601.445/601.645
Practical Cryptographic Systems

Symmetric Cryptography

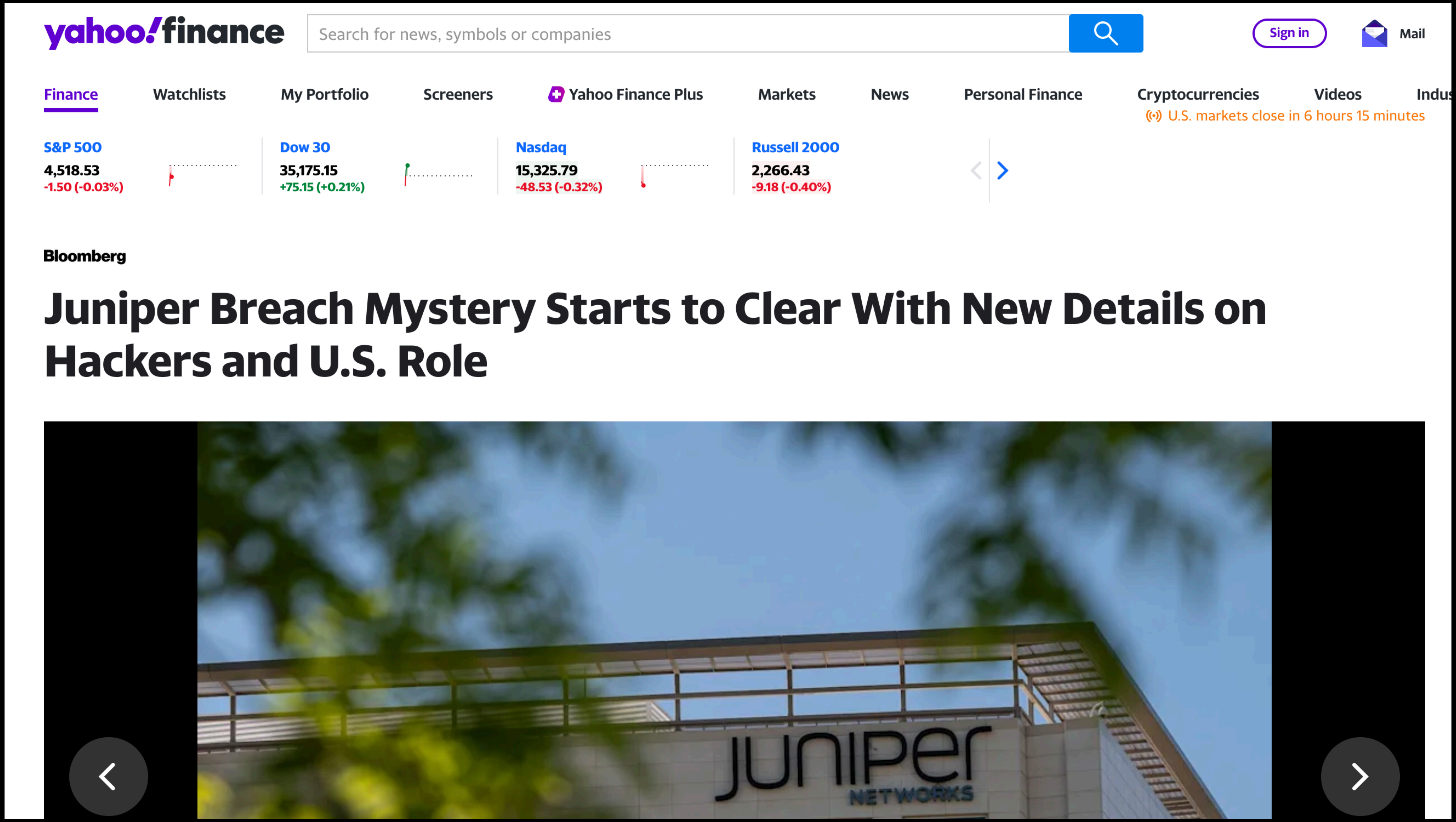
Instructor: Matthew Green

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?

News?


yahoo!finance
Search for news, symbols or companies
Sign in
Mail
Finance
Watchlists
My Portfolio
Screeners
Yahoo Finance Plus
Markets
News
Personal Finance
Cryptocurrencies
Videos
U.S. markets close in 6 hours 15 minutes
S&P 500
4,518.53
-1.50 (-0.03%)
Dow 30
35,175.15
+75.15 (+0.21%)
Nasdaq
15,325.79
-48.53 (-0.32%)
Russell 2000
2,266.43
-9.18 (-0.40%)
Bloomberg
Juniper Breach Mystery Starts to Clear With New Details on Hackers and U.S. Role
JUNIPER
NETWORKS

Security/crypto news

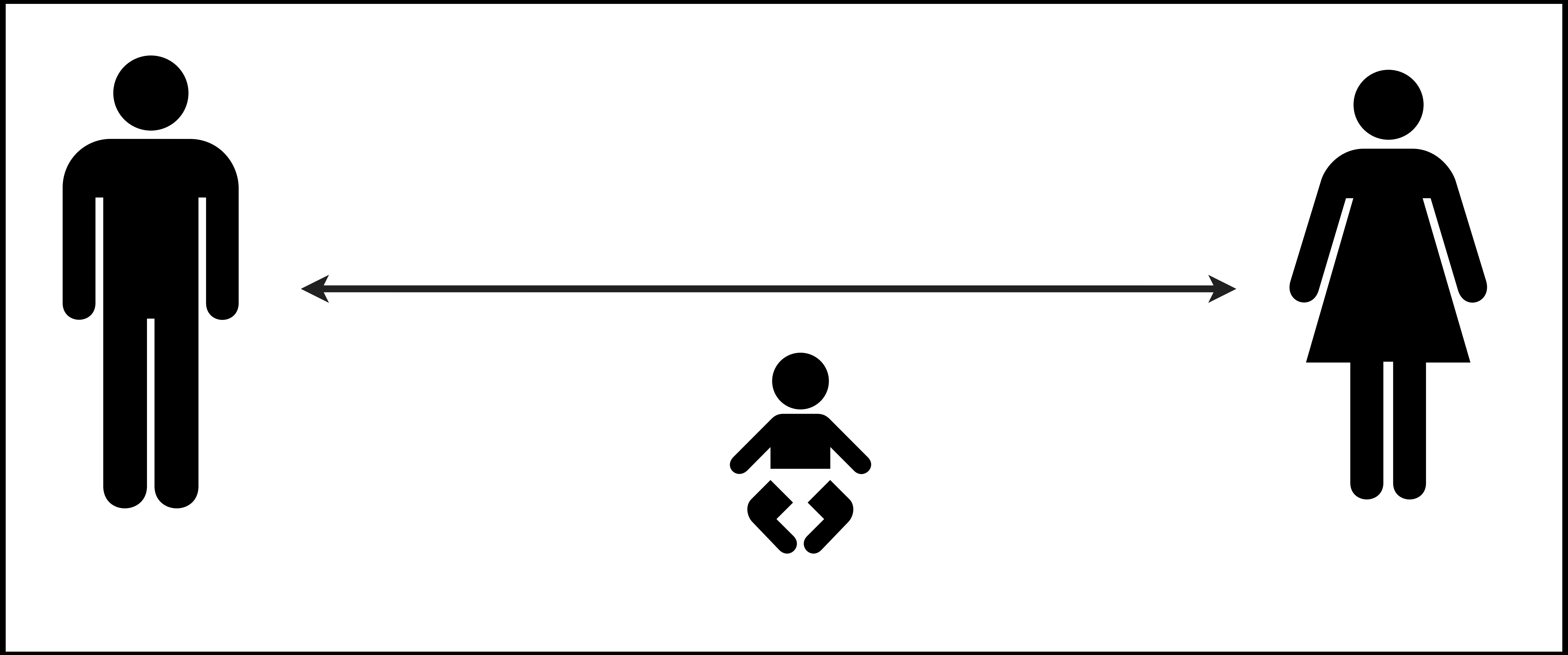
- Hacker news: news.ycombinator.com
- Ars Technica
- Twitter (e.g., here's a list) https://twitter.com/i/lists/953639568816984064?s=20

Review

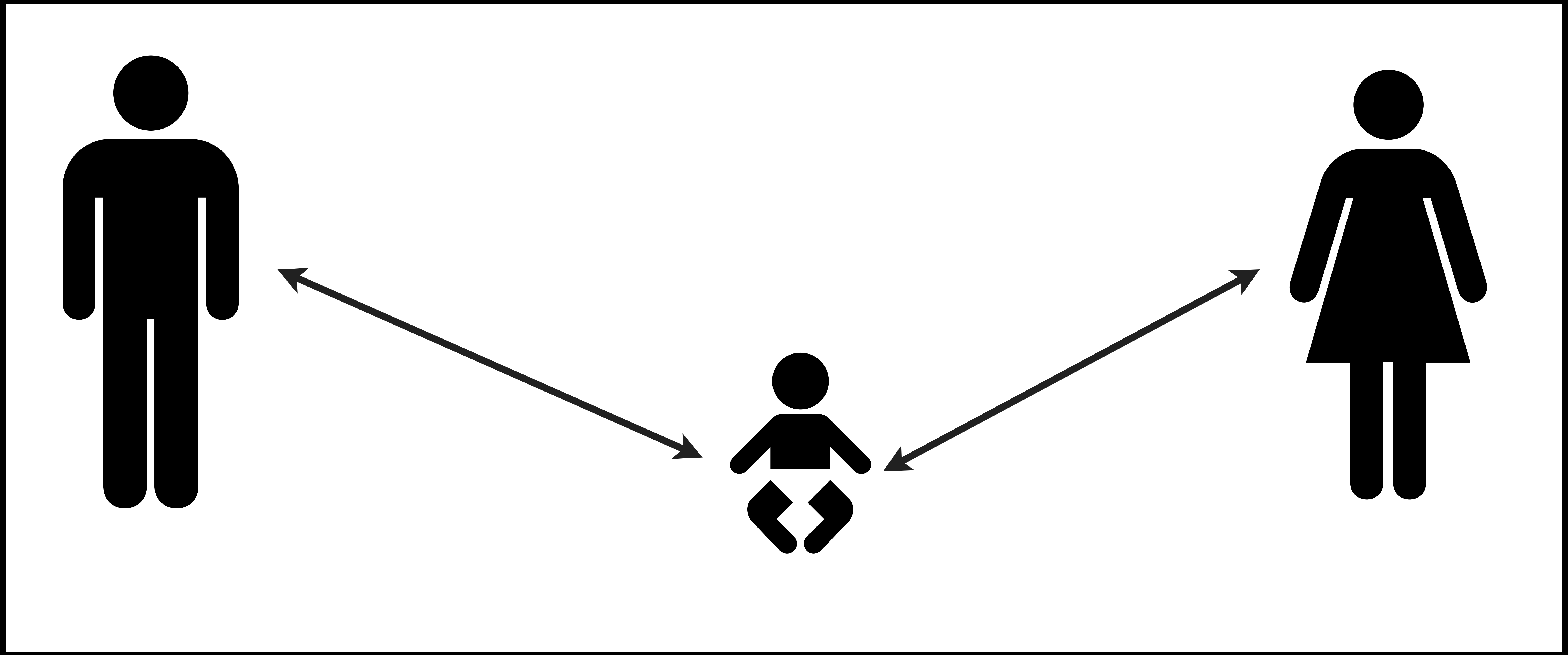
- Last time:
  - A few examples of how systems break
  - Bad primitives, bad protocols, bad implementation
- Today:
  - A (brief) tour through cryptologic history
  - Starting with symmetric (secret-key) crypto

