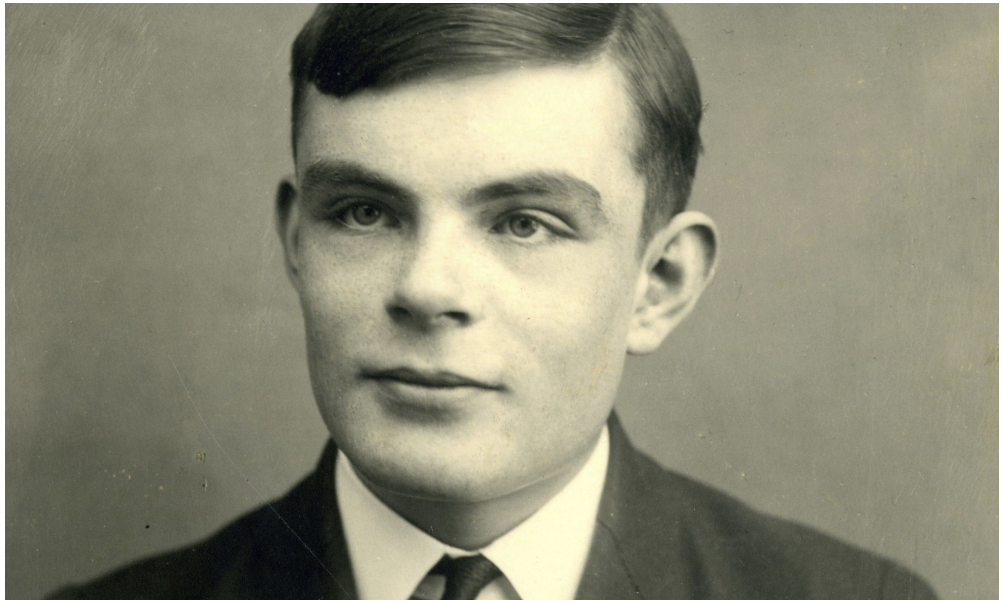
Rejewski, Różycki and Zygalski

Polish Biuro Szyfrów

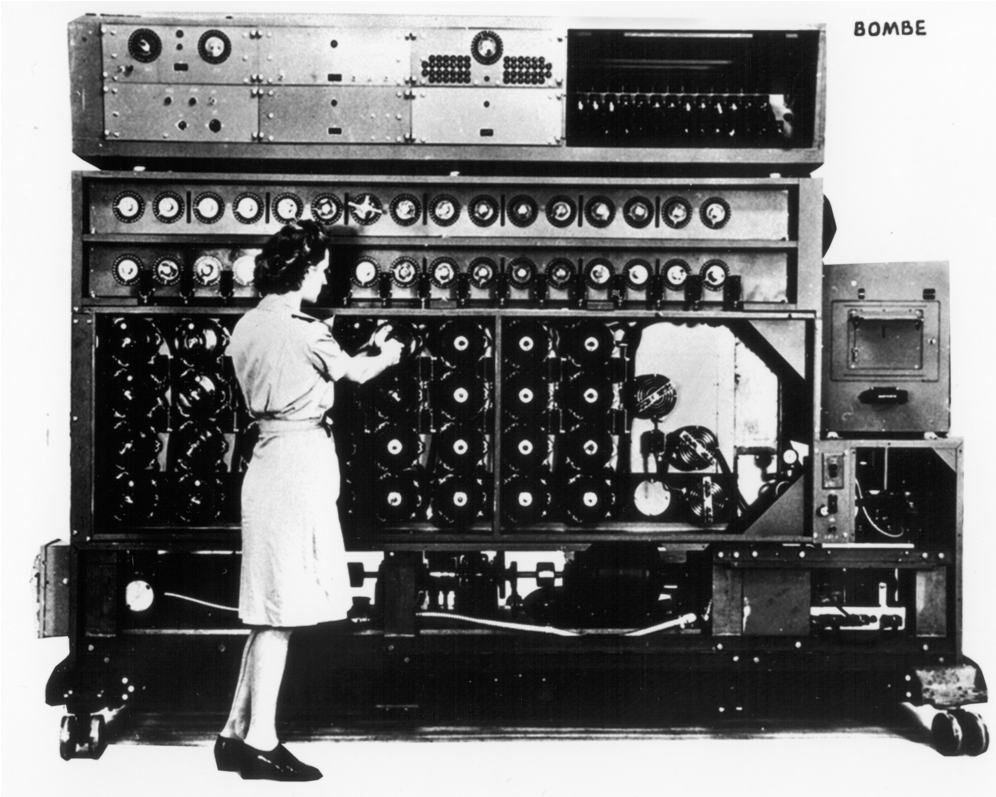
1939: Enigma's New Invulnerability

Bletchley Park (Government Code & Cipher School)

