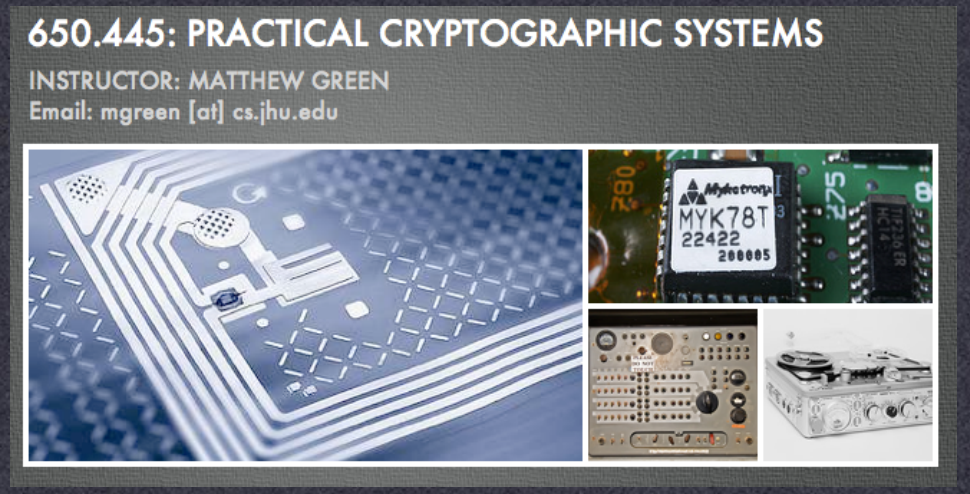
650.445: Practical Cryptographic Systems

Symmetric Cryptography

Instructor: Matthew Green

Housekeeping

- Website is updated
  - http://spar.isi.jhu.edu/~mgreen/650.445/
  - Slides up as we go
  - Reading assignment today (for next Mon)
    - Anderson chap 5.7