Communication Model

Communication Model



Communication Model



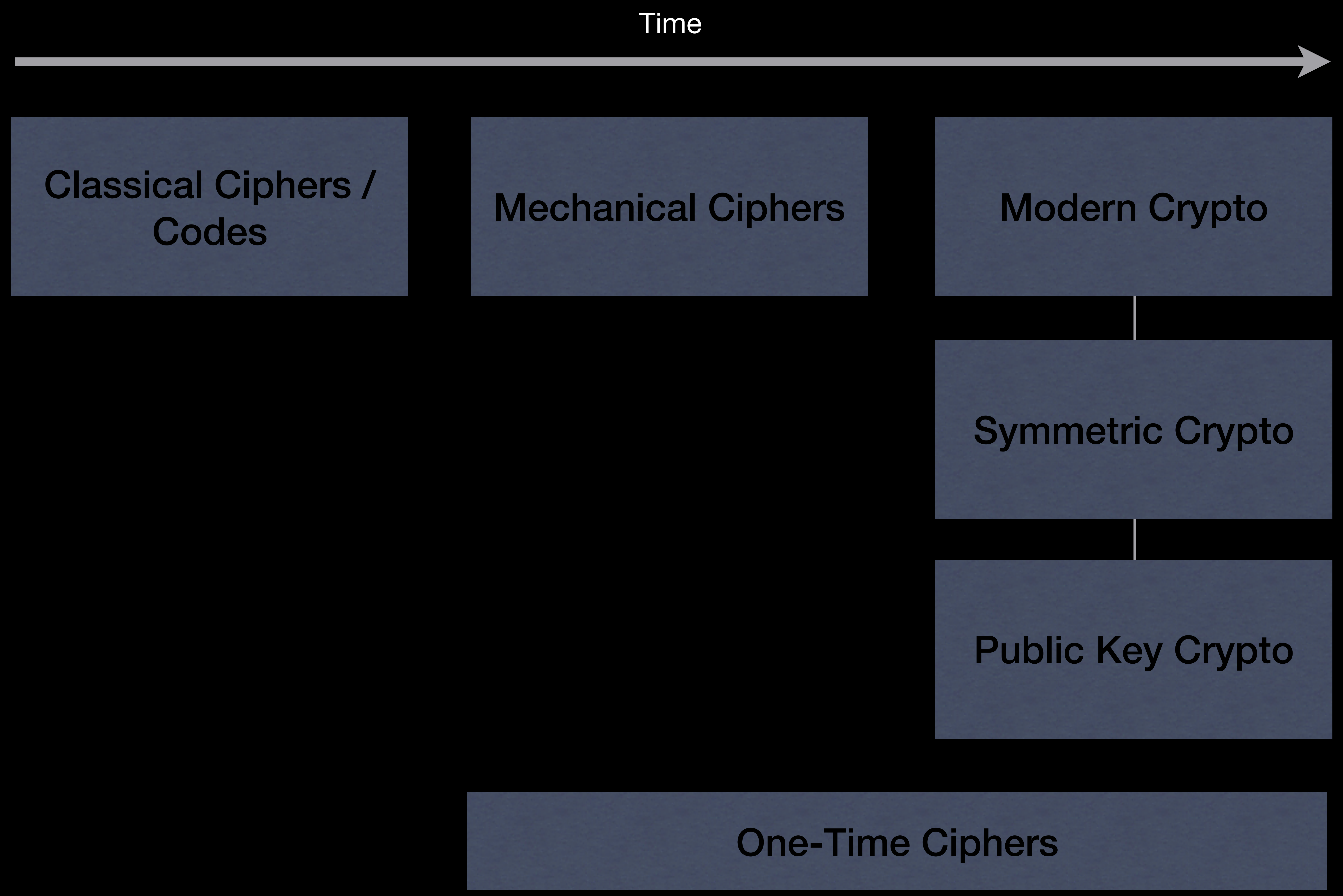
Secure Communication

- Two basic properties we like to achieve:
  - Data <u>confidentiality</u>
  - Data <u>authenticity</u> (“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

