601.445/645
Practical Cryptographic Systems

Symmetric Cryptography

Instructor: Matthew Green

Piazza

- We will use Piazza for all communications, including schedule changes and snow days
- You must sign up!
- You can also find links to all of the class resources (syllabus, readings, Gradescope, etc.)

https://piazza.com/class/lqwivnfma0526

Housekeeping

- Waitlist: all students who are waitlisted should be allowed to join
- Assignment 1: out tomorrow!
  - This is a programming assignment in classical cryptography
  - We will send a “to all” message to the Piazza, and pin it as an announcement
  - Will also appear on the “Assignments” page in our Git repo

News

Security researchers hacked a Tesla Modem and collected awards of $722,500 on the first day of Pwn2Own Automotive 2024 for three bug collisions and 24 unique zero-day exploits.

Synacktiv Team (@Synacktiv) took home $100,000 after successfully chaining three zero-day bugs to get root permissions on a Tesla Modem.

They also used two unique two-bug chains to hack a Ubiquiti Connect EV Station and a JuiceBox 40 Smart EV Charging Station, earning an additional $120,000.

A third exploit chain targeting the ChargePoint Home Flex EV charger was already known but still brought them $16,000 in cash, with a total of $295,000 in prizes during the first day of the contest.

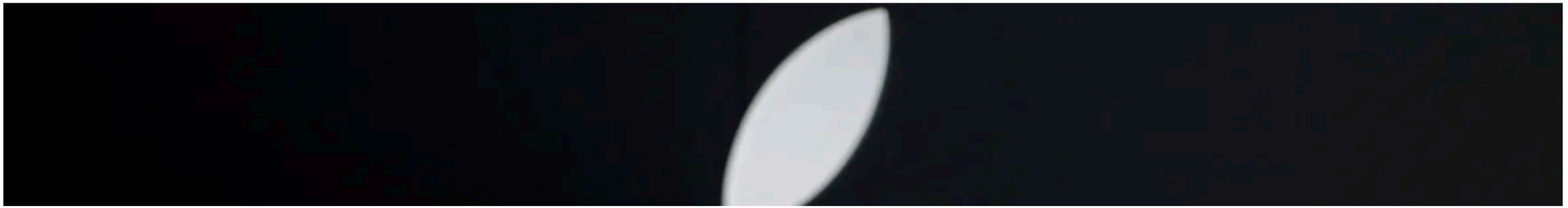
Security researchers also successfully hacked multiple fully patched EV charging stations and infotainment systems, with the NCC Group EDG team taking the second place on the leaderboard after winning $70,000 for zero-days exploited to hack the Pioneer DMH-WT7600NEX infotainment system and the Phoenix Contact CHARX SEC-3100 EV charger.

News

China claims it has cracked Apple AirDrop’s encryption to identify senders

By Juliana Liu and Hassan Tayir, CNN

2 minute read · Updated 2:46 AM EST, Wed January 10, 2024



News

PrivateDrop: Practical Privacy-Preserving Authentication for Apple AirDrop

Alexander Heinrich, Matthias Hollick, Thomas Schneider, Milan Stute, and Christian Weinert, *TU Darmstadt*