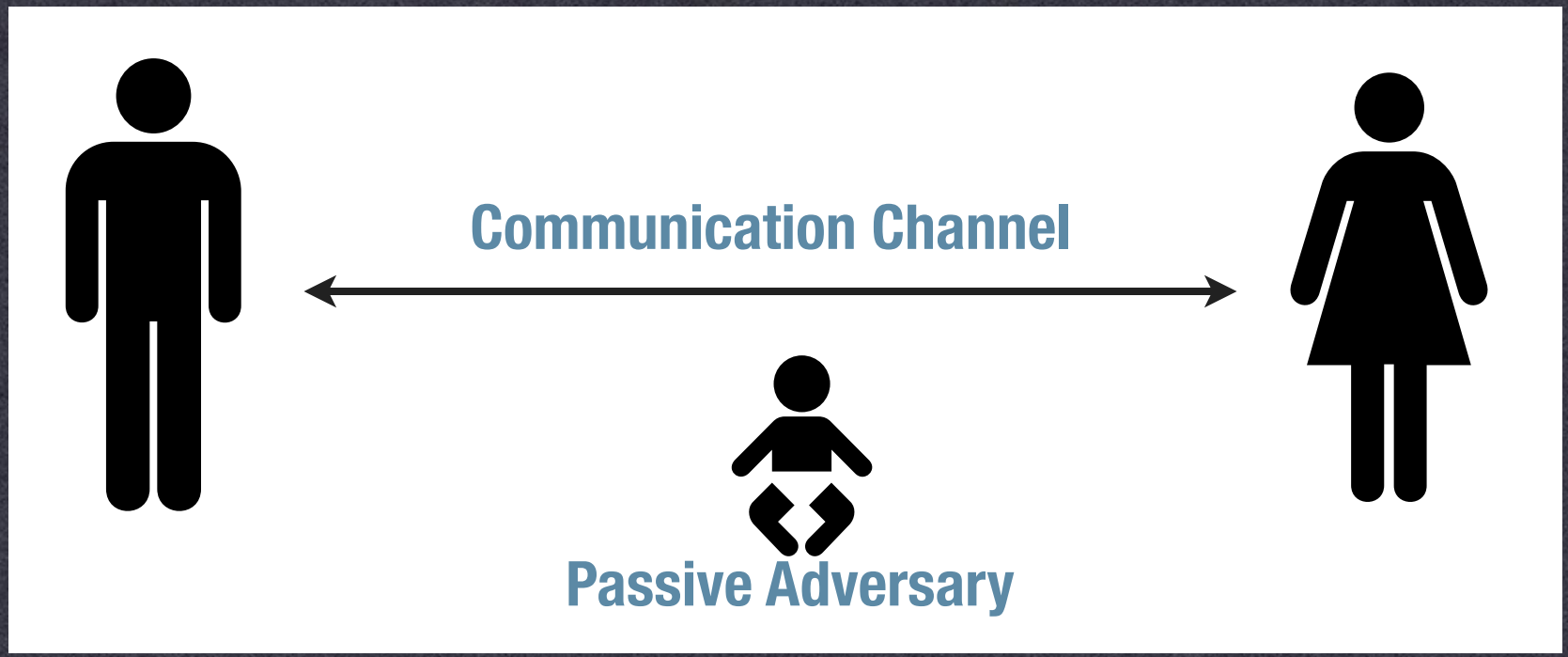


Review

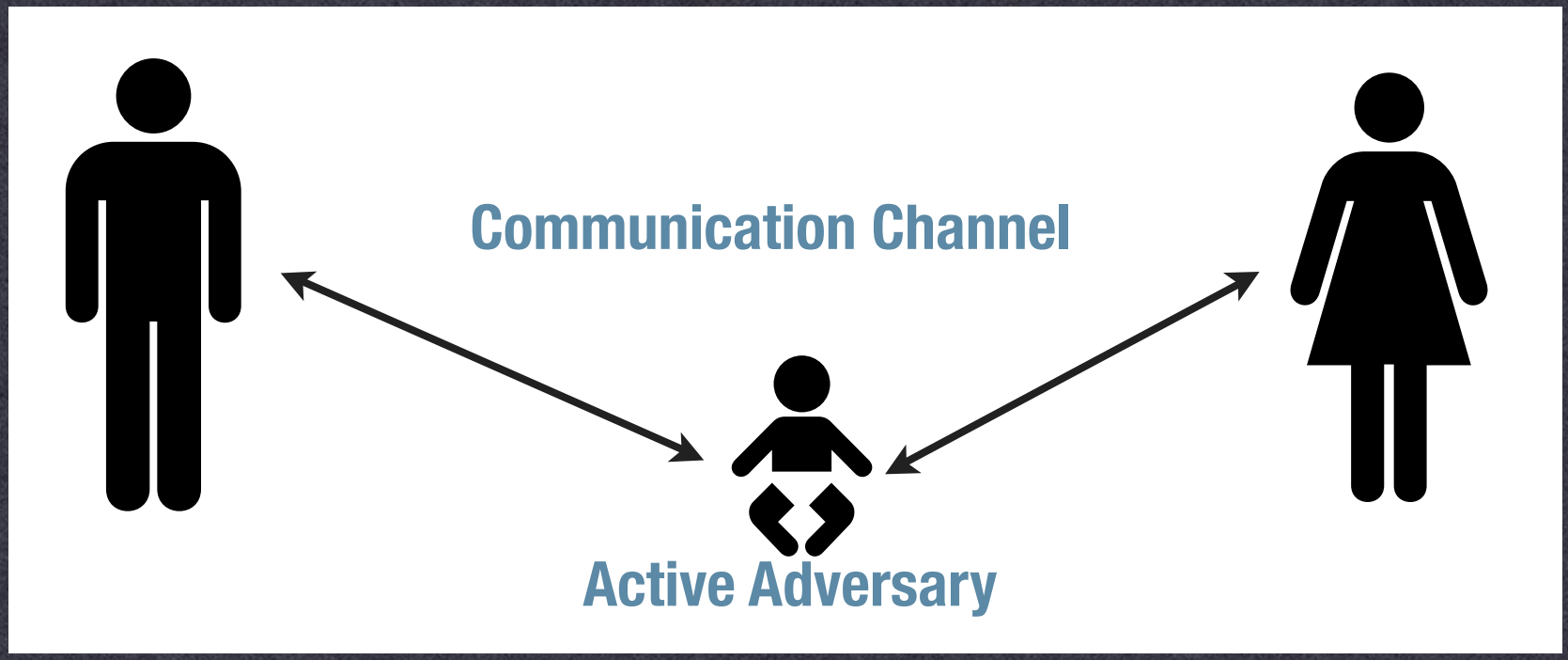
- Last time:
  - A few examples of how systems break
  - Bad primitives, bad protocols, bad implementation
- Today & Weds:
  - A (brief) tour through cryptologic history
  - Starting with symmetric (secret-key) crypto

Communication Model

Communication Model



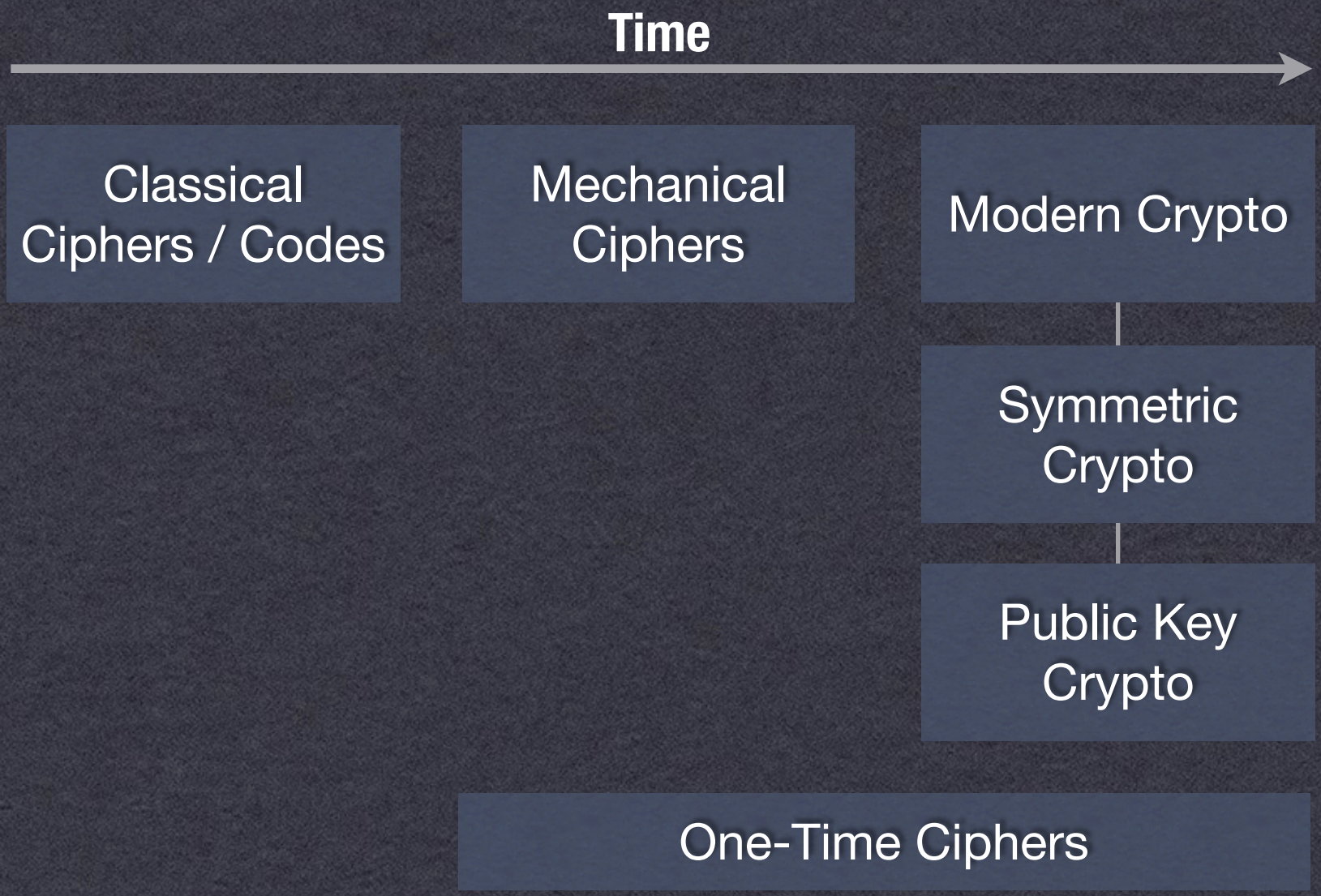
Communication Model



Secure Communication

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

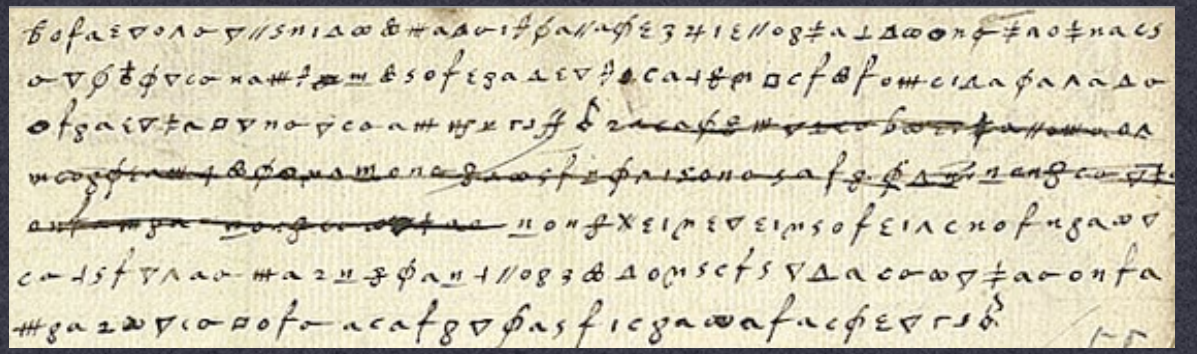
A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z