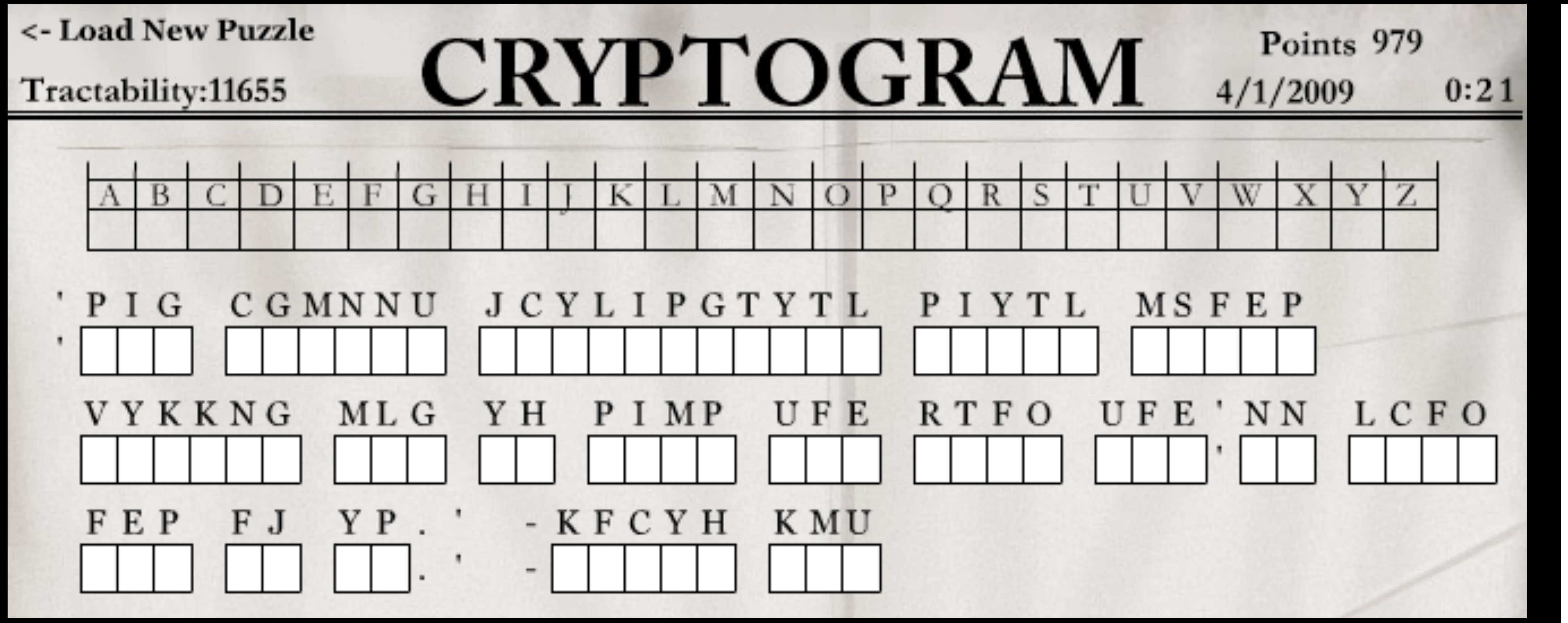
History of Encryption

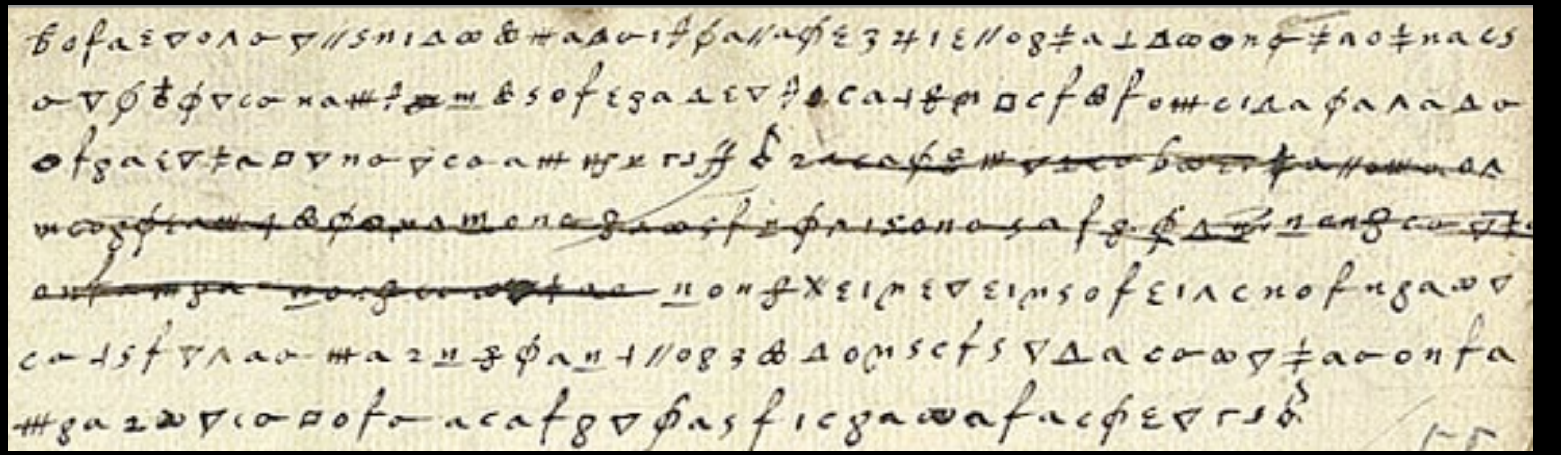


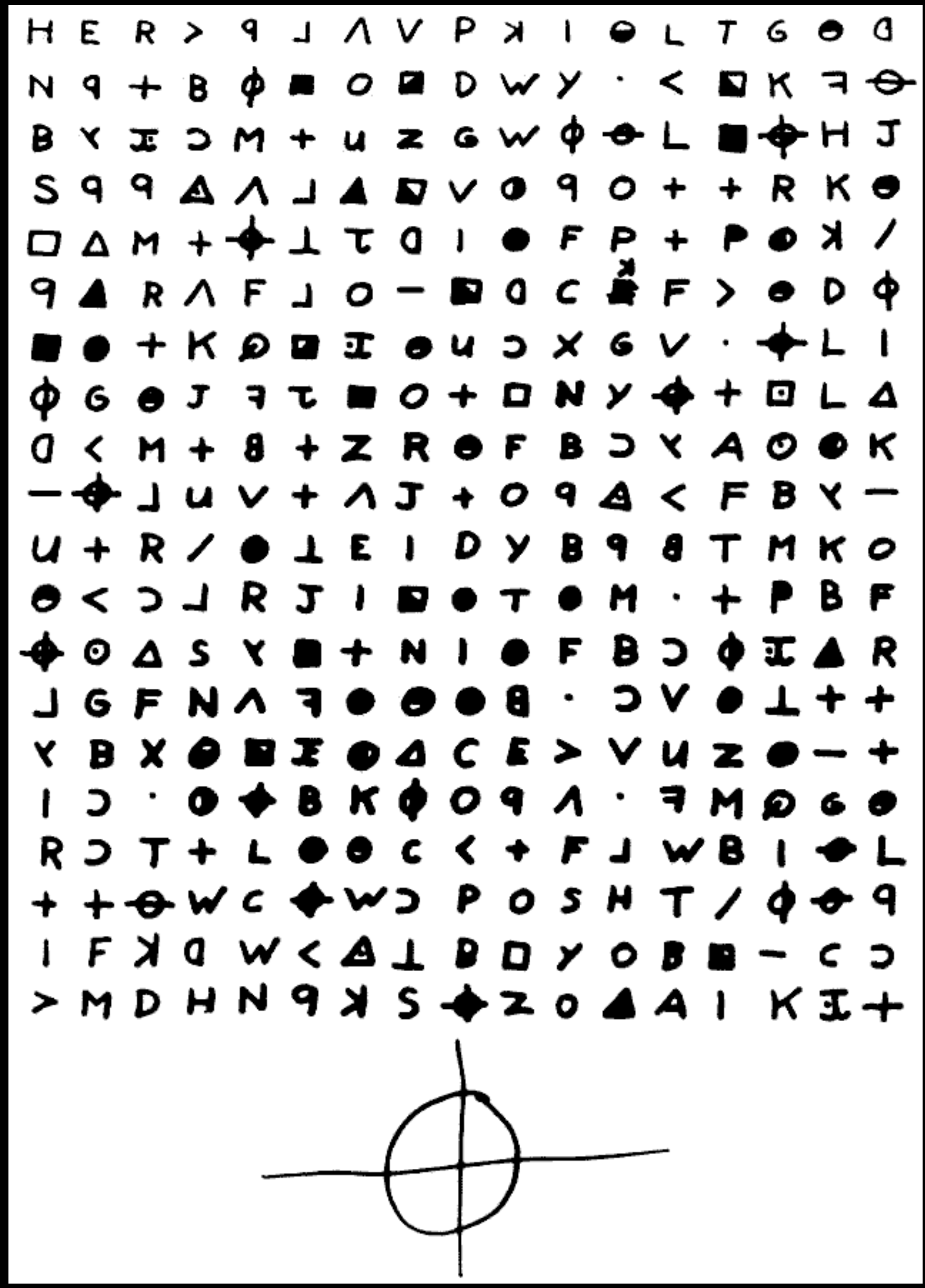
Classical Cryptography

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

Increasing
Complexity







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

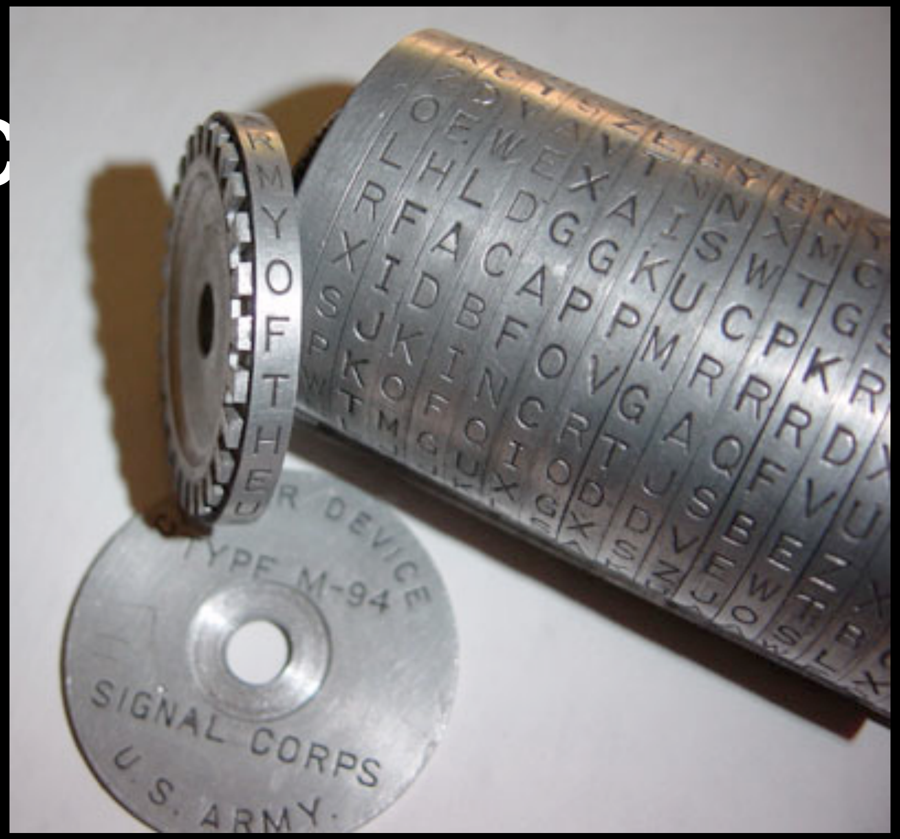
- 1900s
    - Vernam & Mauborgne's "Unbreakable" cipher
- Based on Baudot code for Teletypes
- Added (XORed) a random Key (sequence of bits) to a binary message
    - Perfectly secure, provided:
- key is perfectly random
- key is <u>at least as long</u> as the message
- key is never re-used

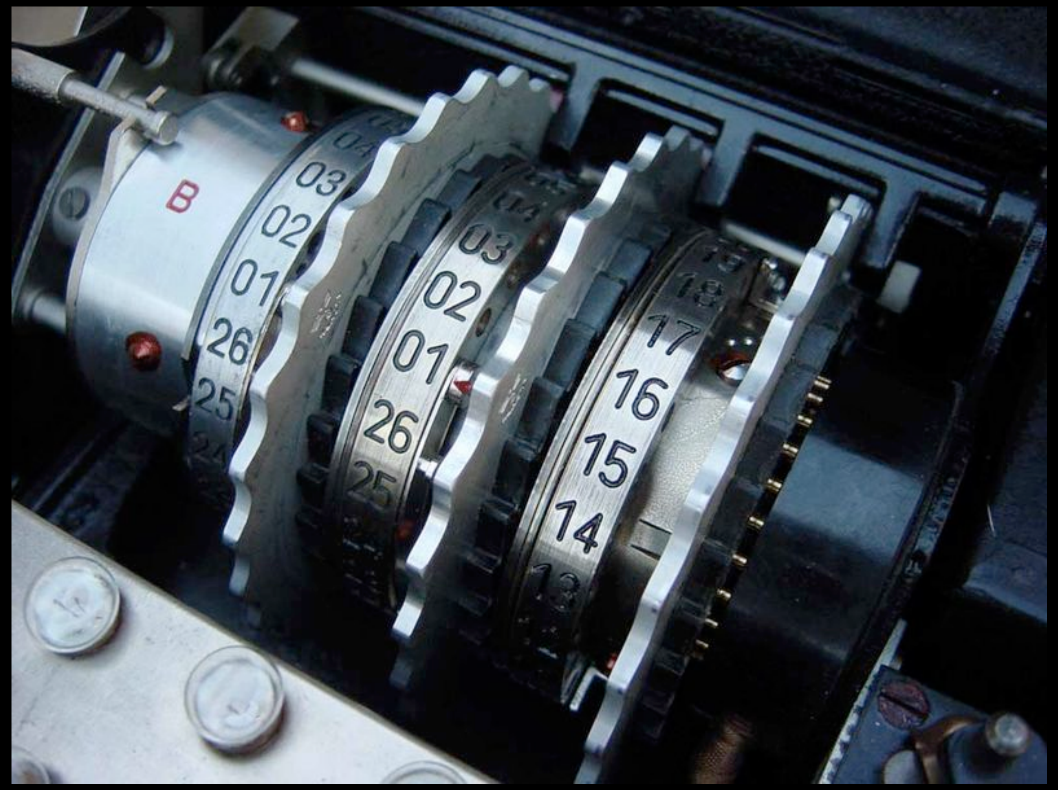
Image by Flickr user "spratmackrel" used under a Creative Commons license.

