601.445/601.645
Practical Cryptographic Systems

Symmetric Cryptography

Instructor: Matthew Green

Housekeeping

- Website updated
  - Slides up as we go (https://github.com/matthewdgreen/practicalcrypto)
  - Reading assignment today (for Mon)
    Anderson chap 5.7
  - Assignment 1 out this afternoon

News?

Security/crypto news

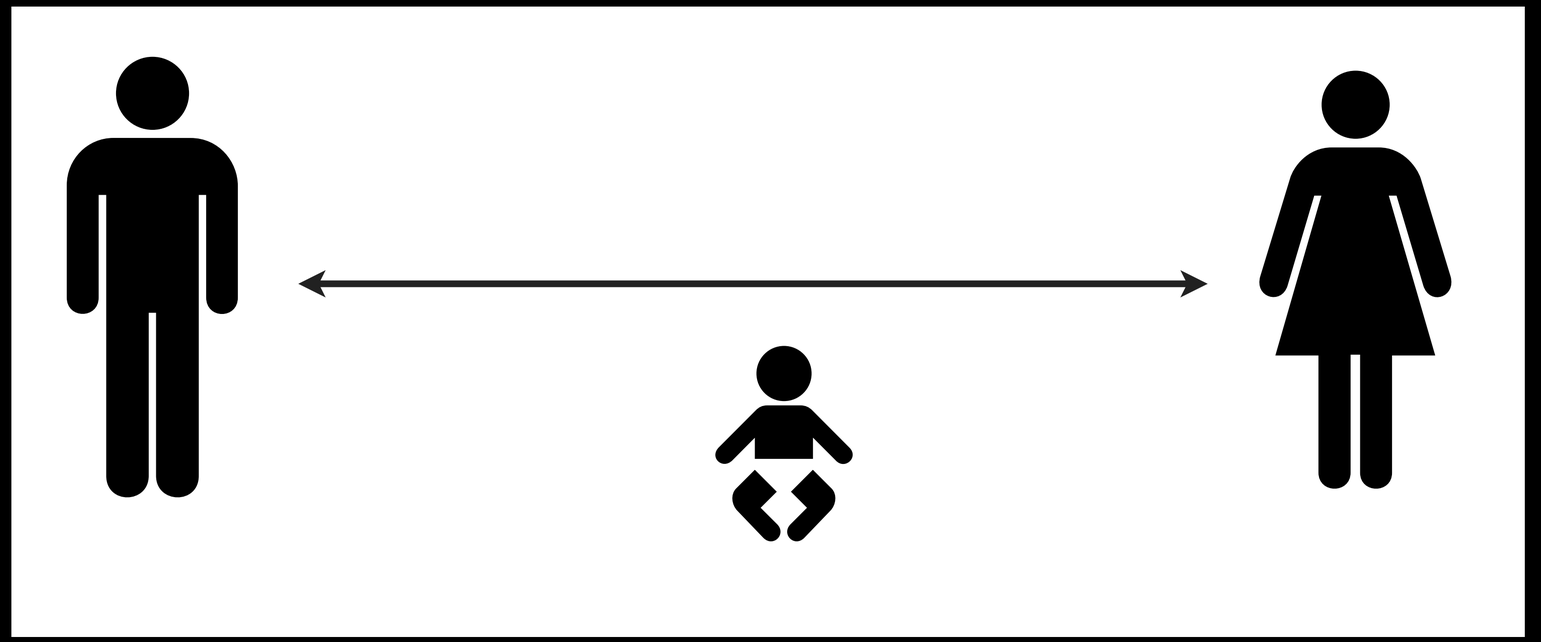
- Hacker news: news.ycombinator.com
- Ars Technica
- Twitter (e.g., here's a list) https://twitter.com/i/lists/953639568816984064?s=20