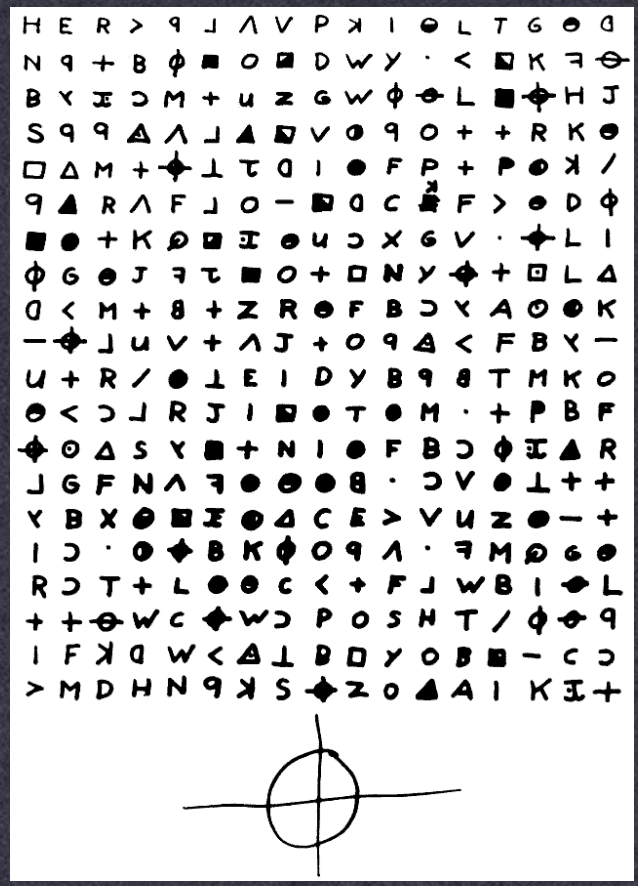
' P I G C G M N N U J C Y L I P G T Y T L P I Y T L M S F E P

'