Mechanical Cryptography

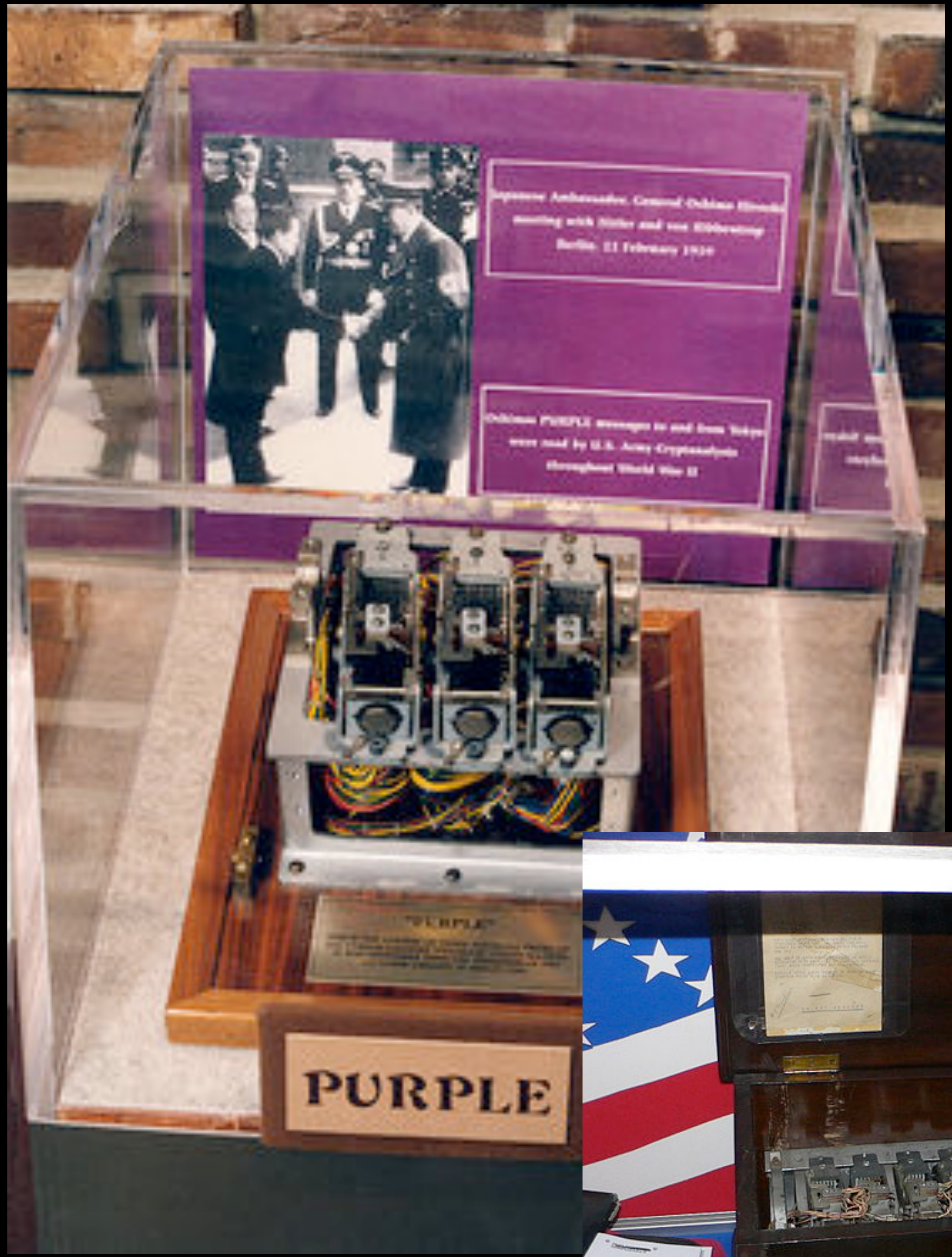
- 1900s
  - Mass production and usage of cipher devices
  - Rotor ciphers
  - Elec