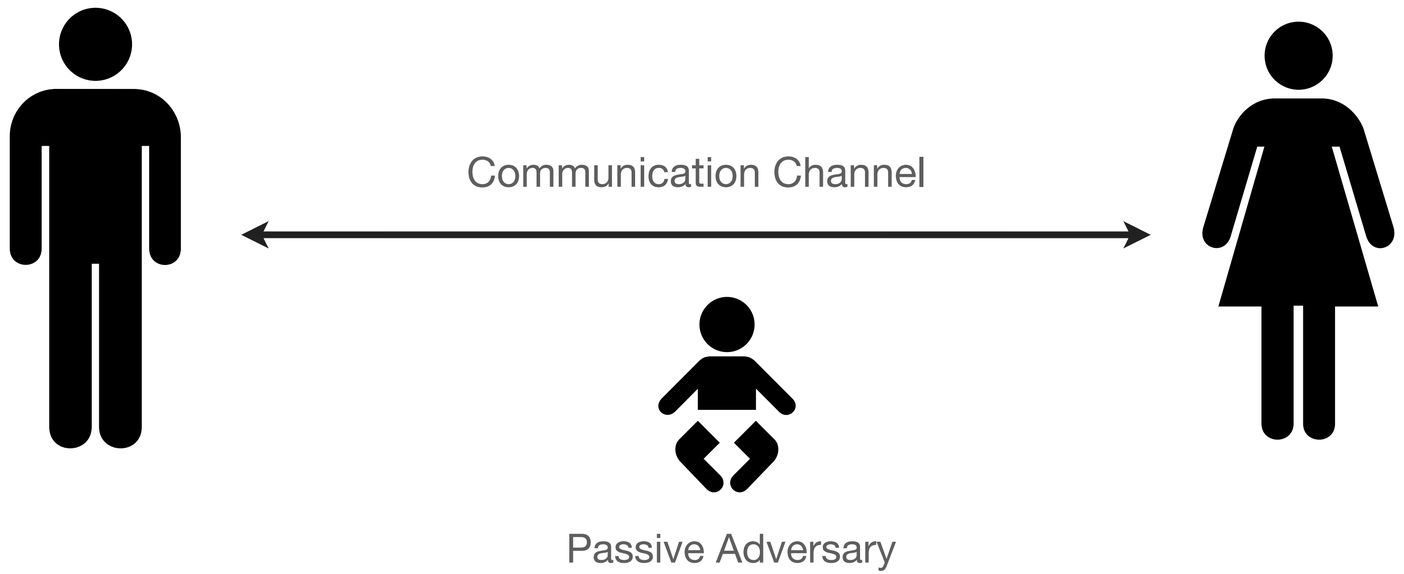
https://www.usenix.org/conference/usenixsecurity21/presentation/heinrich

Review

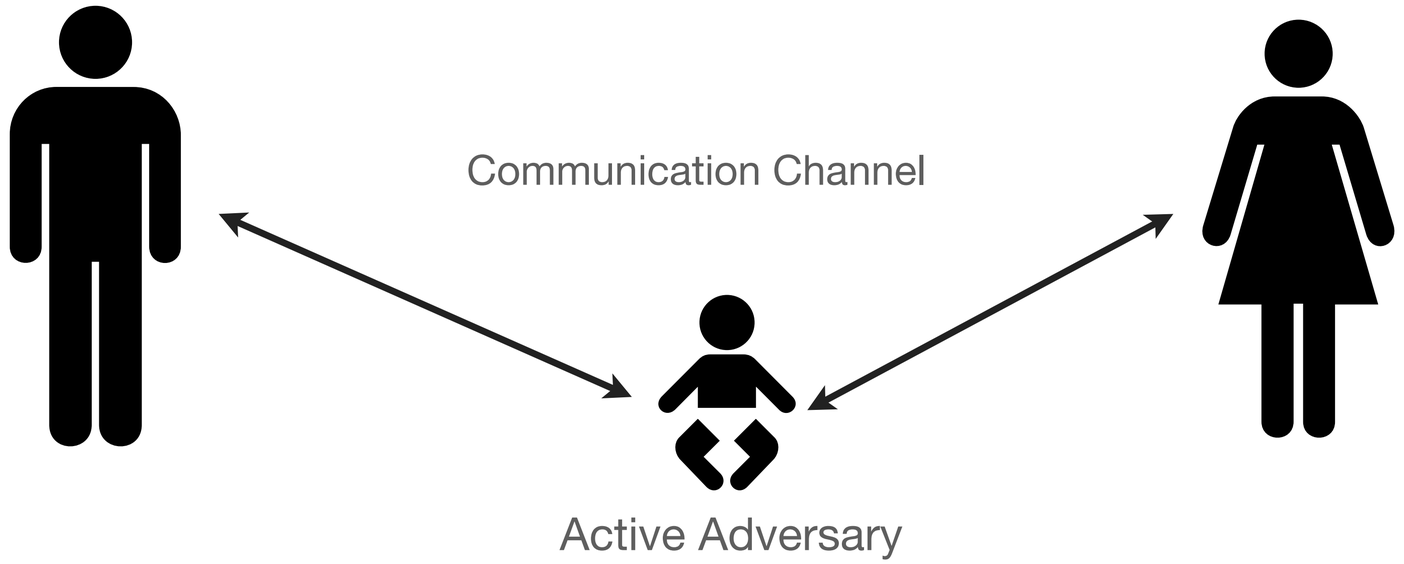
- Last time:
  - A few examples of how systems break
  - Bad primitives, bad protocols, bad implementation
- Today & Weds:
  - A (brief) tour through cryptologic history
  - Starting with symmetric (secret-key) crypto