Review

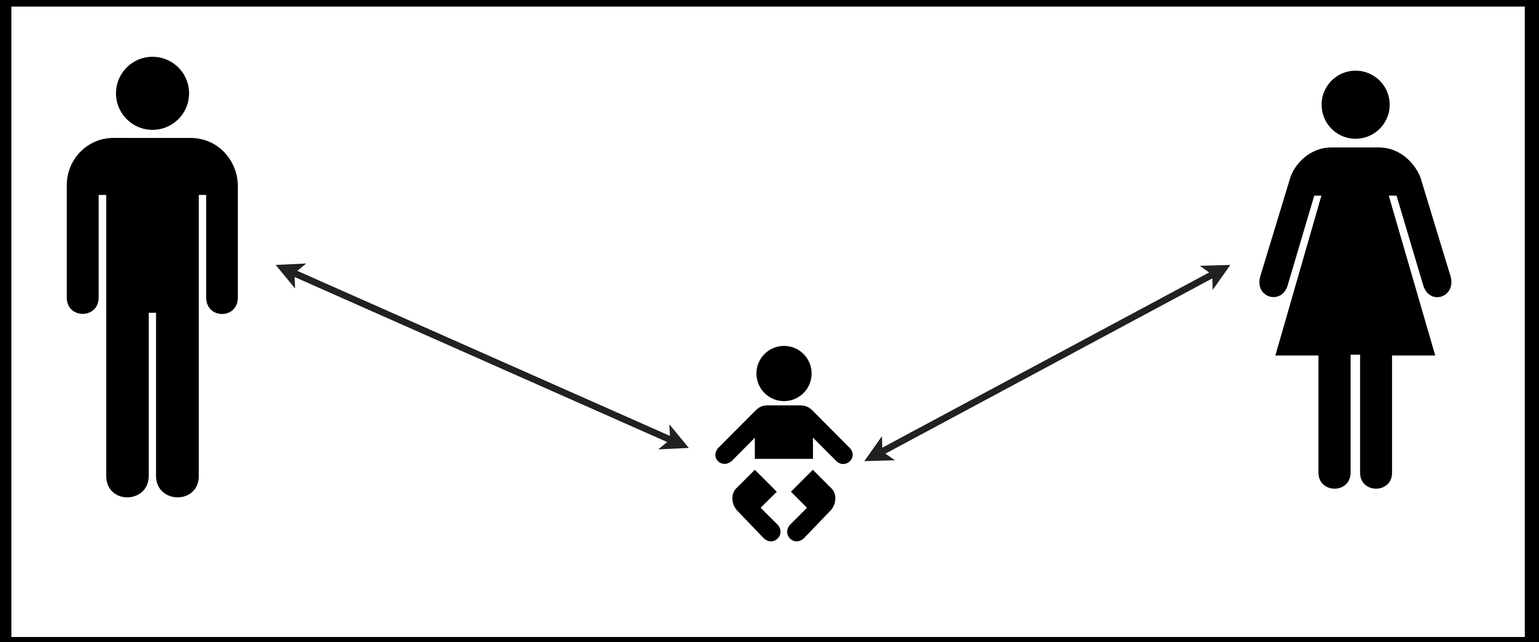
- Last time:
  - A few examples of how systems break
  - Bad primitives, bad protocols, bad implementation
- Today:
  - A (brief) tour through cryptologic history
  - Starting with symmetric (secret-key) crypto