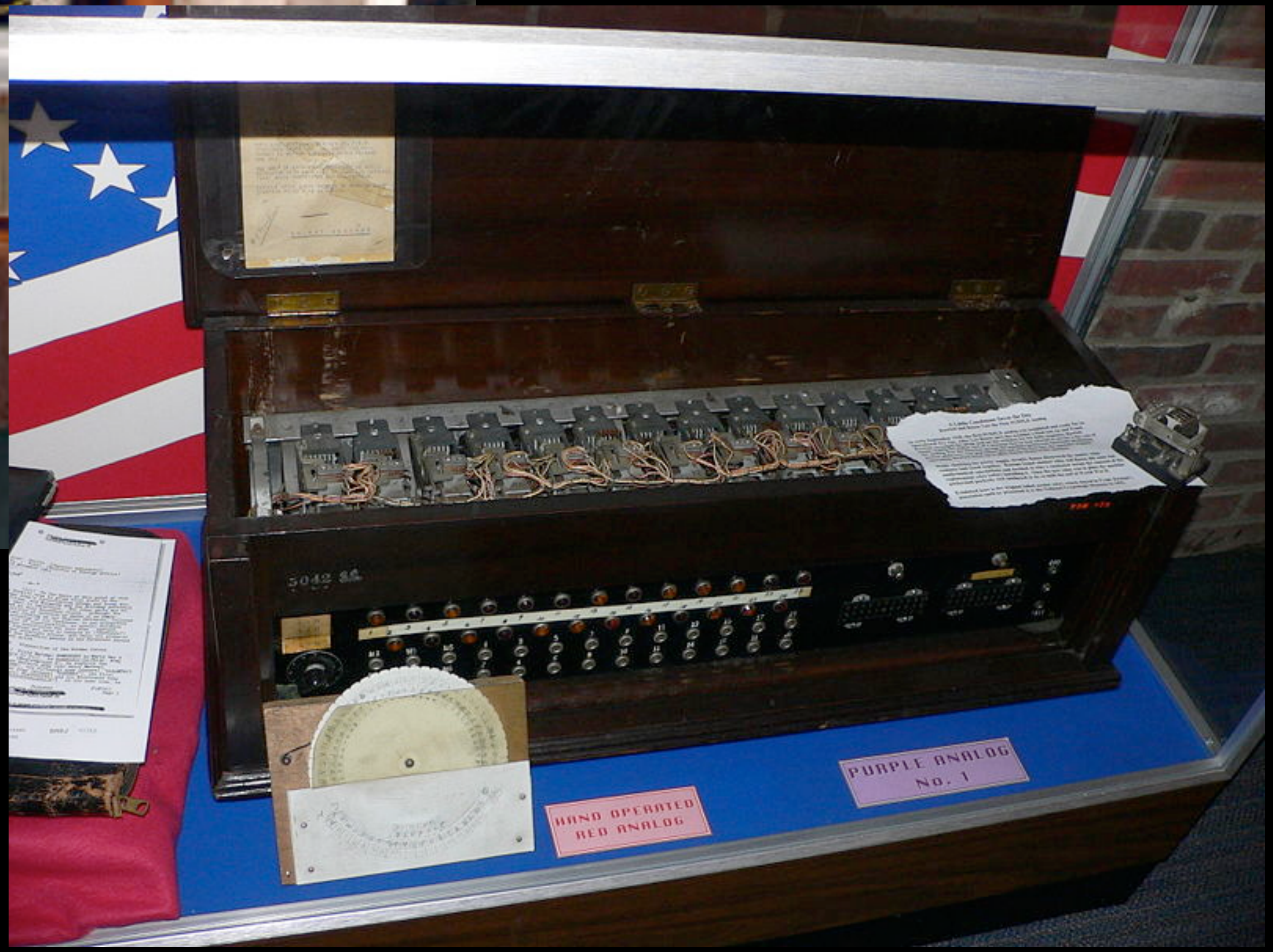
Increasing Complexity

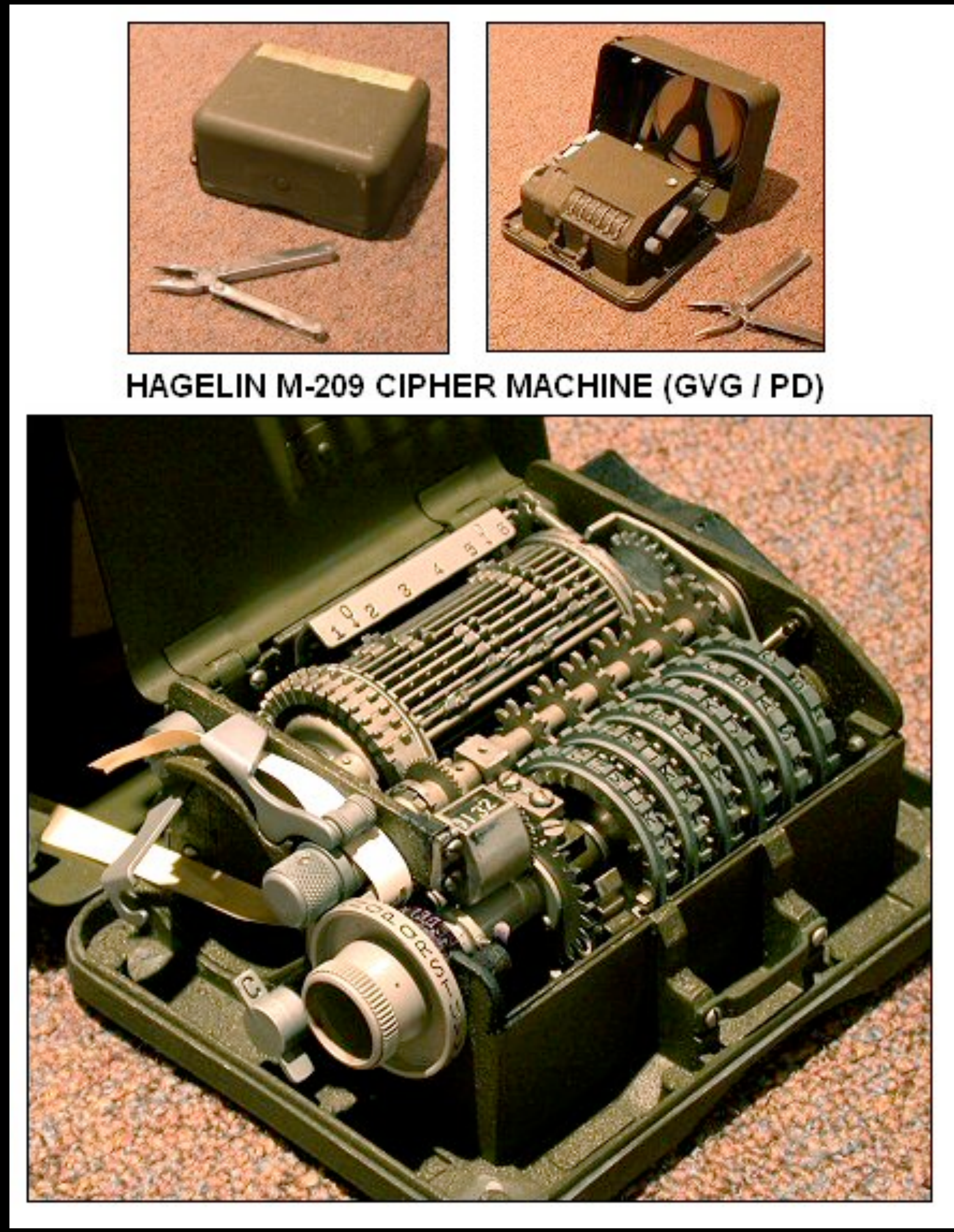




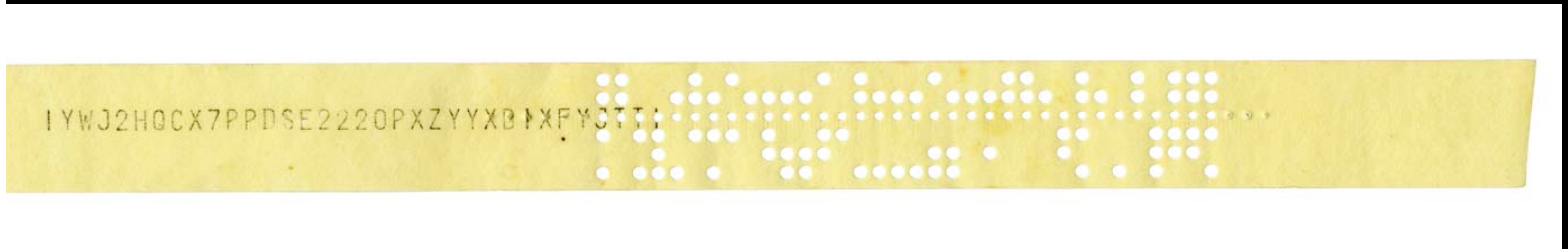
M-94 Cipher Wheel image by Bob Lord, used under a Creative Commons license.
Remaining images: Wikipedia [M-94, Enigma] used under GFDL.







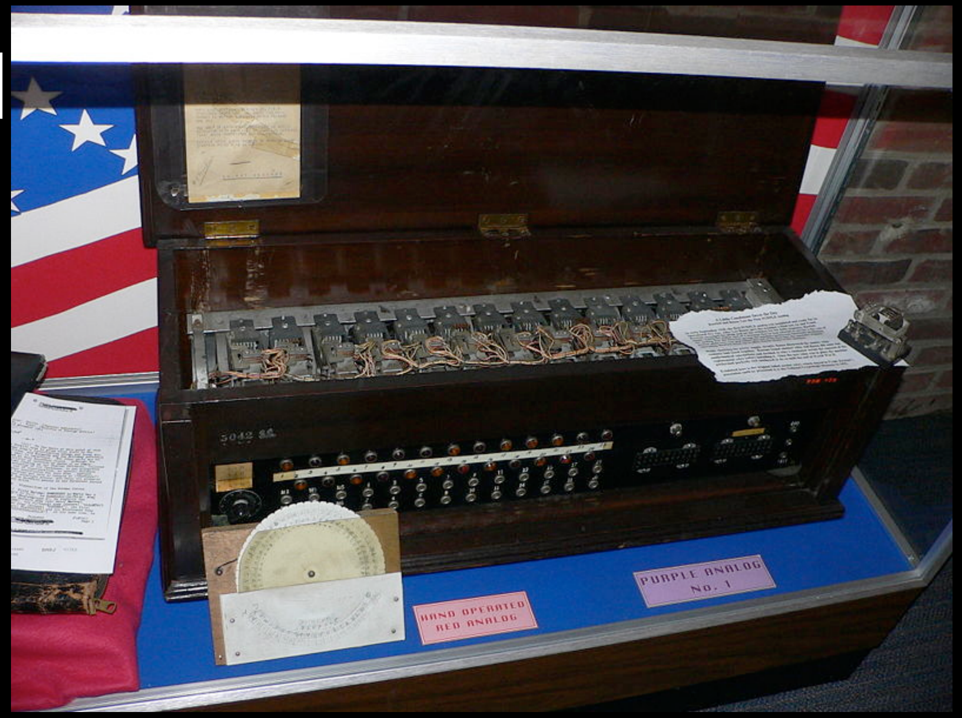
Purple Machine (top left) courtesy NSA, US Purple Replica (center) & M-209 images: Wikipedia used under GFDL/CC License.

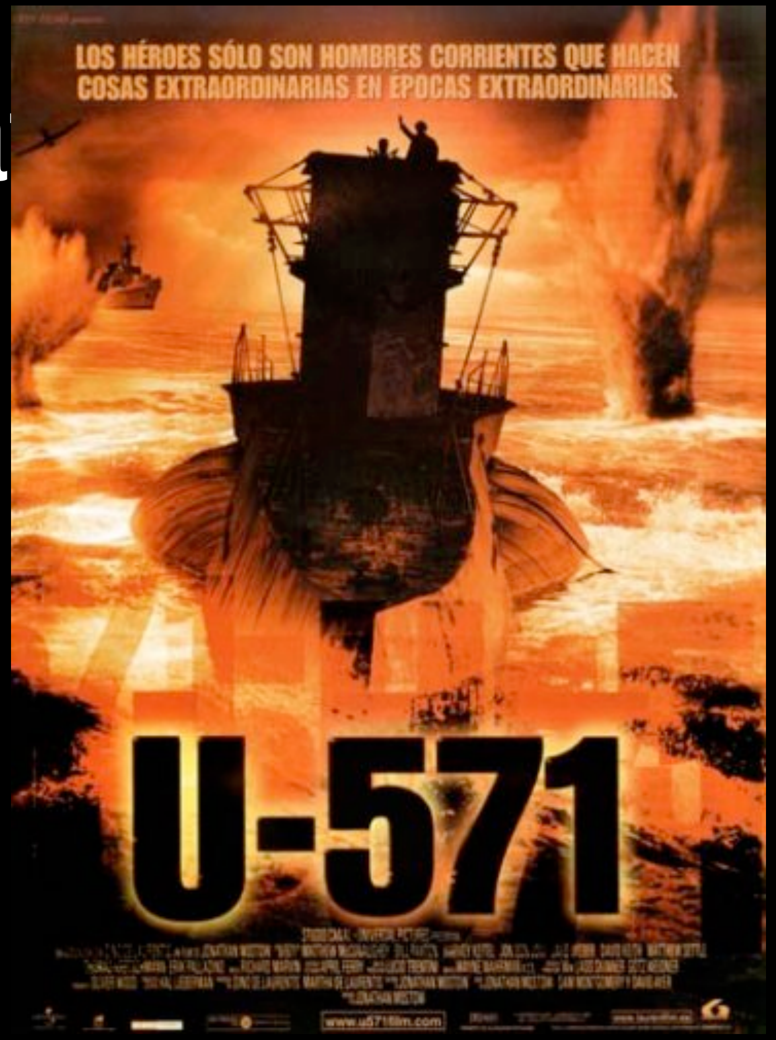


Russian Fialka device and tape by Bob Lord, used under a Creative Commons license.
HC-9 Image: Wikipedia, used under GFDL.

Summary

- Most cryptosystems ultimately broken
  - Sophistication of the attackers outpaces that of the cryptosystem
  - Security relies on <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;

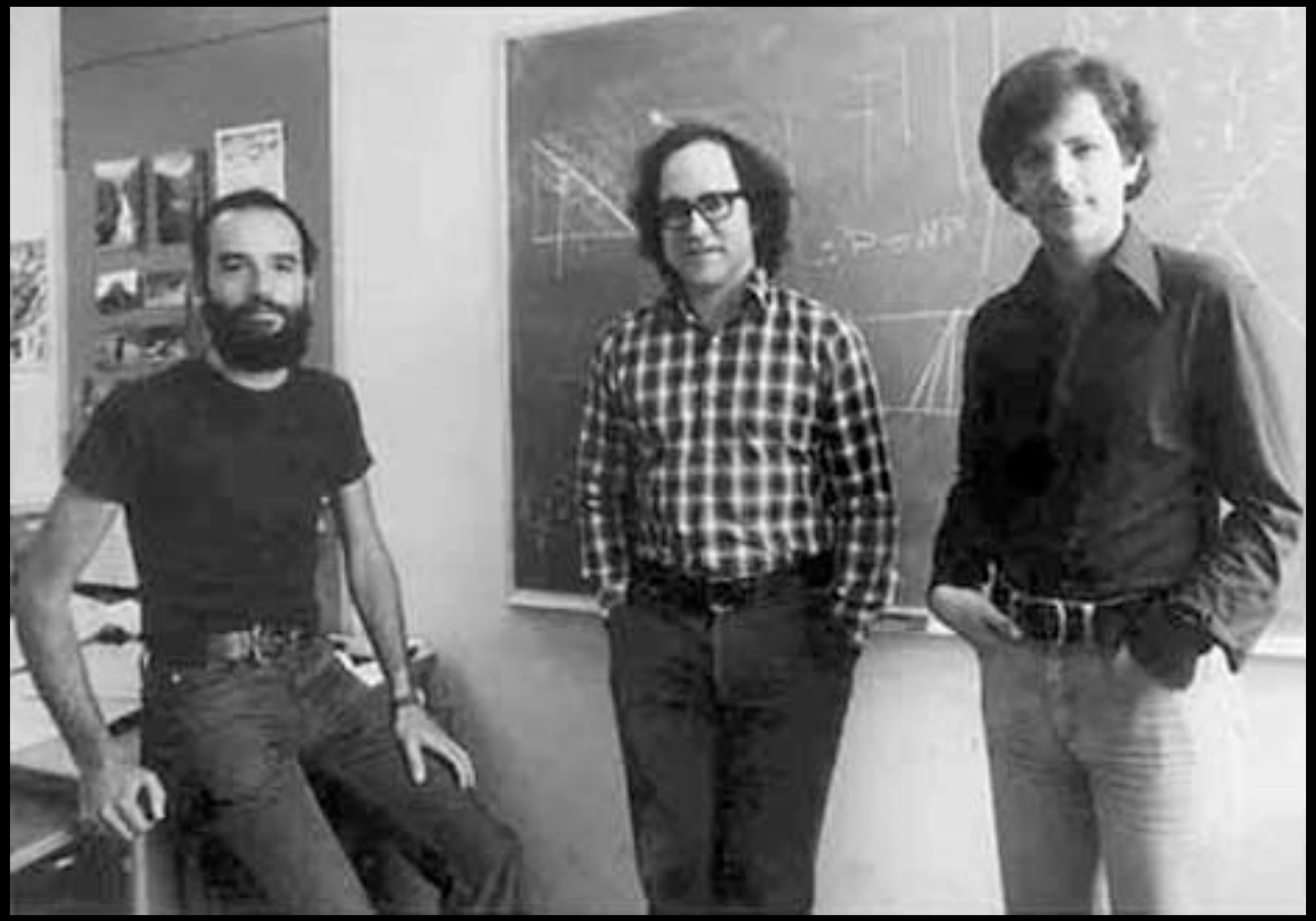
“The enemy knows the System”
-- Claude Shannon’s Maxim