Communication Model

Communication Model



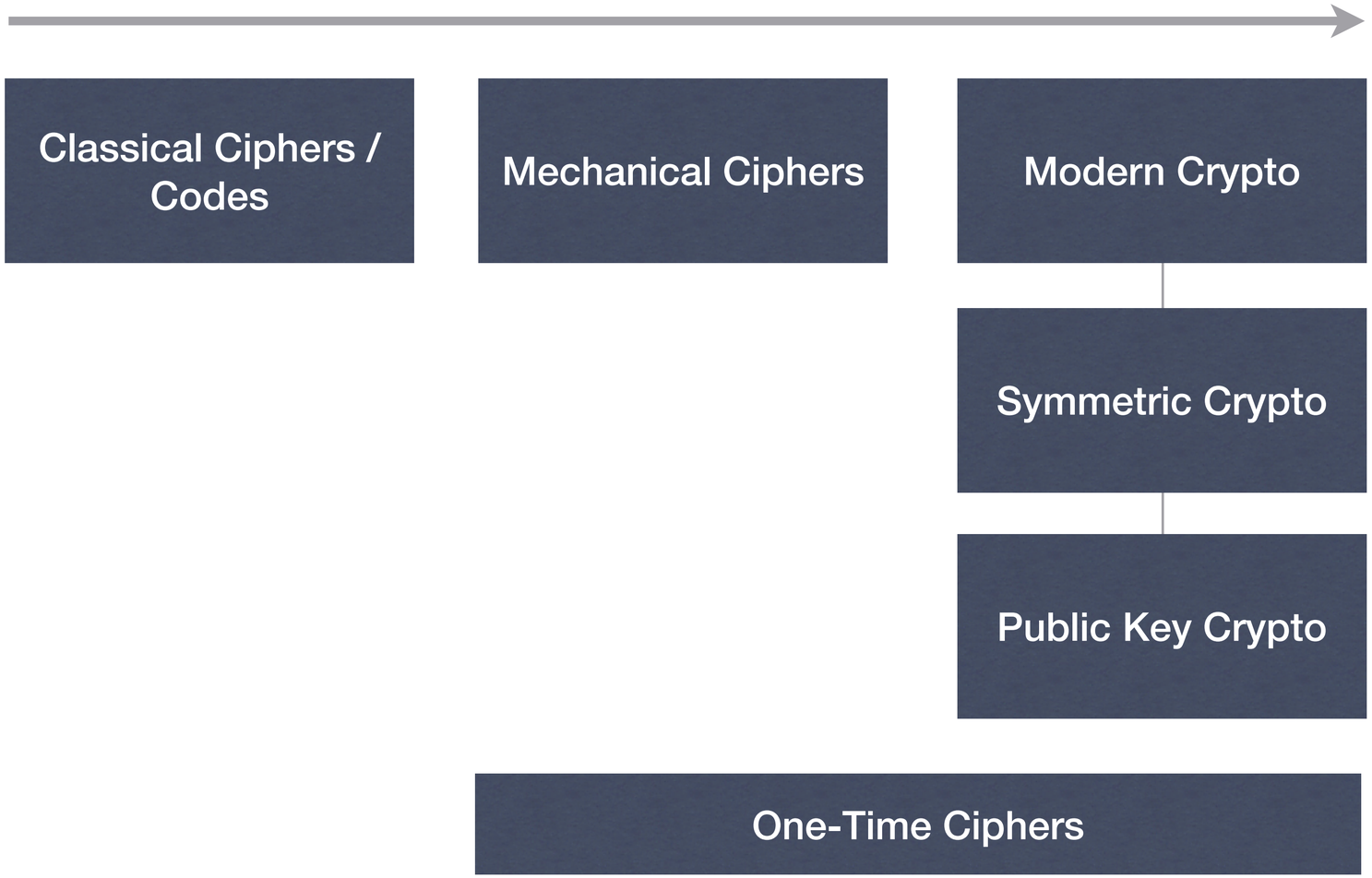
Communication Model



Secure Communication

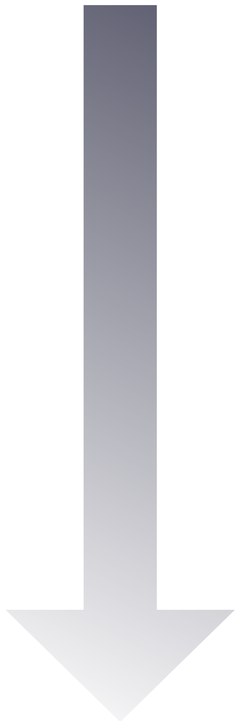
- Two basic properties we like to achieve:
  - Data confidentiality
  - Data authenticity (“integrity”)
- Tools:
  - Encryption
  - Message Authentication Codes (MACs)
  - Digital Signatures

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

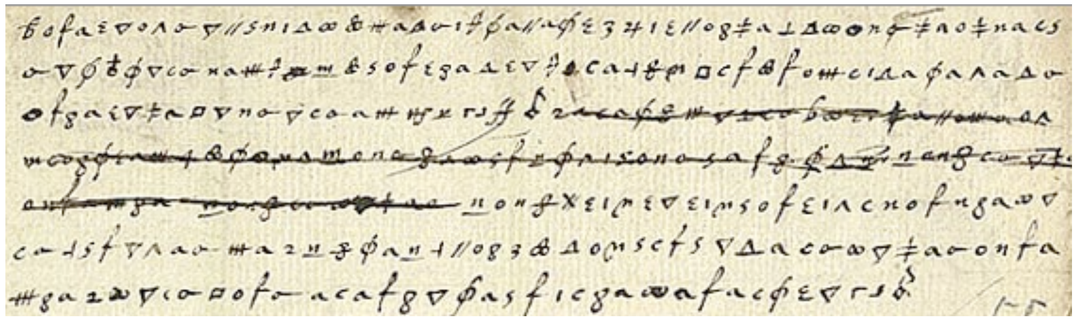
' P I G C G M N N U J C Y L I P G T Y T L P I Y T L M S F E P