Building the Bombe

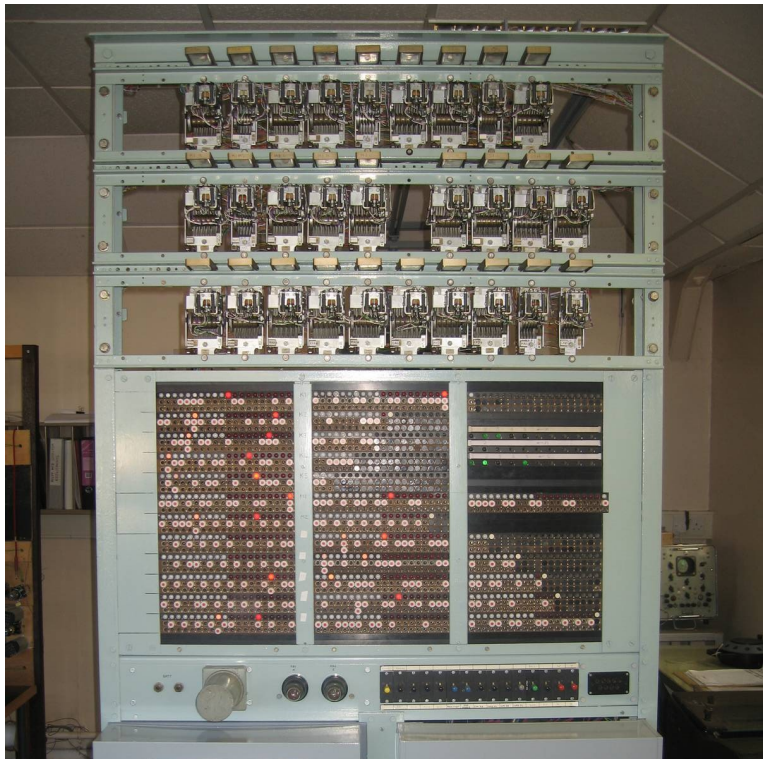


Alan Turing (1912–1954)