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

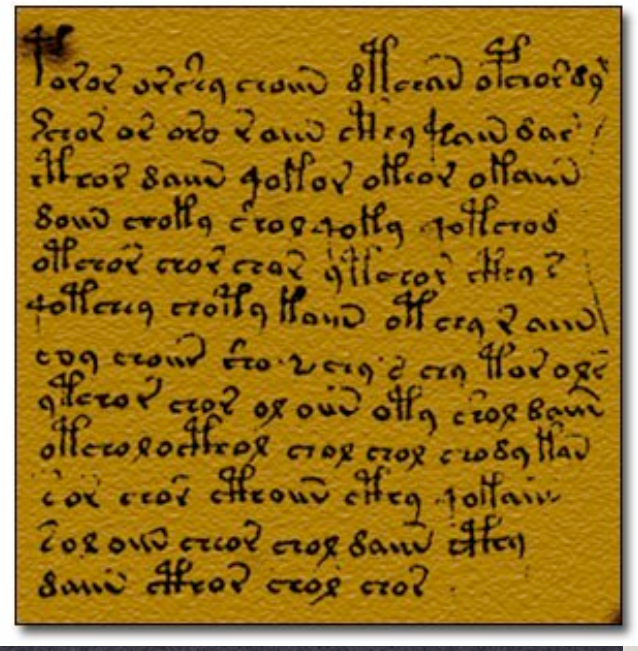
F E P F J Y P . ' - K F C Y H K M U

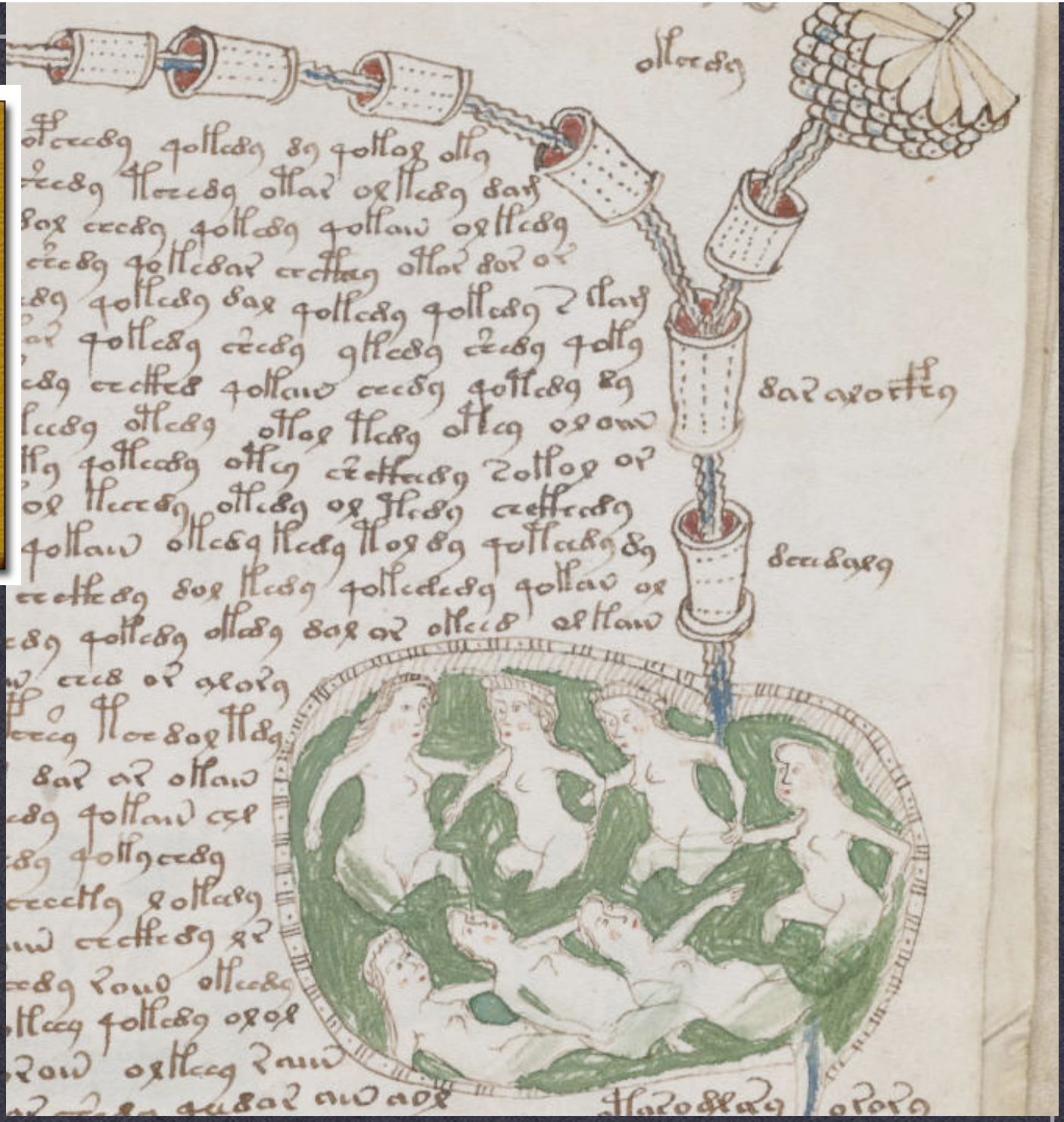




A	G	R	P	T
B	I	K	C	Q
S	L	D	M	E
N	Y	W	F	X
G	J	H	O	Z

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





One-Time Ciphers

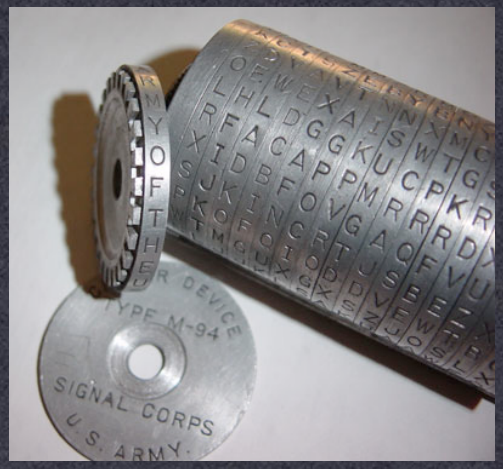
- 1900s
  - Vernam & Mauborgne's "Unbreakable" cipher
    - Based on Baudot code for Teletypes
    - Added (XORed) a random Key (sequence of bits) to a binary message
  - Perfectly secure, provided:
    - key is perfectly random
    - key is at least as long as the message
    - kev is never re-used