Communication Model

Communication Model



Communication Model



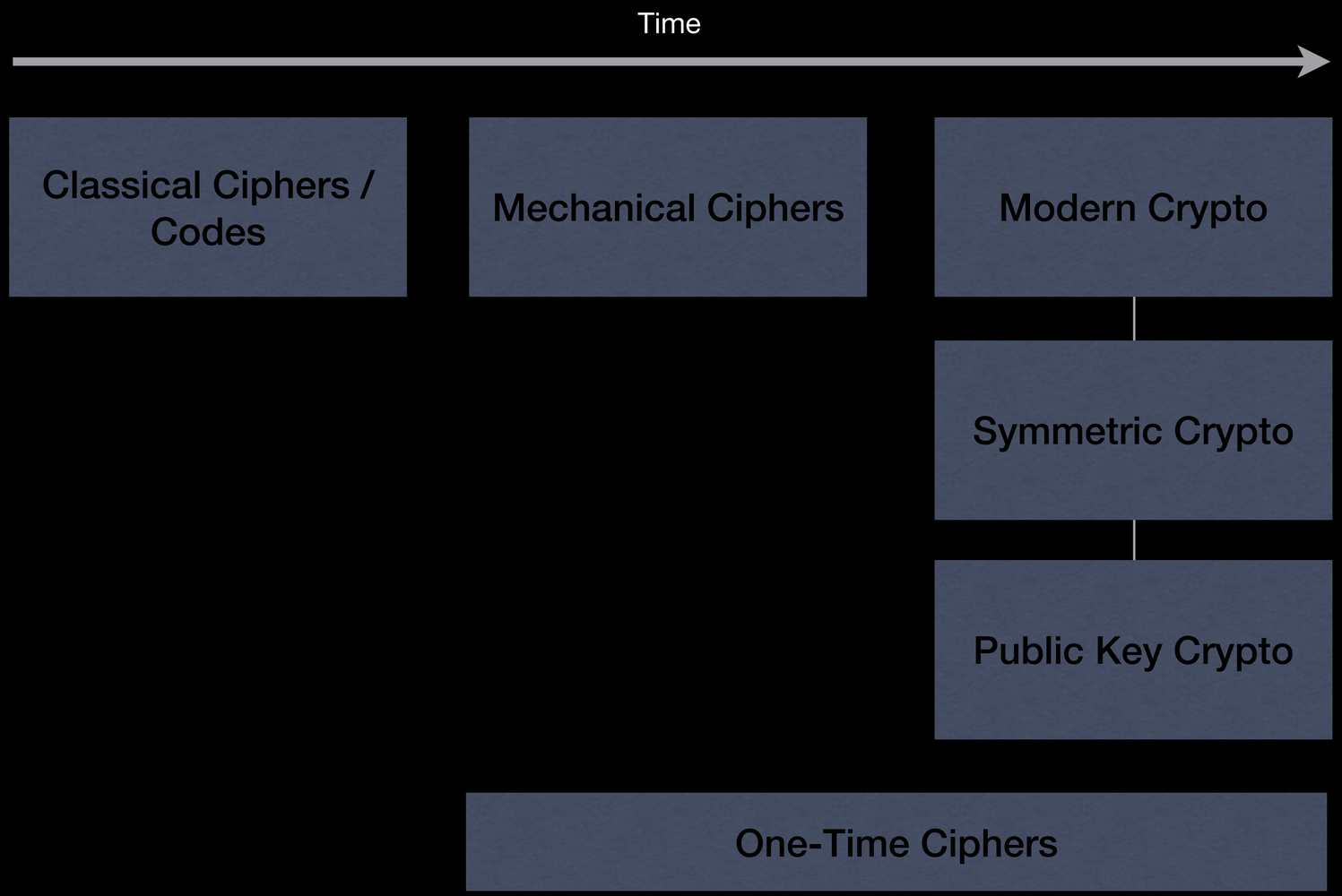
Secure Communication

- Two basic properties we like to achieve:
  - Data confidentiality
  - Data authenticity (“integrity”)

Secure Communication

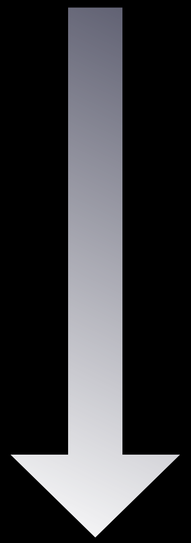
- Two basic properties we like to achieve:
  - Data confidentiality
  - Data authenticity (“integrity”)
- Tools:
  - Encryption / Key exchange
  - Message Authentication Codes (MACs)
  - Digital Signatures

History of Encryption



Classical Cryptography

- Beginning of time to 1900s or so
  - Shift (Caesar) cipher
  - Substitution ciphers
  - Polyalphabetic ciphers (Vigenère)
  - Digraph ciphers (Playfair)
  - A multitude of others...