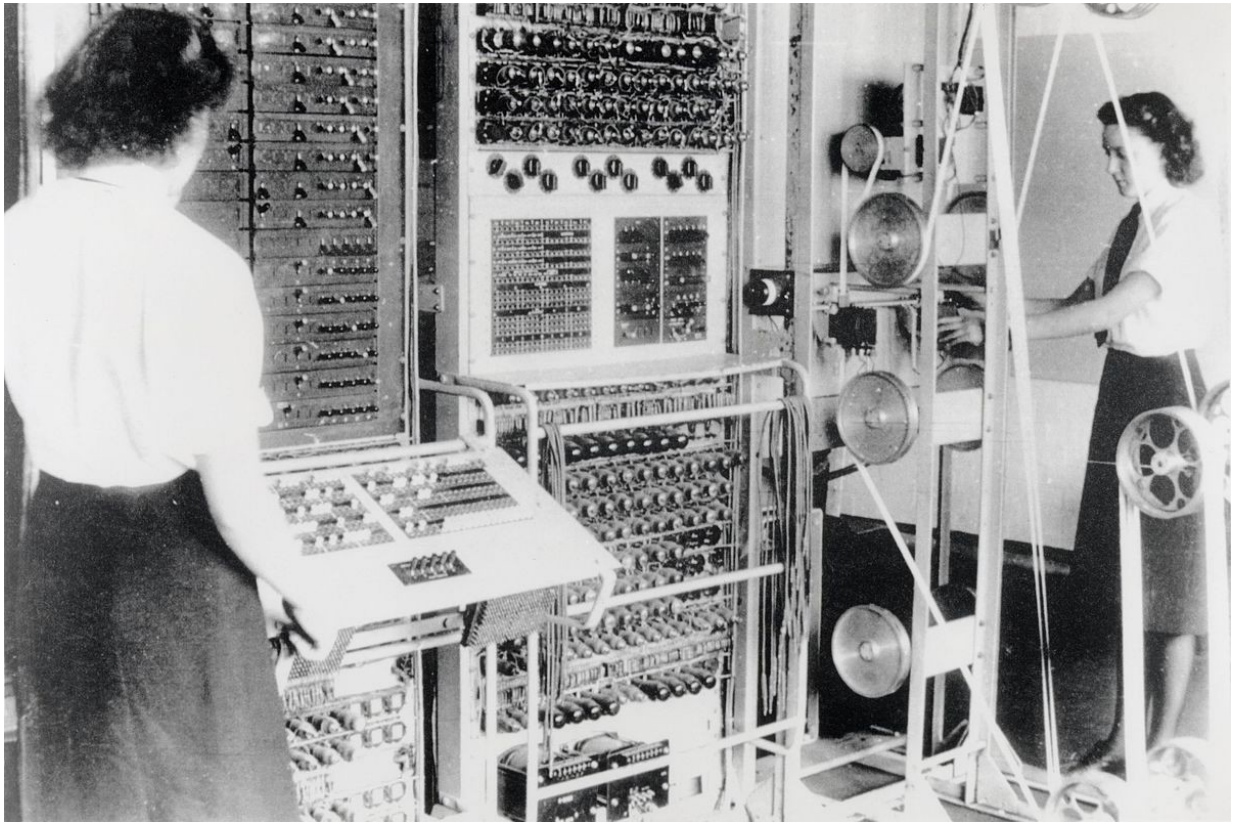
The Lorenz vs. the Tunny

Lorenz Cipher Machine



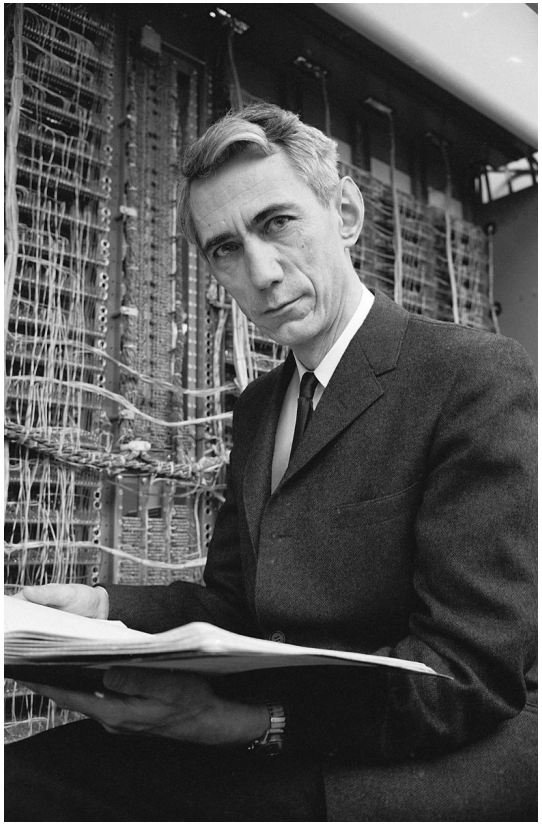
Bletchley Park “Tunny”

Colossus: First Electronic Digital Programmable Computer



Tommy Flowers
(1905–1998)