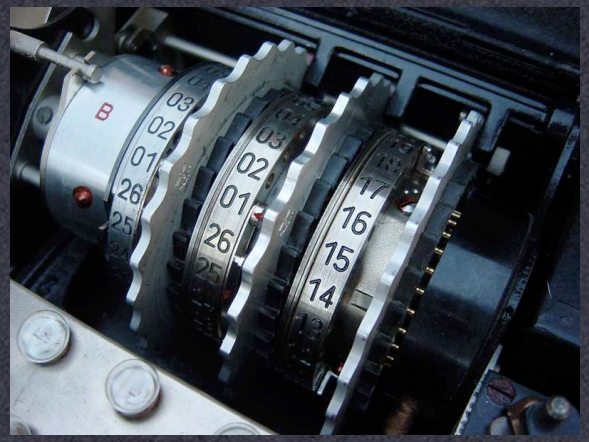
Numbers Stations

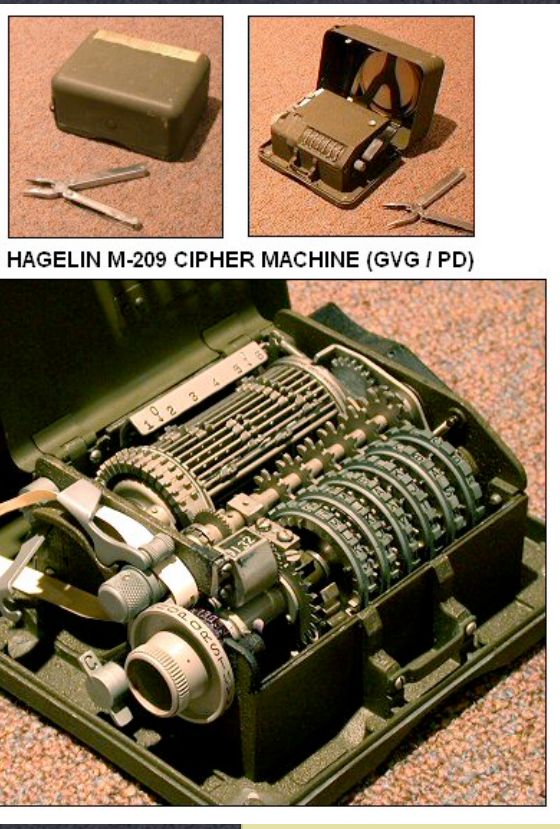
Mechanical Cryptography

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

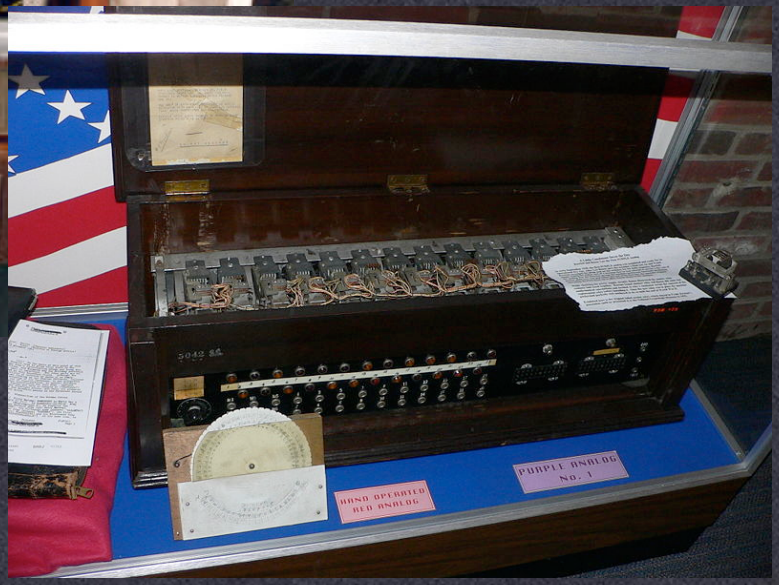
Increasing Complexity







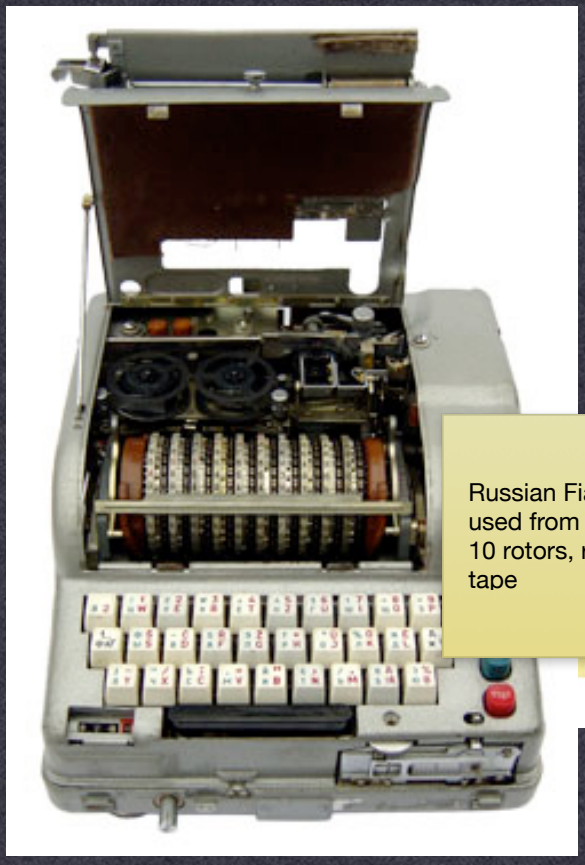
US M-209, broken by Germans in 1943 but still used tactically



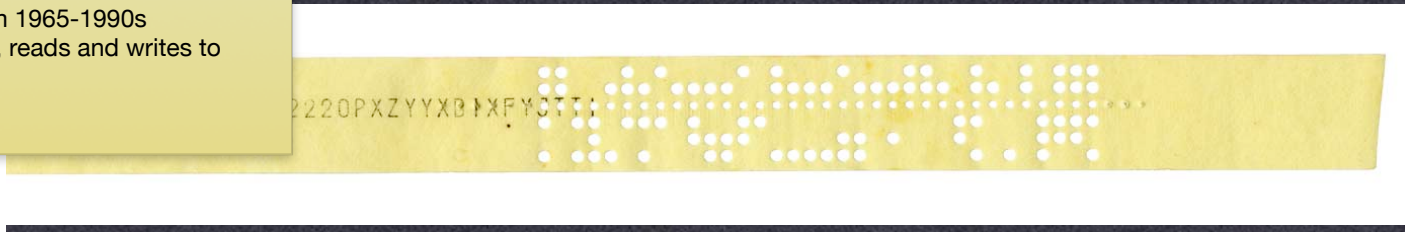
Purple Machine (top left) courtesy NSA, US Purple Replica (center) & M-209 images: Wikipedia used under GFDL/CC License.

Swedish AB Transvertex HC-9.
Commercial devices used for low-level communications until 1970s. Punch

Swiss NEMA
Late 1940s. "Improved" version of the Enigma-K.
10 rotors.
Same weakness as Enigma: ciphertext never equals plaintext.
Declassified in 1992.
Simple attack = 2^41



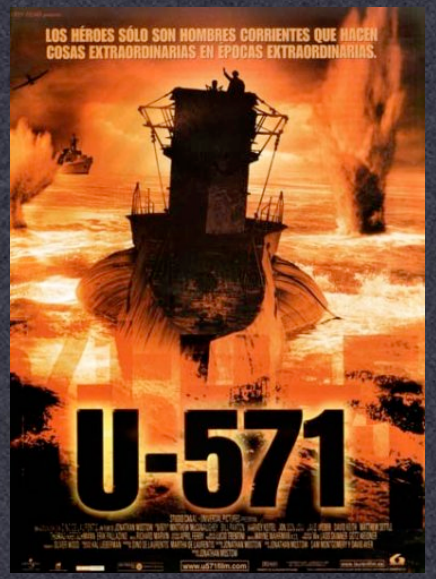
Russian Fialka
used from 1965-1990s
10 rotors, reads and writes to tape



Images of Swiss Nema, 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 attacks
  - Key generation/distribution procedures
  - 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

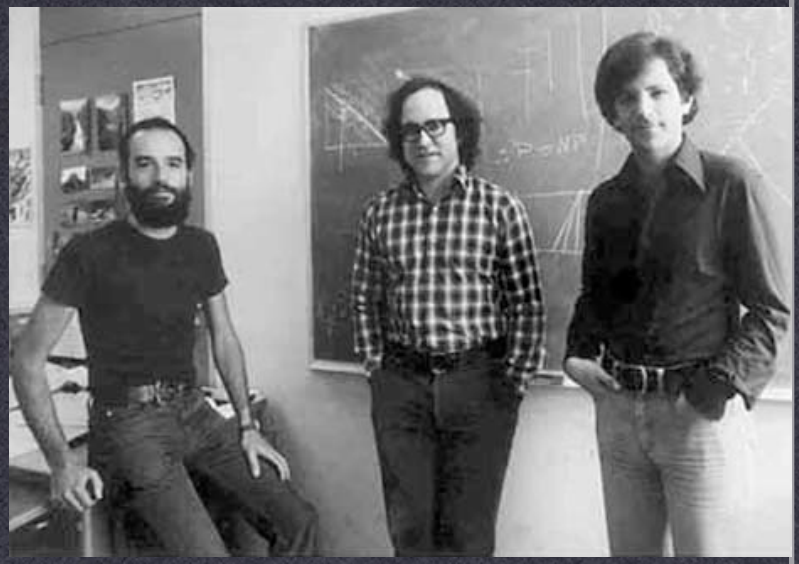
Public Domain image from David Kahn's The Codebreakers, credited to "Eugen Drezen, Historio de la Mondo Lingvo (Leipzig, 1931), 102".