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)



1977
(1973)

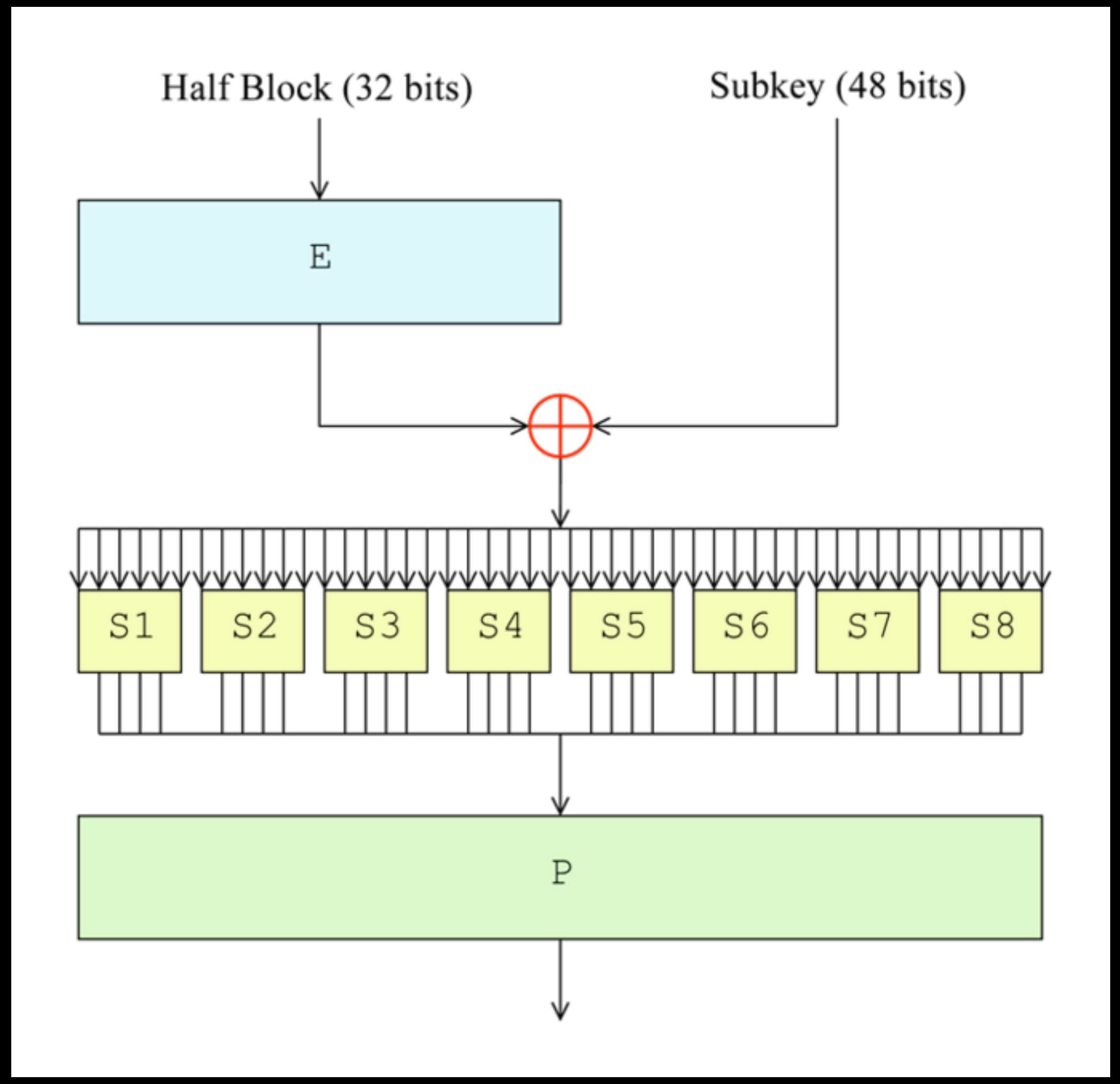
U.K. GCHQ

The Implications

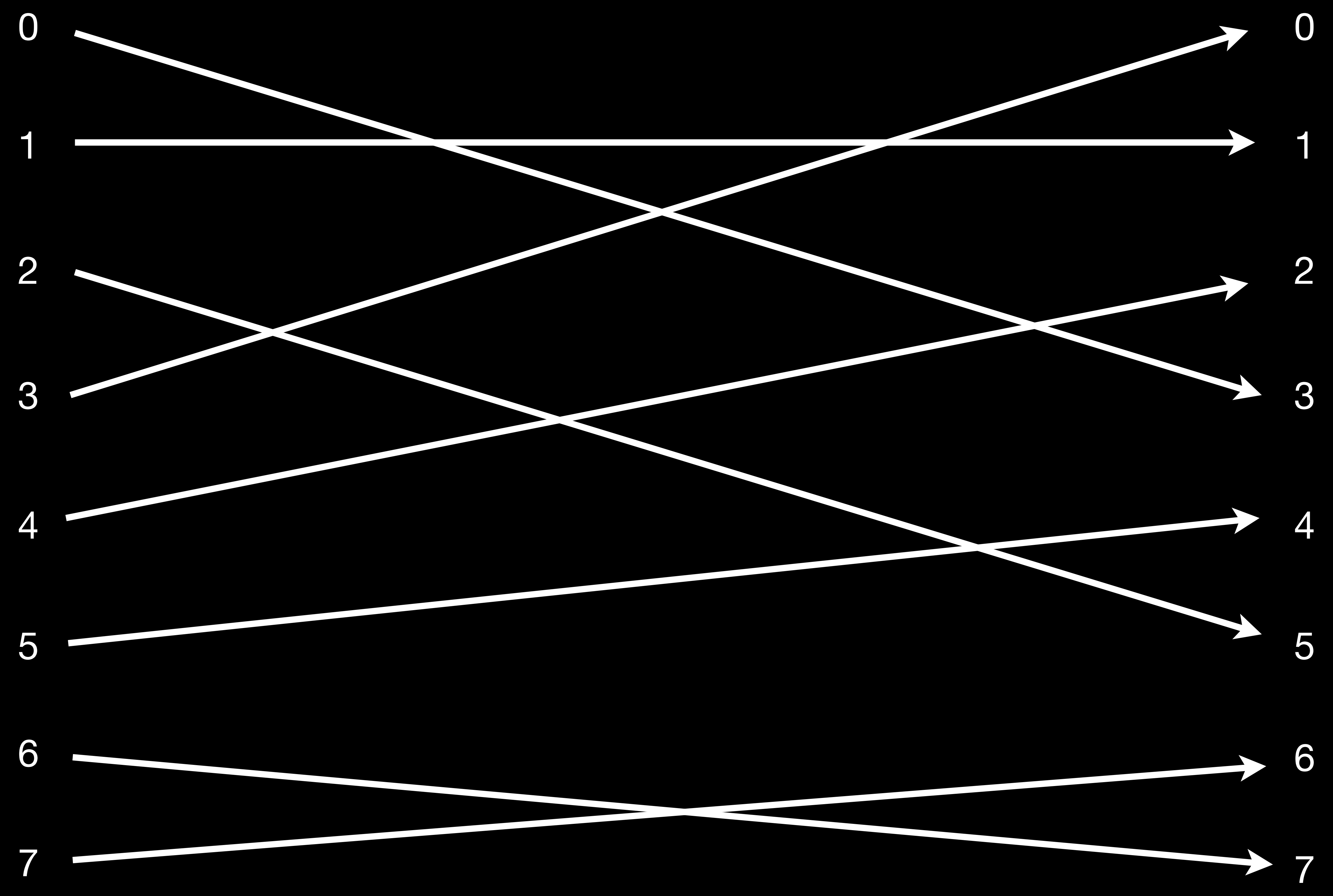
- Exponential increase in study & usage of cryptography in industry, academia
- Wide-scale deployment of cryptographic systems
- <u>Provable Security</u>
    - Cryptographic Systems can be <u>reduced</u> to some hard mathematical problem