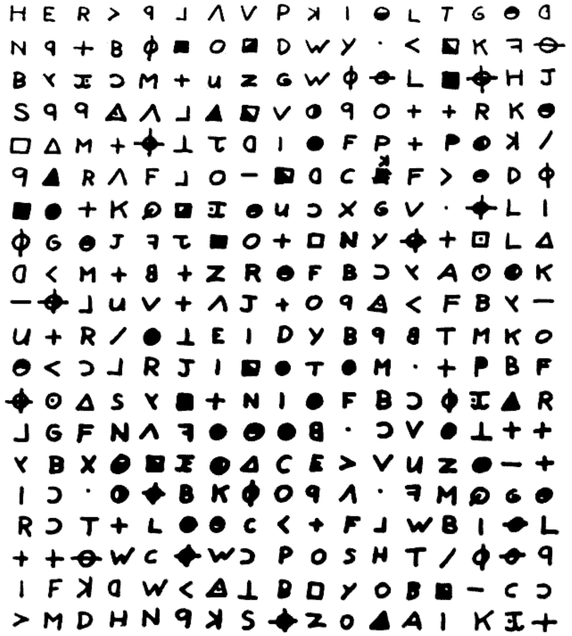
'

V Y K K N G M L G Y H P I M P U F E R T F O U F E ' N N L C F O

F E P F J Y P . ' - K F C Y H K M U

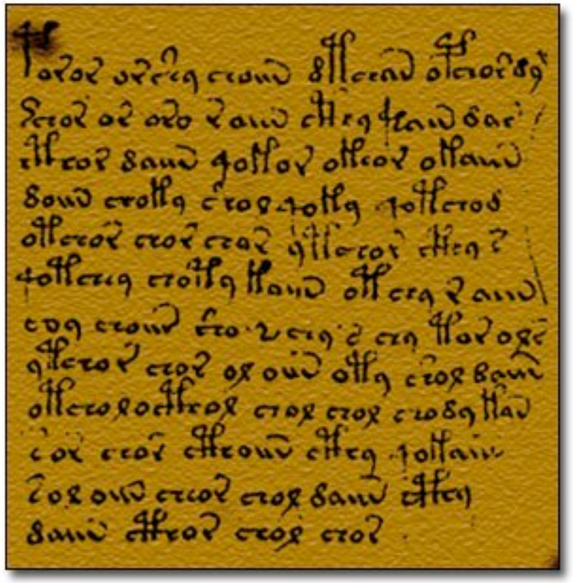
. ' -