The 1970s

1972

1976

(1974) ⟵ U.K. GCHQ ⟶ (1973)



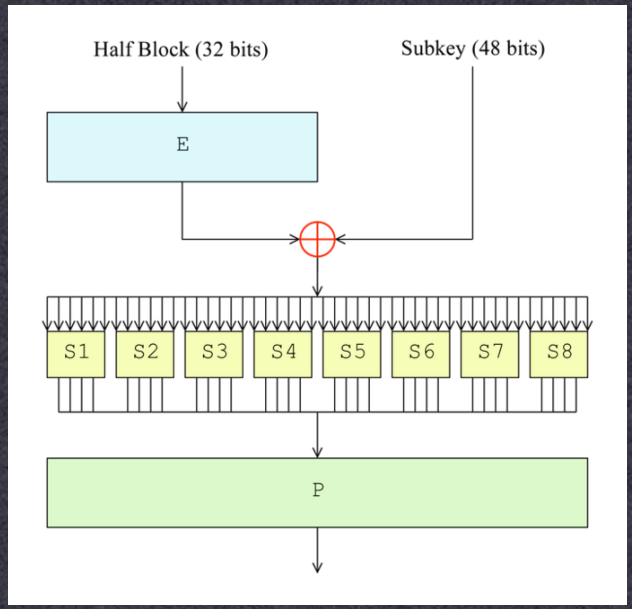
1977

The Implications

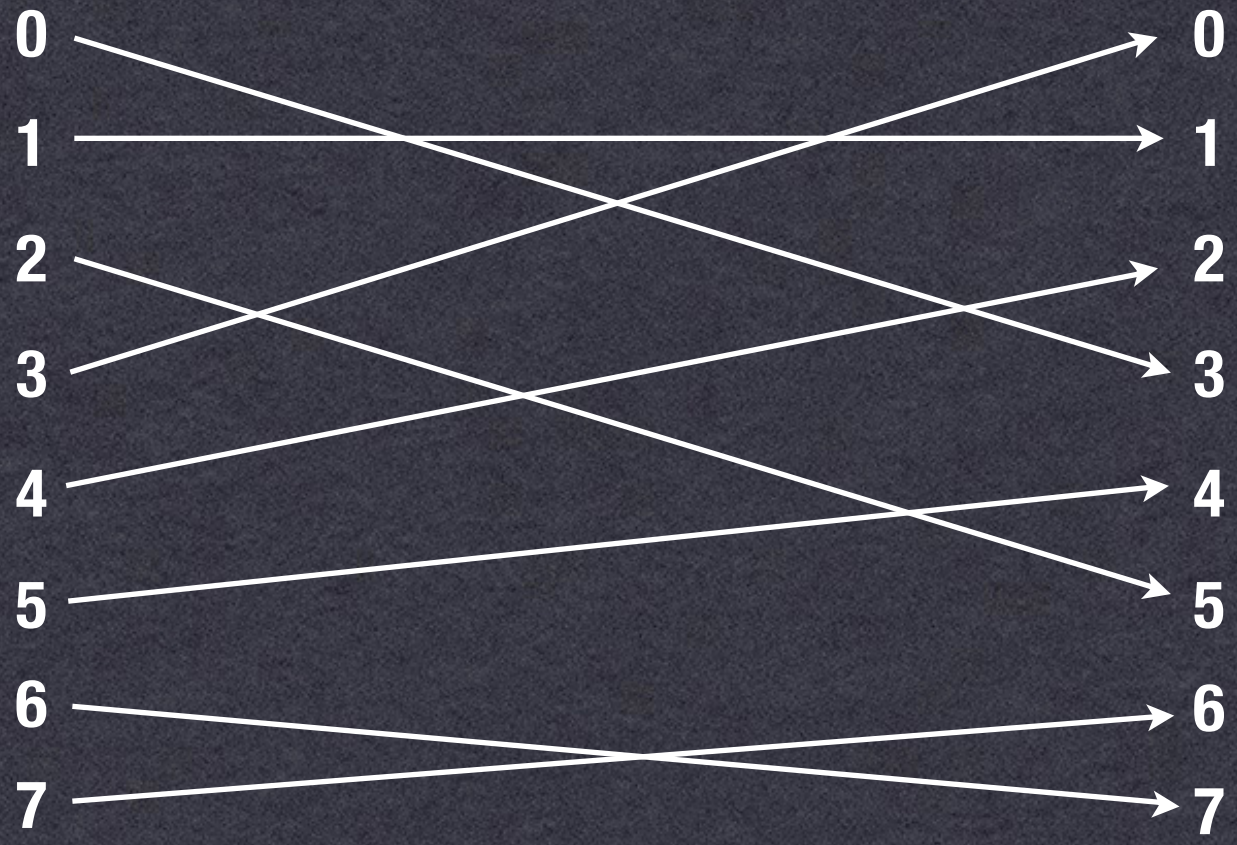
- Exponential increase in study & usage of cryptography in industry, academia
- Wide-scale deployment of cryptographic systems
- Provable Security
  - Cryptographic Systems can be reduced to some hard mathematical problem