Data Encryption Standard

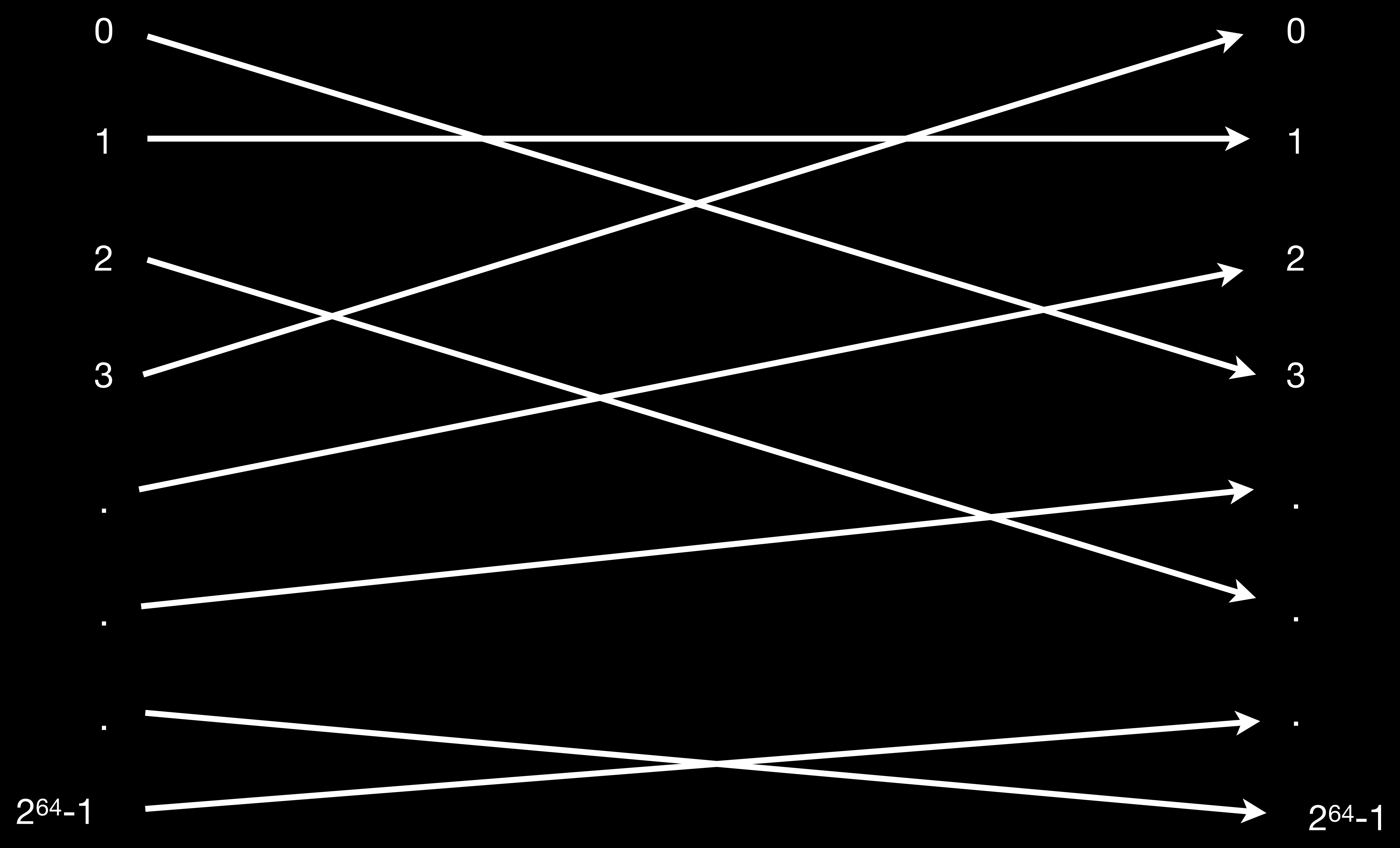
- Commercial-grade Block Cipher
  - 64-bit block size
  - 56 bit key (+ 8 bits parity)
  - “Feistel Network” Construction



Permutation



Permutation



Permutation Families

- Can't have just <u>one</u> 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 <u>random</u> permutation, or a PRP)

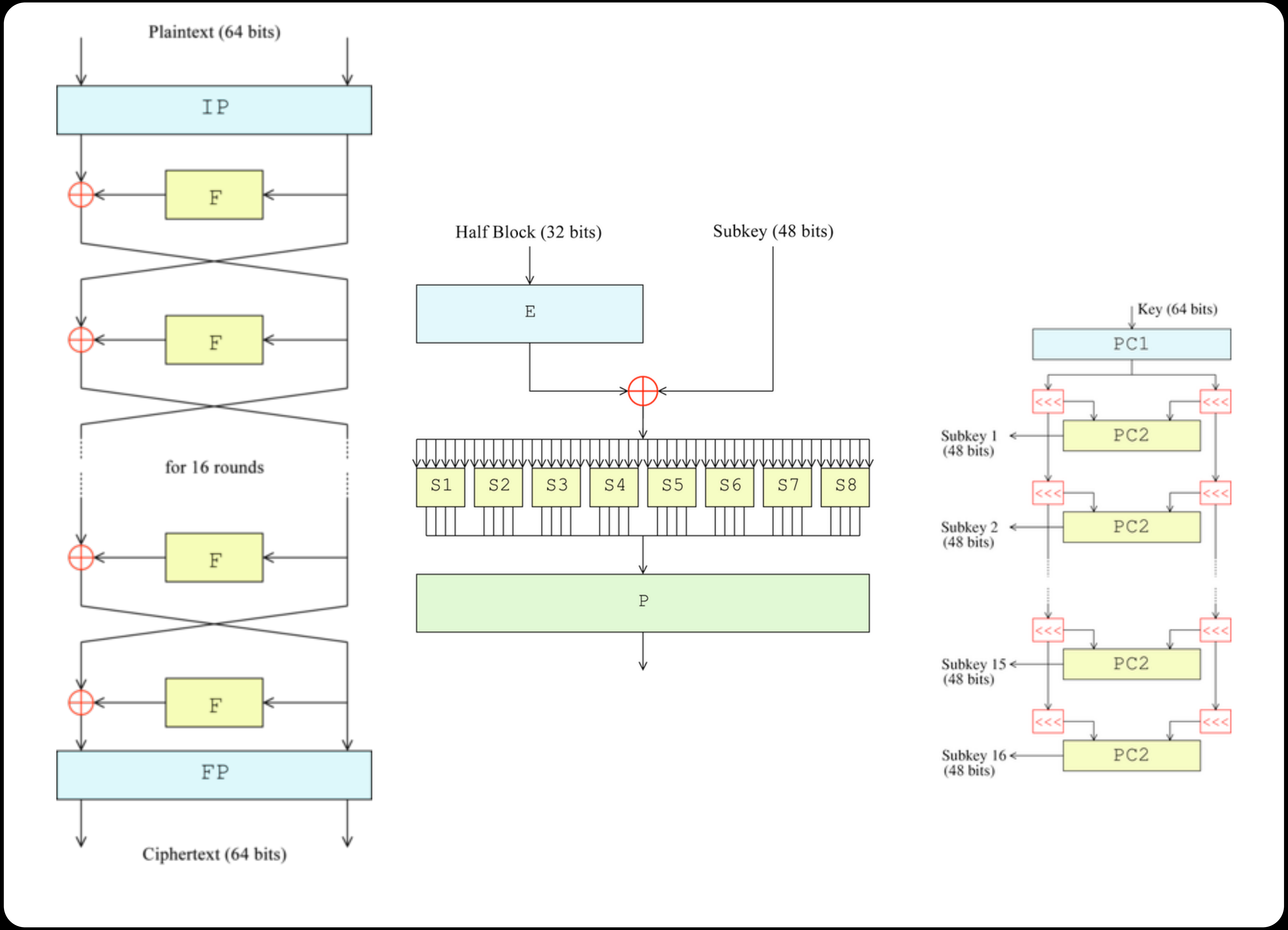
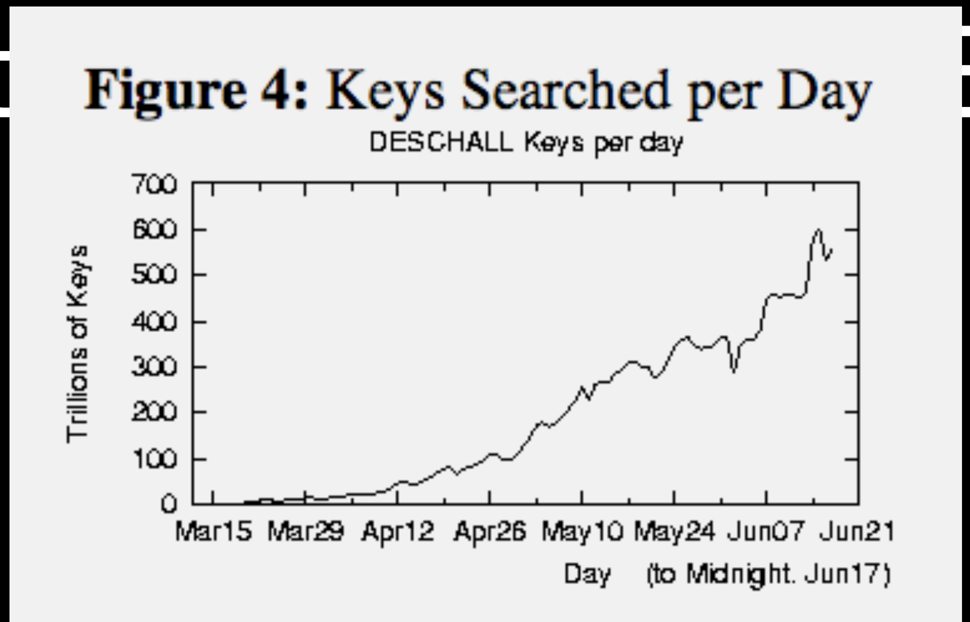
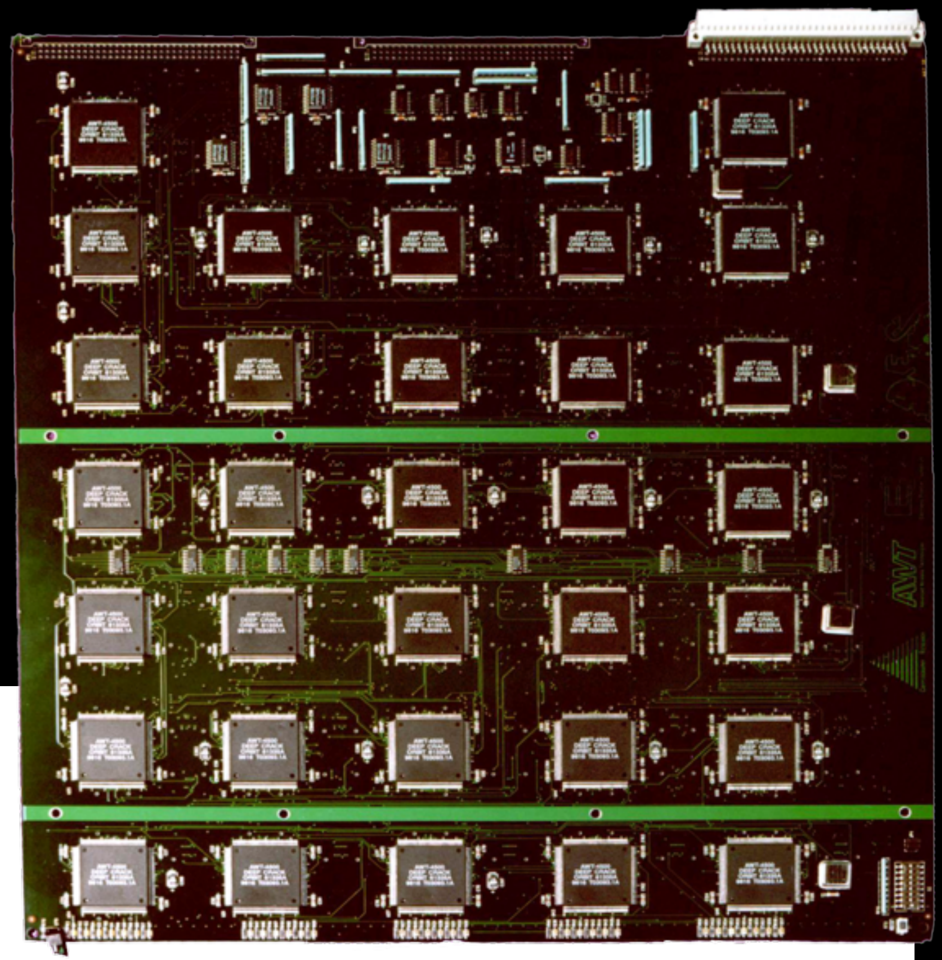