Increasing
Complexity

<- Load New Puzzle

Tractability:11655

CRYPTOGRAM

Points 979

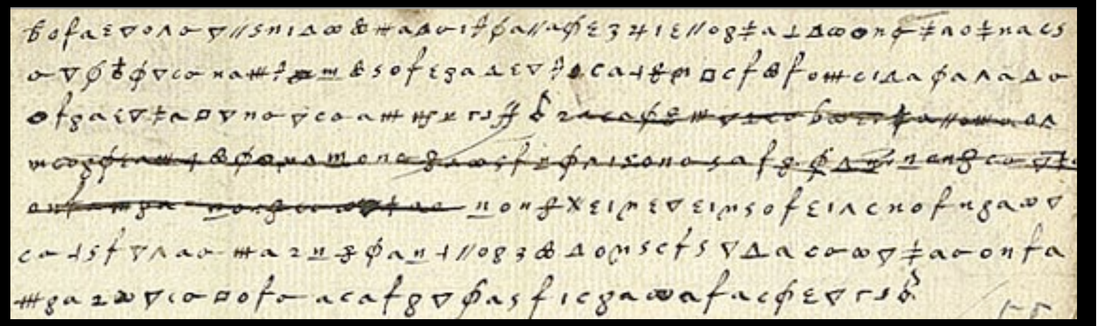
4/1/2009 0:21

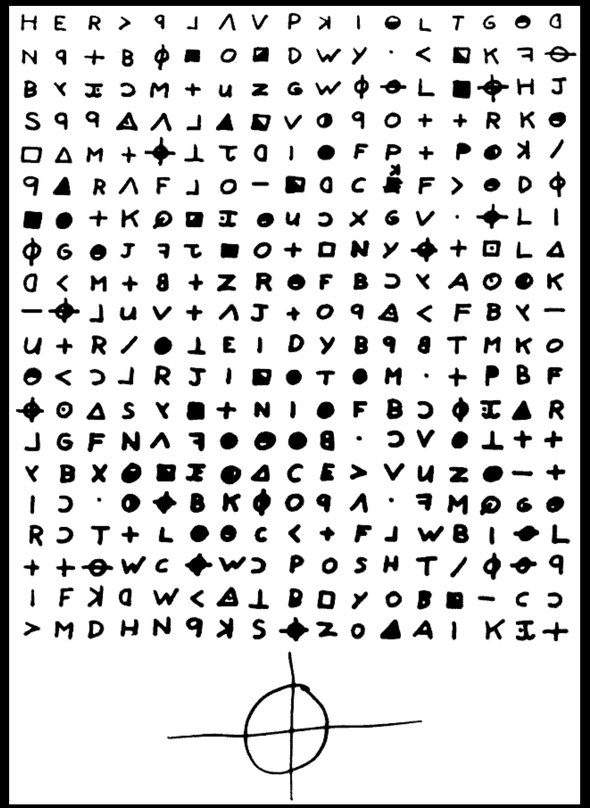
A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z

' P I G C G M N N U J C Y L I P G T Y T L P I Y T L M S F E P

VYKKNG MLG YH PIMP UFE RTFO UFE ' NN LCFO

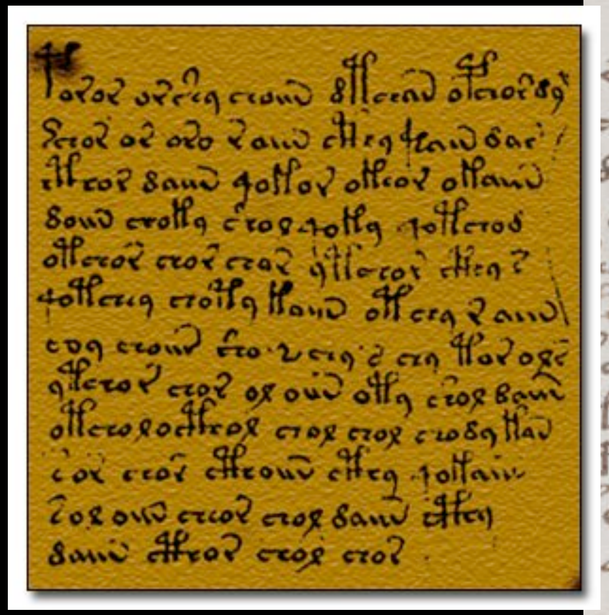
FEP FJ YP . ' - KFCYH KMU





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

S	E	N	D	R	E	I	N	F	O	R	C	E	M	E	N	T	S
V	I	G	E	N	E	R	E	V	I	G	E	N	E	R	E	V	I
N	M	T	H	E	I	Z	R	A	W	X	G	R	Q	V	R	O	A



Vigenere

S	E	N	D	R	E	I	N	F	O	R	C	E	M	E	N	T	S
V	I	G	E	N	E	R	E	V	I	G	E	N	E	R	E	V	I
N	M	T	H	E	I	Z	R	A	W	X	G	R	Q	V	R	O	A

One-Time Ciphers

- 1900s
  - Vernam & Mauborgne's "Unbreakable" cipher

•Based on Baudot code for Teletypes

•Added (XORed) a random Key (sequence of bits) to a binary message

  - Perfectly secure, provided:

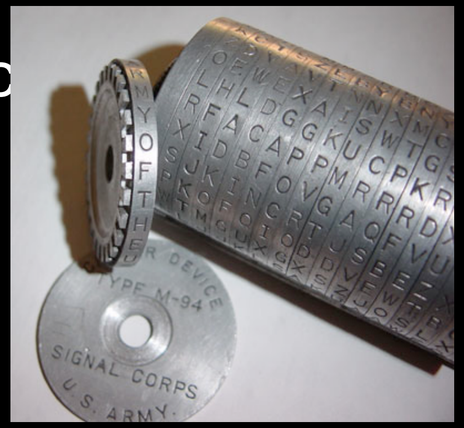
•key is perfectly random

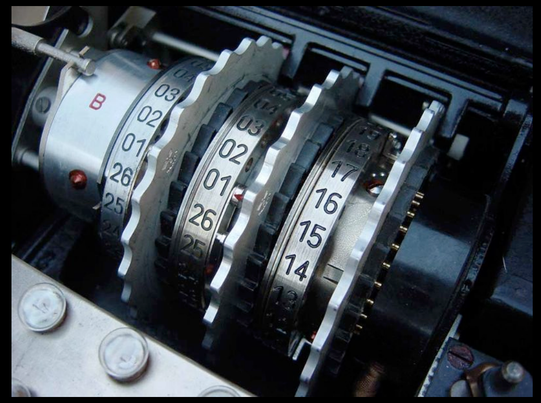
•key is at least as long as the message

•key is never re-used

Mechanical Cryptography

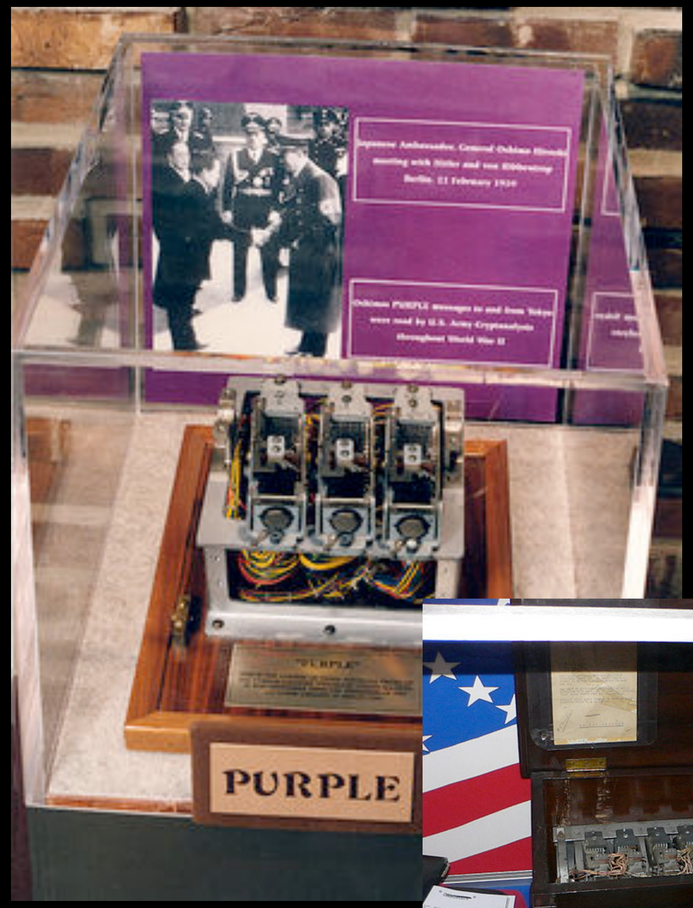
- 1900s
  - Mass production and usage of cipher devices
  - Rotor ciphers
  - Elec