Data Encryption Standard

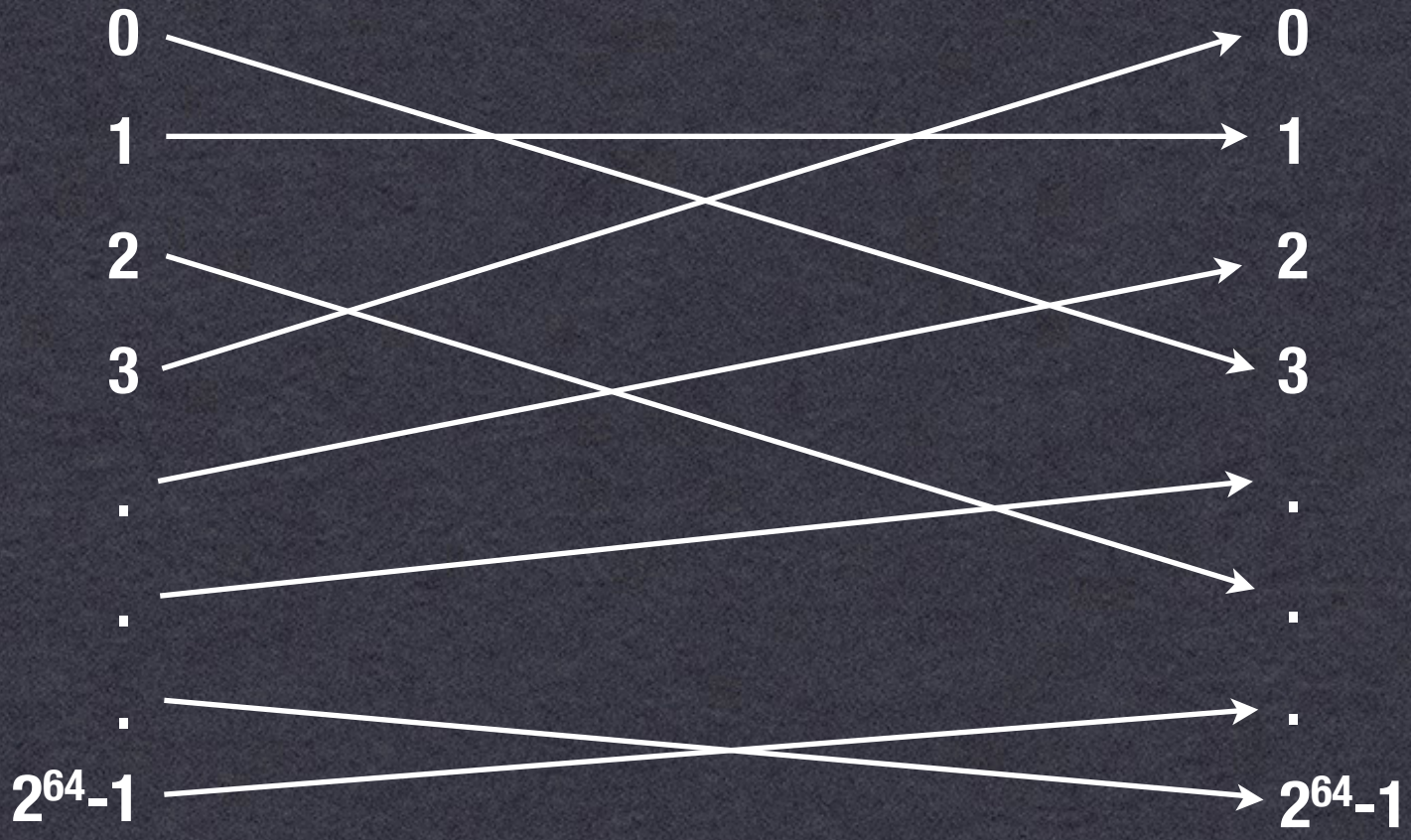
- Commercial-grade Block Cipher
  - 64-bit block size
  - 56 bit key (+ 8 bits parity)
  - “Feistel Network” Construction



Permutation



Permutation



Permutation Families

- Can't have just one permutation
  - Alice & Bob know the permutation
    Adversary doesn't
  - Permutation is "random" (ish)
  - But there are $2^{64}!$ possible permutations
  - DES has a 56 bit key...

Block Cipher

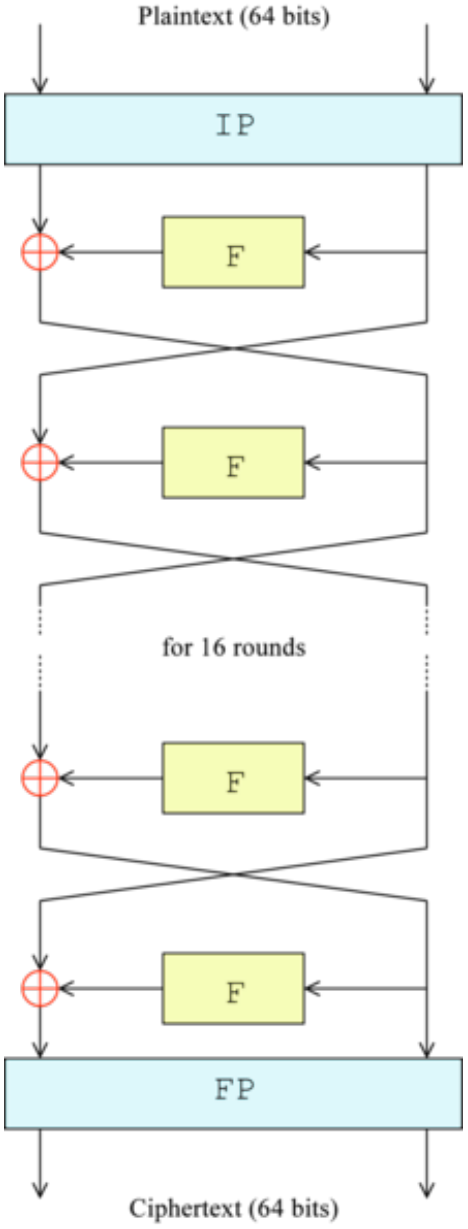
- Block cipher is a family of permutations
  - Indexed by a key (DES = 56 bit key)
  - “Pseudo-random”

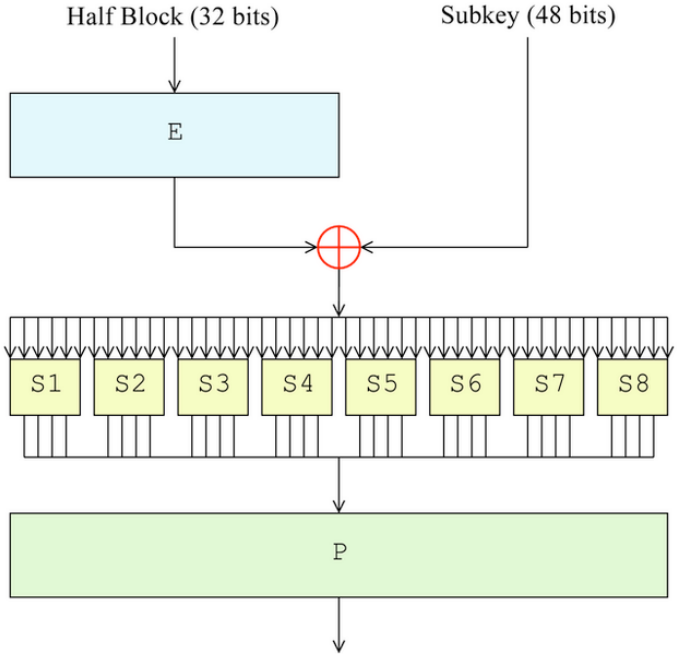
Block Cipher

- Block cipher is a family of permutations
  - Indexed by a key (DES = 56 bit key)
  - Ideally: “Pseudo-random permutation (PRP)”

    (i.e., attacker who does not know the key can’t determine whether you’re using a random permutation, or a PRP)