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

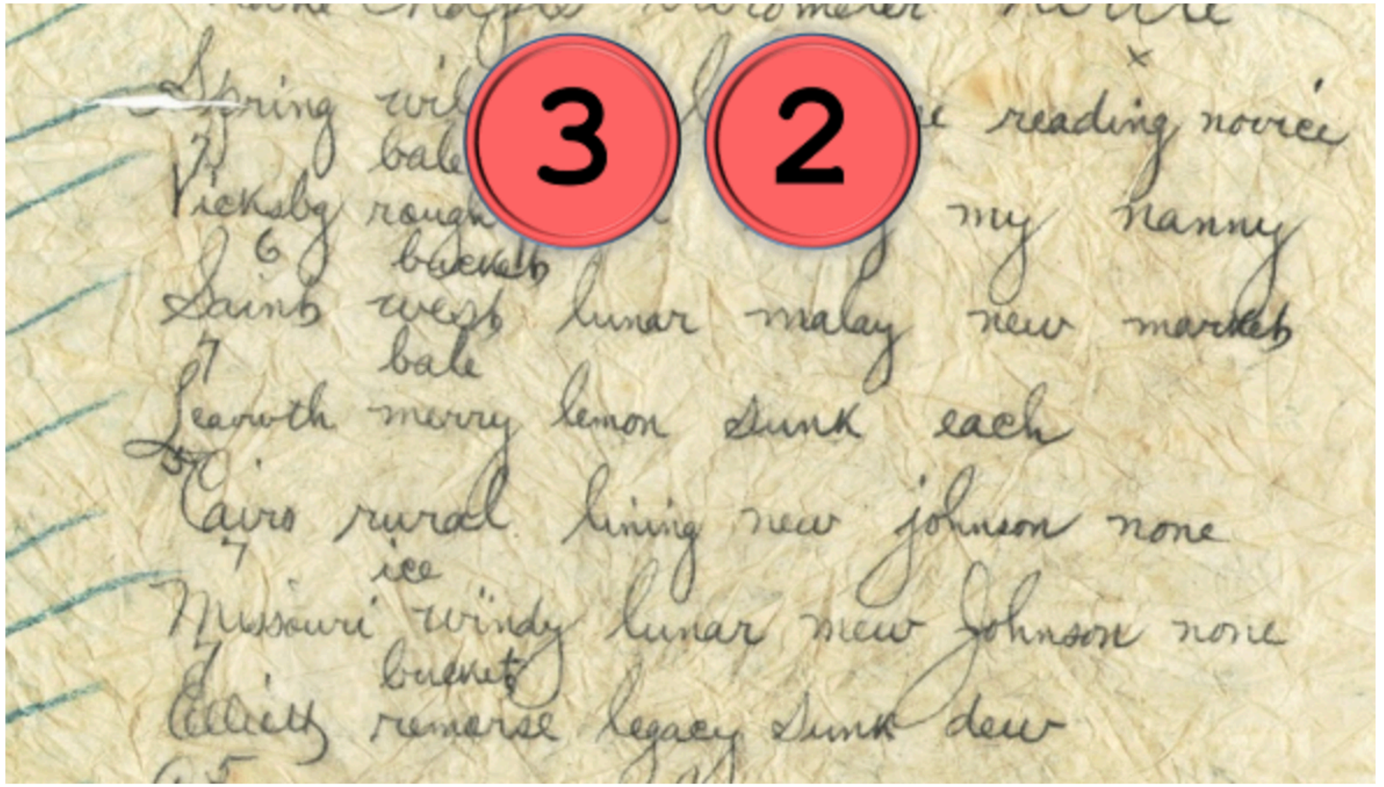
S	E	N	D	R	E	I	N	F	O	R	C	E	M	E	N	T	S
V	I	G	E	N	E	R	E	V	I	G	E	N	E	R	E	V	I
N	M	T	H	E	I	Z	R	A	W	X	G	R	Q	V	R	O	A