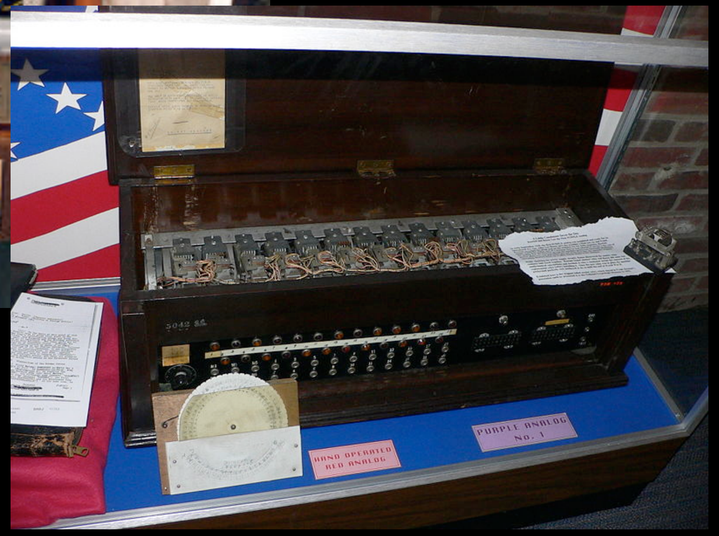


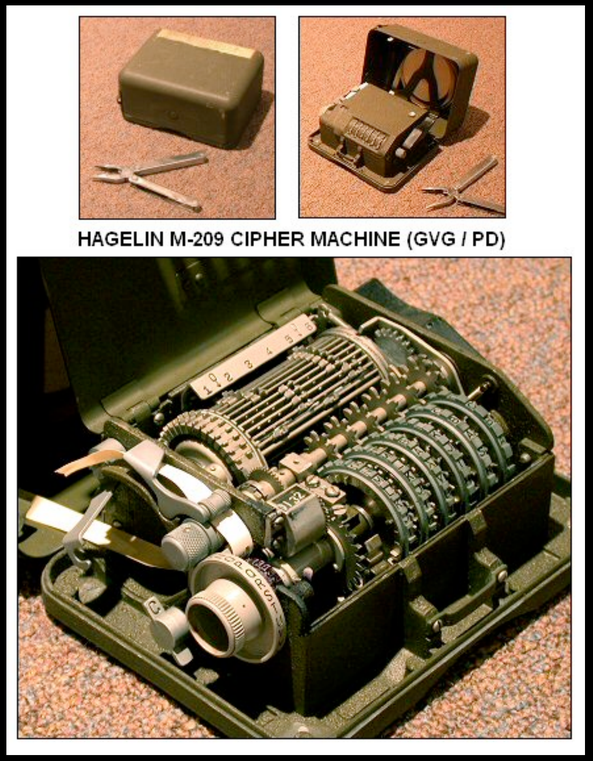


Increasing Complexity

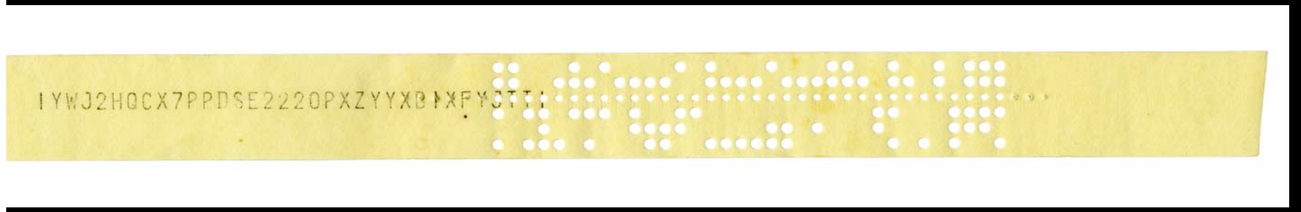
M-94 Cipher Wheel image by Bob Lord, used under a Creative Commons license.
Remaining images: Wikipedia [M-94, Enigma] used under GFDL.







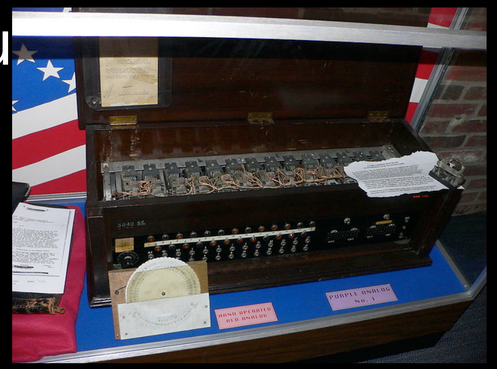
Purple Machine (top left) courtesy NSA, US Purple Replica (center) & M-209 images: Wikipedia used under GFDL/CC License.