DES: 64-bit Block, 56-bit Key





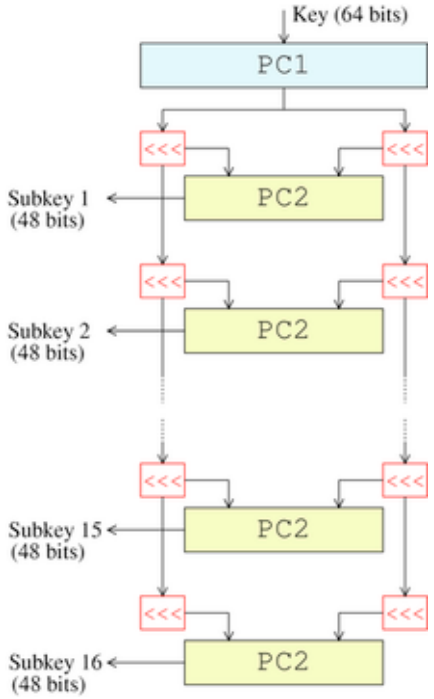
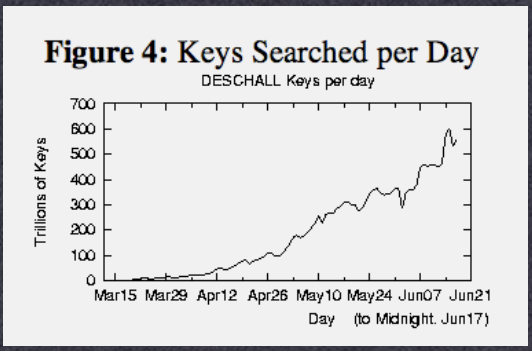
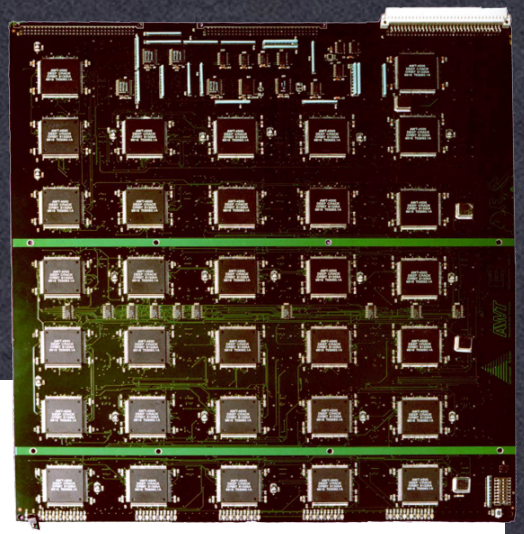


Image from Wikipedia, used under GFDL

DES

- Some “clever” attacks on DES
  - However: practical weakness = 56 bit key size
  - Practical solution: 3DES (now being deprecated)





U.S. Data-Scrambling Code Cracked With Homemade Equipment

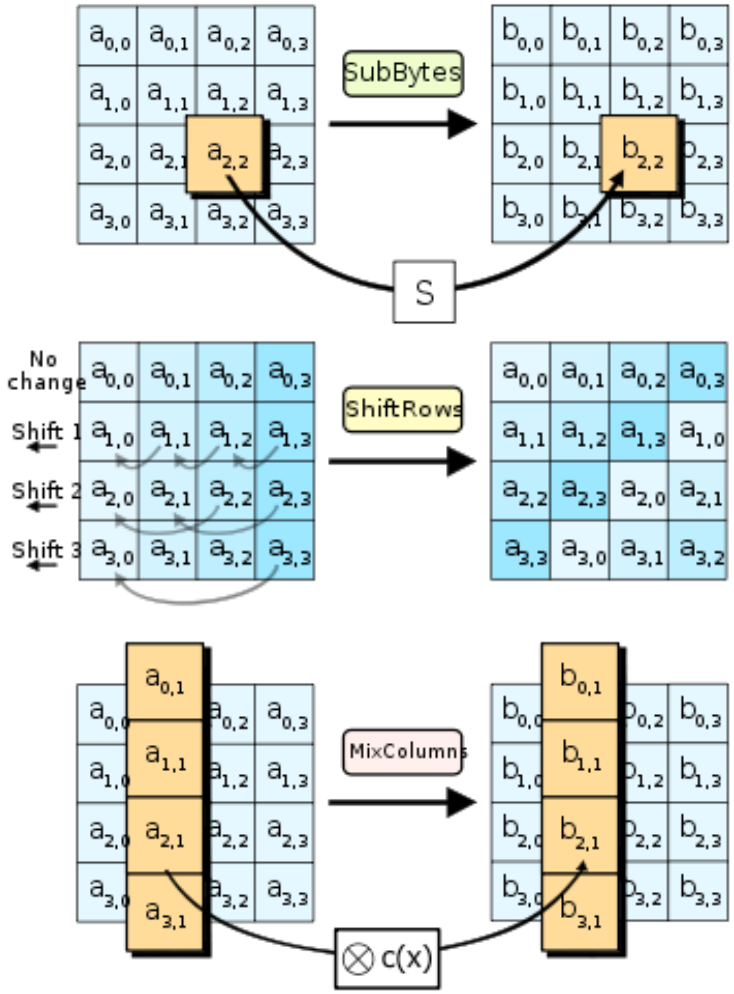
By JOHN MARKOFF

SAN FRANCISCO -- In a 1990s variant of a John Henry-style competition between man and machine, researchers using a homemade supercomputer have cracked the government's standard data-scrambling code in record time -- and have done it by out-calculating a team that had harnessed thousands of computers, including some of the world's most powerful.

AES

- NIST open competition:
  - Fast in software & hardware
  - Larger block size (128 bit)
  - Longer keys (128/192/256-bit)
- 5 finalists:
  - MARS, RC6, Rijndael, Serpent, and Twofish

AES: 128-bit Block, 128/192/256-bit Key



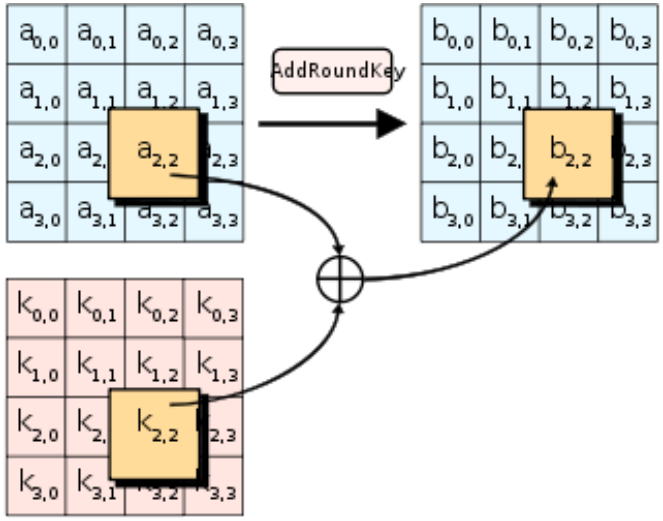


Image from Wikipedia, used under GFDL

Review

- ECB Mode: Encrypt each block separately
  - Problems?