Measuring the Security of a Cipher

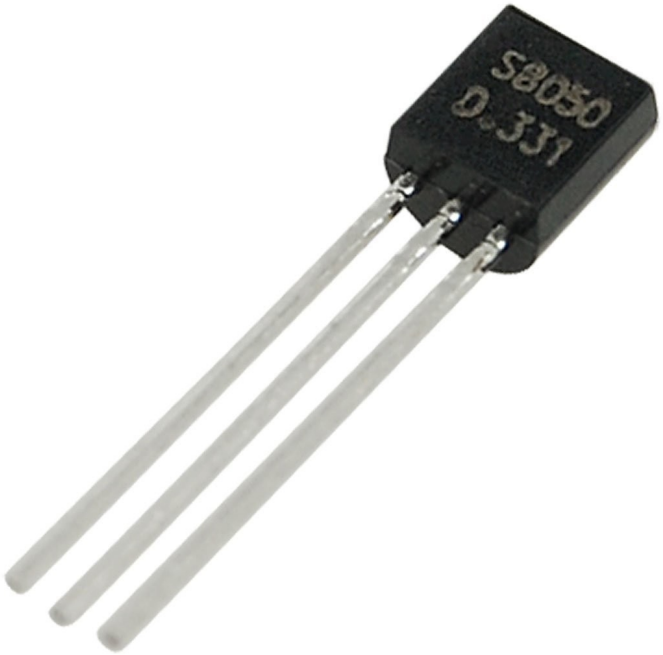


Claude Shannon

“Communication Theory of Secret Systems,” 1949

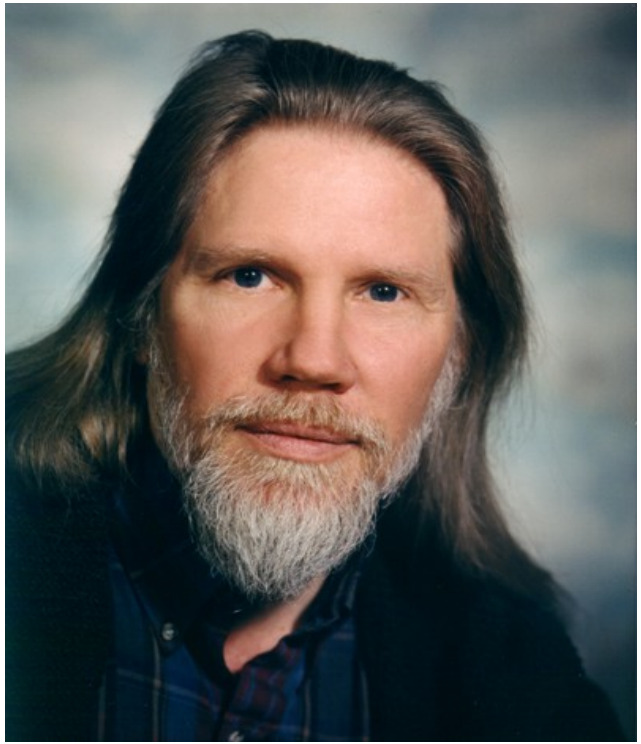
From Vacuum Tubes to Transistors

Vacuum Tube



Transistor
(definitely not to scale)

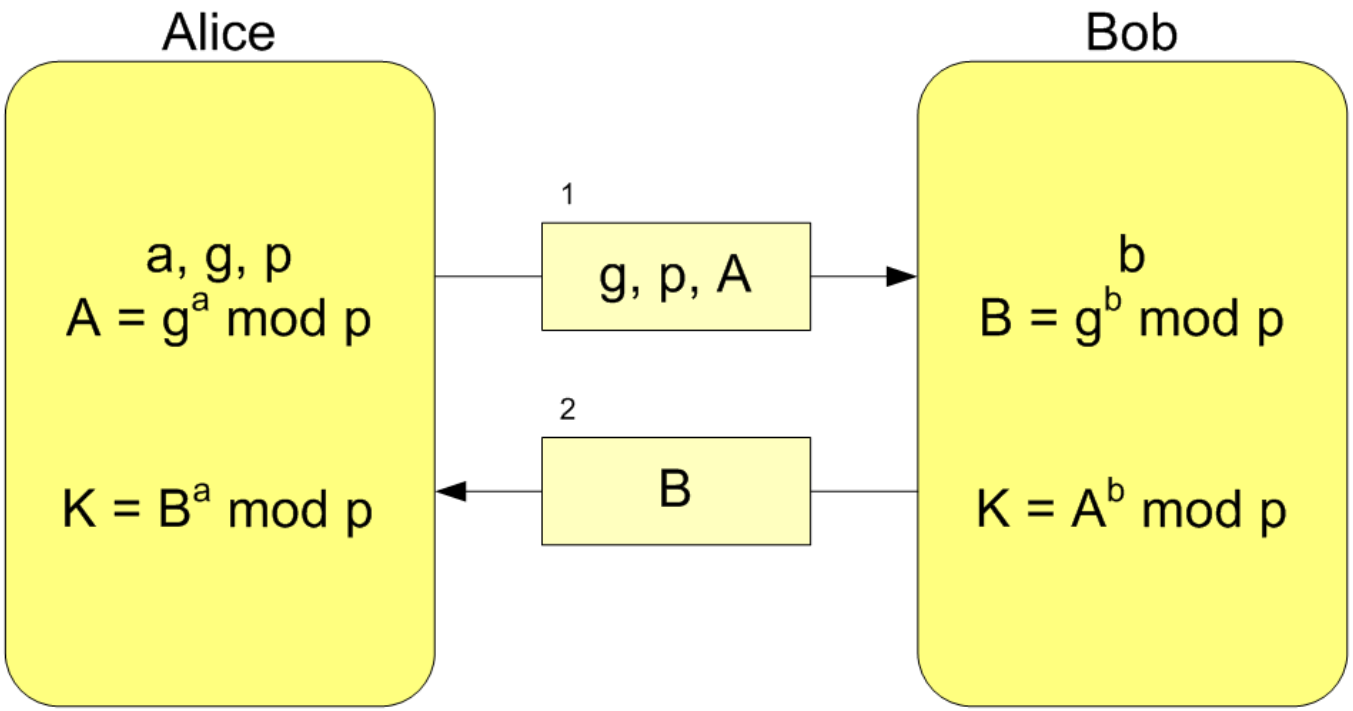
A New Direction in Cryptography: Diffie-Hellman



Whitfield Diffie

Martin Hellman

Diffie-Hellman Key Exchange



$$K = A^b \bmod p = (g^a \bmod p)^b \bmod p = g^{ab} \bmod p = (g^b \bmod p)^a \bmod p = B^a \bmod p$$

Encryption and the Surveillance State

National Security Agency compound in Fort Meade, MD

- Largest employer of mathematicians in the world
- Largest buyer of computer equipment in the world
- Largest consumer of electricity in Maryland
- **Uses more electricity than Anapolis!**

Modern Cryptography in Your Pocket

How many Enigma machines are in your pocket?

Questions and Answers

Thank You!

@pymander

earneson@arnesonium.com

https://arnesonium.com/