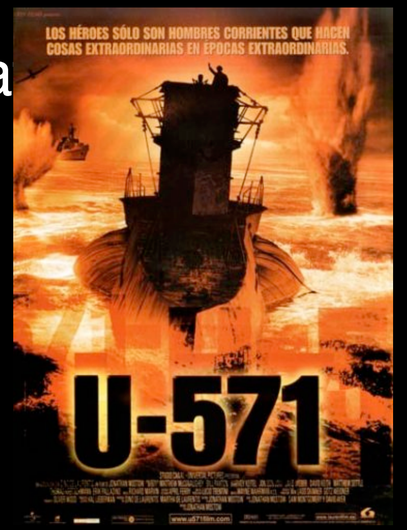


Russian Fialka device and tape by Bob Lord, used under a Creative Commons license.
HC-9 Image: Wikipedia, used under GFDL.

Summary

- Most cryptosystems ultimately broken
  - Sophistication of the attackers outpaces that of the cryptosystem
  - Security relies on secrecy of design
  - Not evaluated for chosen plaintext, known plaintext a
  - Key generation/distribution procedu
  - It’s an arms race...





Kerckhoffs' Principle

2. It must not be required to be secret, and it must be able to fall into the hands of the enemy without inconvenience;

"The enemy knows the System"
-- Claude Shannon's Maxim

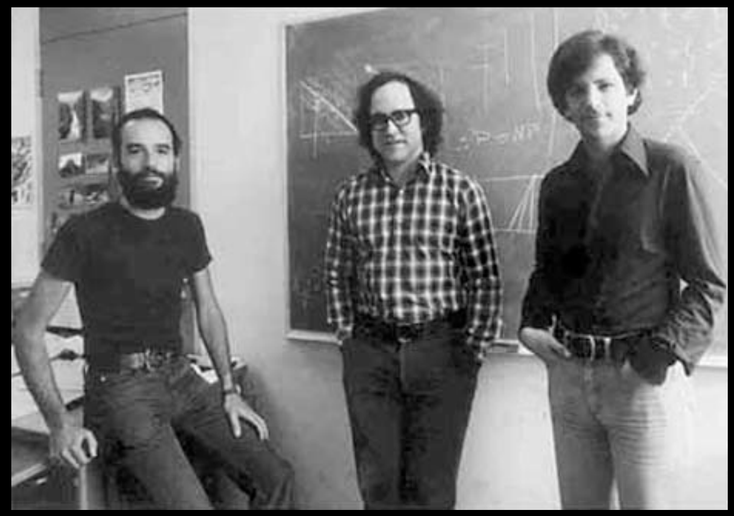
Public Domain image from David Kahn's The Codebreakers, credited to "Eugen Drezen, Historio de la Mondo Lingvo (Leipzig, 1931), 102".

The 1970s

1972

1976
(1974)

U.K. GCHQ



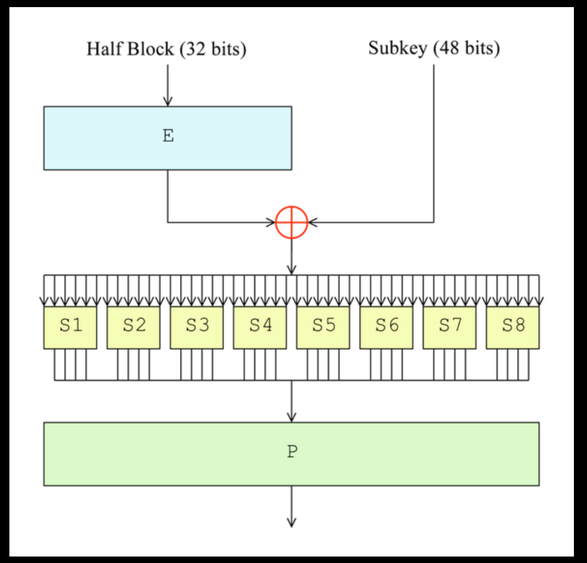
1977
(1973)

The Implications

- Exponential increase in study & usage of cryptography in industry, academia
- Wide-scale deployment of cryptographic systems
- Provable Security
  - Cryptographic Systems can be reduced to some hard mathematical problem

Data Encryption Standard

- Commercial-grade Block Cipher
  - 64-bit block size
  - 56 bit key (+ 8 bits parity)
  - “Feistel Network” Construction



Permutation