78

The Top 50 unsolved encrypted messages: 32. The silk dress cryptogram

Von Klaus Schmeh / 13. Mai 2017 / 6 Kommentare / Seite 1 von 2 / Auf einer Seite lesen



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

(No Model.)

11 Sheets—Sheet 6.

J. M. E. BAUDOT.

PRINTING TELEGRAPH.

No. 388,244. Patented Aug. 21, 1888.

Fig. 24.

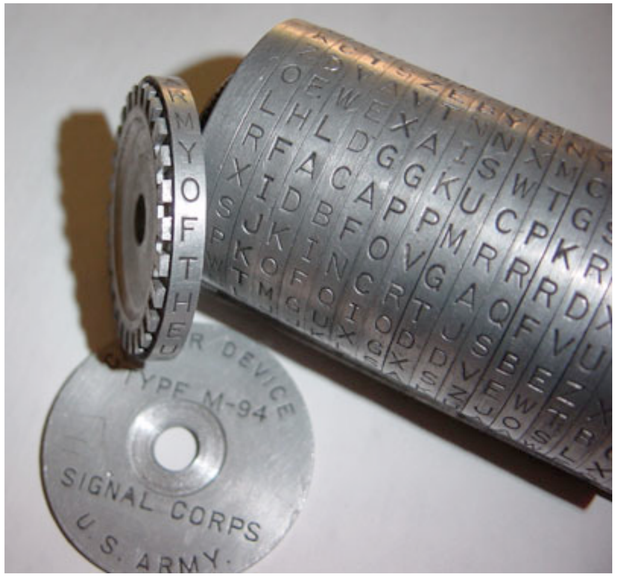
	1	2	3	4	5
A	+	−	−	−	−
B	−	−	+	+	−
C	+	−	+	+	−
D	+	+	+	−	−
E	−	+	−	−	−
F	+	+	−	+	−
G	−	+	−	+	−
H	+	+	−	+	−
I	−	−	+	−	−
J	+	−	+	−	−
K	+	+	+	−	+
L	−	+	+	+	+
M	+	+	+	+	+
N	−	+	+	+	−
O	+	+	+	+	+
P	+	−	+	+	+
Q	−	−	+	−	+
R	−	−	+	−	+
S	+	−	+	−	−
T	−	−	+	−	+
U	+	+	+	−	+
V	−	+	−	−	+
W	−	+	−	−	+
X	+	−	+	−	−
Y	+	−	−	−	+
Z	−	−	−	+	+
Ł	−	−	−	+	−
Ń	−	−	−	−	+

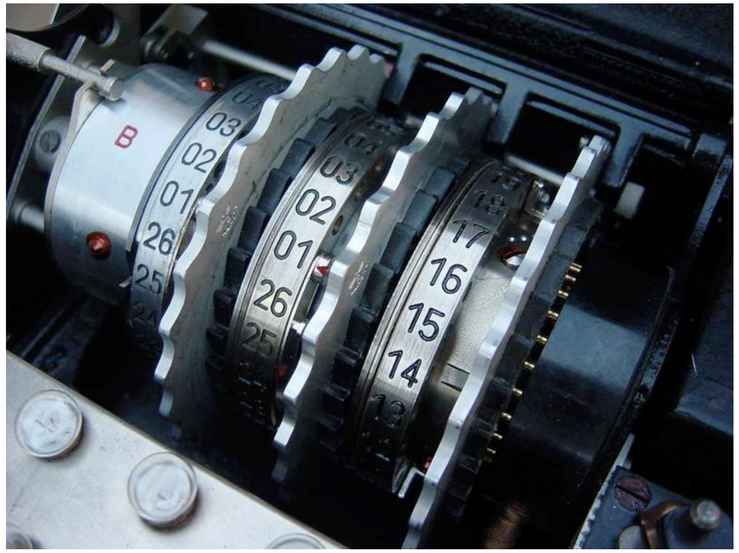
INVENTOR:

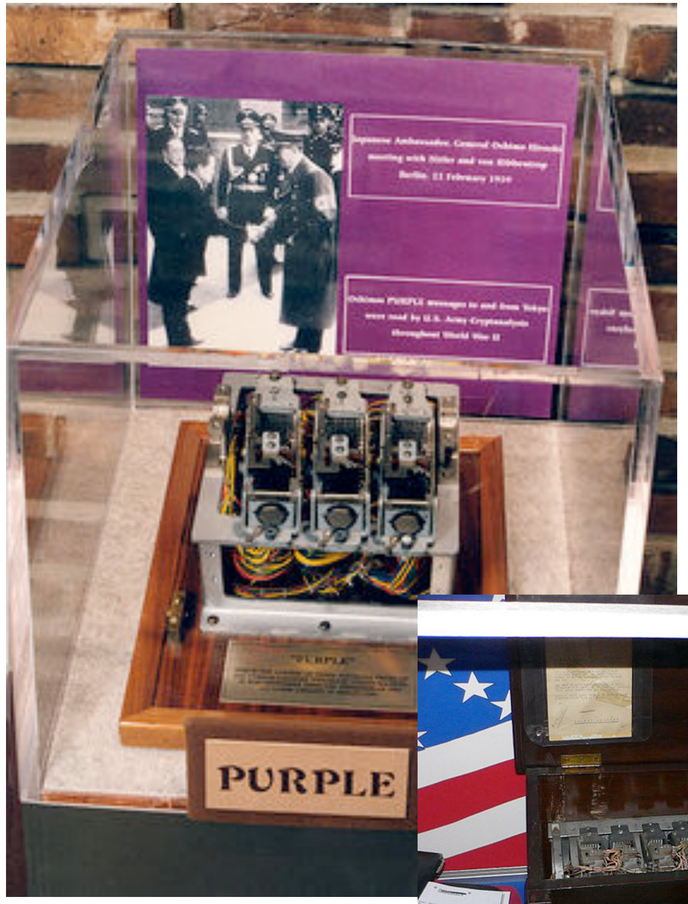
Jean Maurice Émile Baudot

Mechanical Cryptography

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

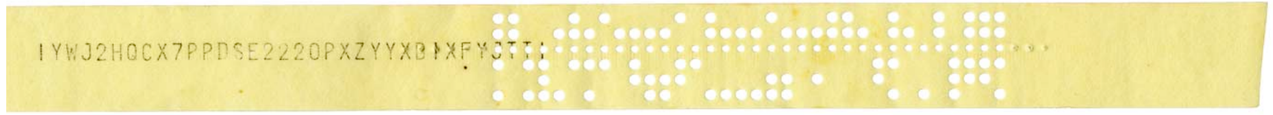






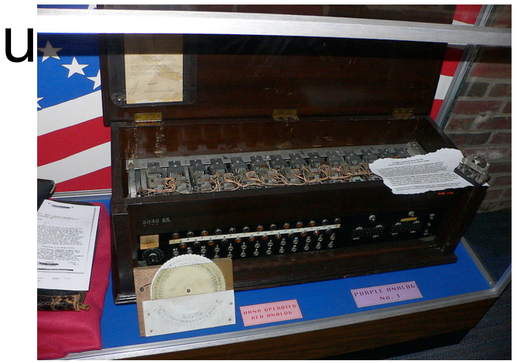
HAGELIN M-209 CIPHER MACHINE (GVG / PD)

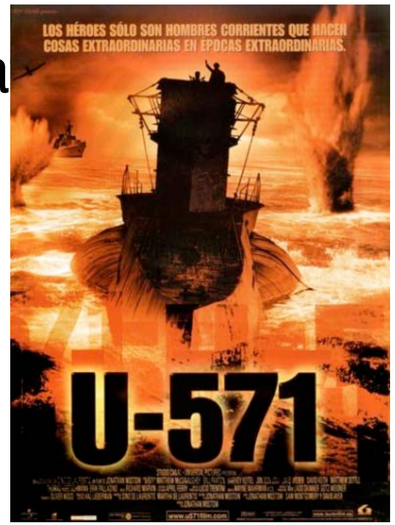

0015
AB CD EF GH I J KL MN OP QR ST UV WX YZ
AB CD EF GH I J KL MN OP QR ST UV WX YZ
0 AB
1 CD
2 EF
3 GH
4 I J
5 KL
6 MN
7 OP
8 ST
9 UV



Summary

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



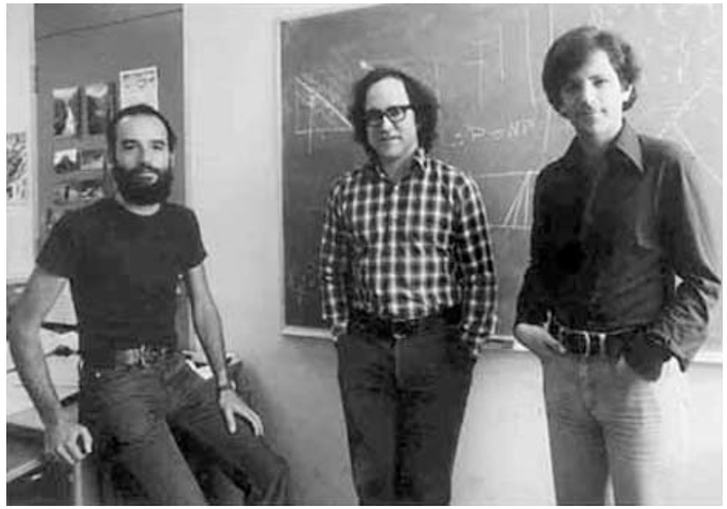


Kerckhoffs' Principle

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

The 1970s



U.K. GCHQ

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