Image from Wikipedia, used under GFDL

DES

- Some “clever” attacks on DES
  - However: practical weakness = 56 bit key size
  - Pract ES (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 (200s):
  - Fast in software & hardware
  - Larger block size (128 bit)
  - Longer keys (128/192/256-bit)
- 5 finalists:
  - MARS, RC6, Rijndael, Serpent, and Twofish

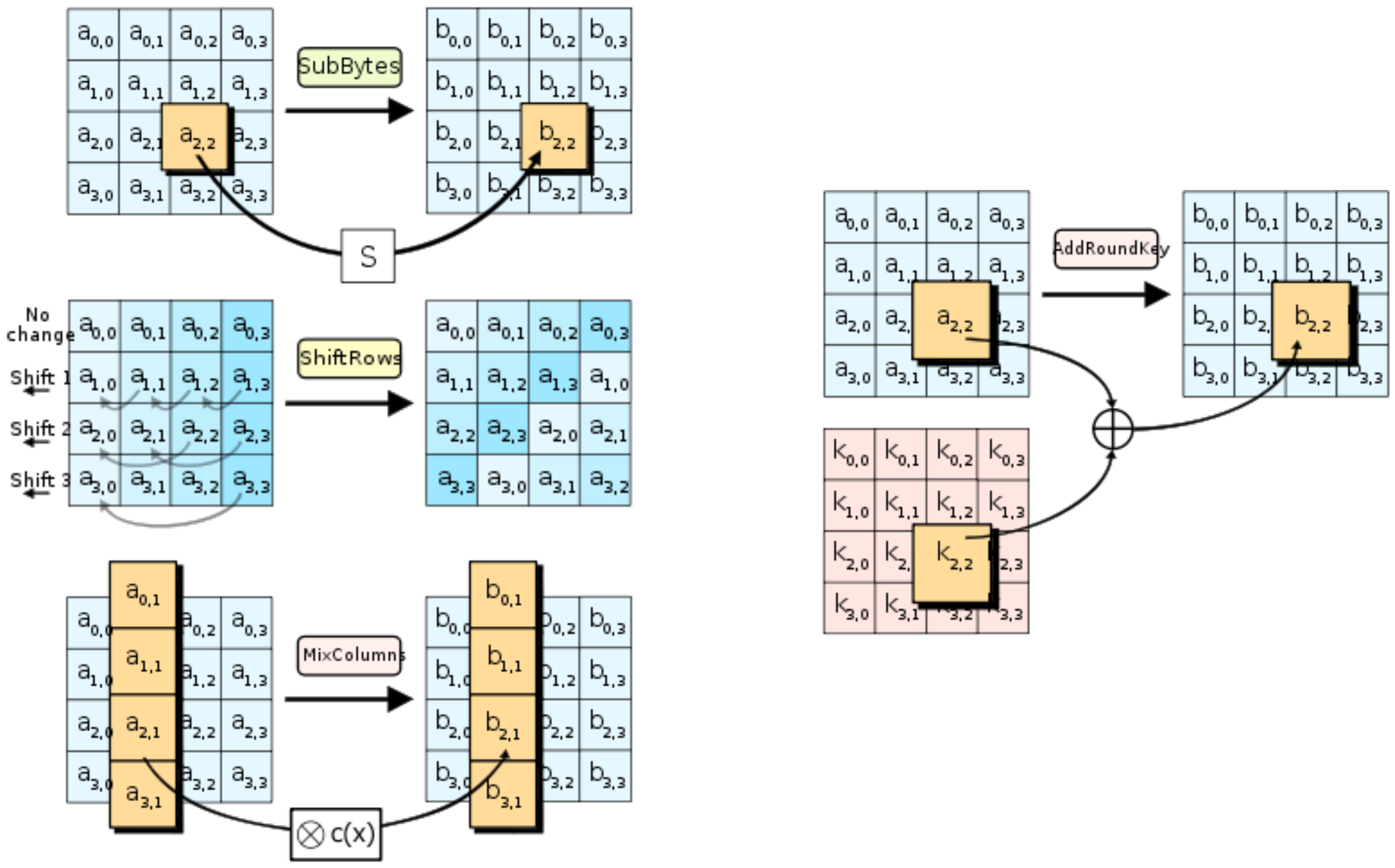
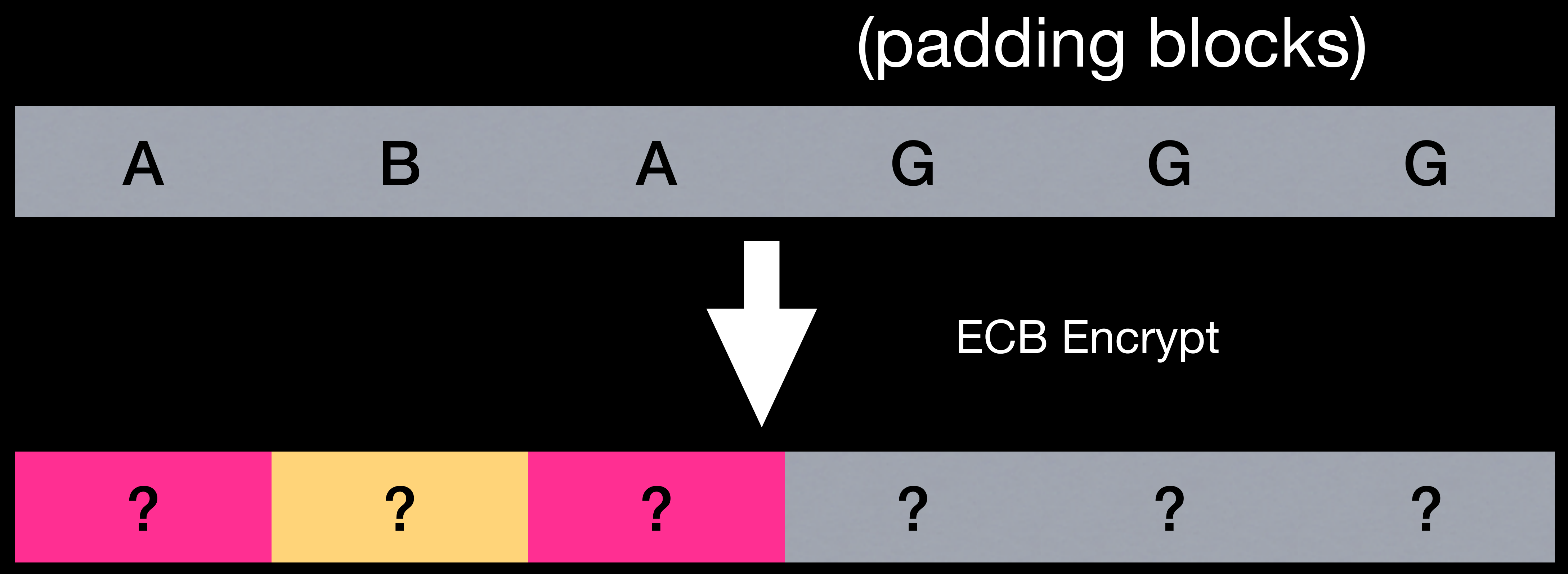
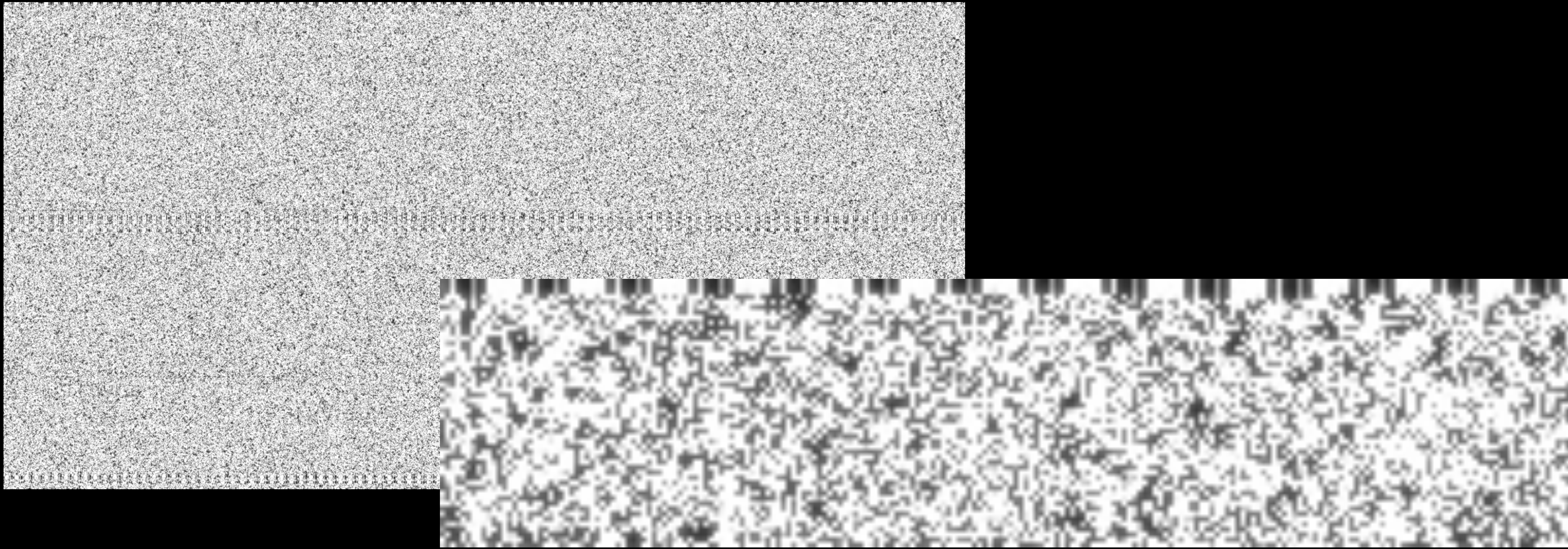


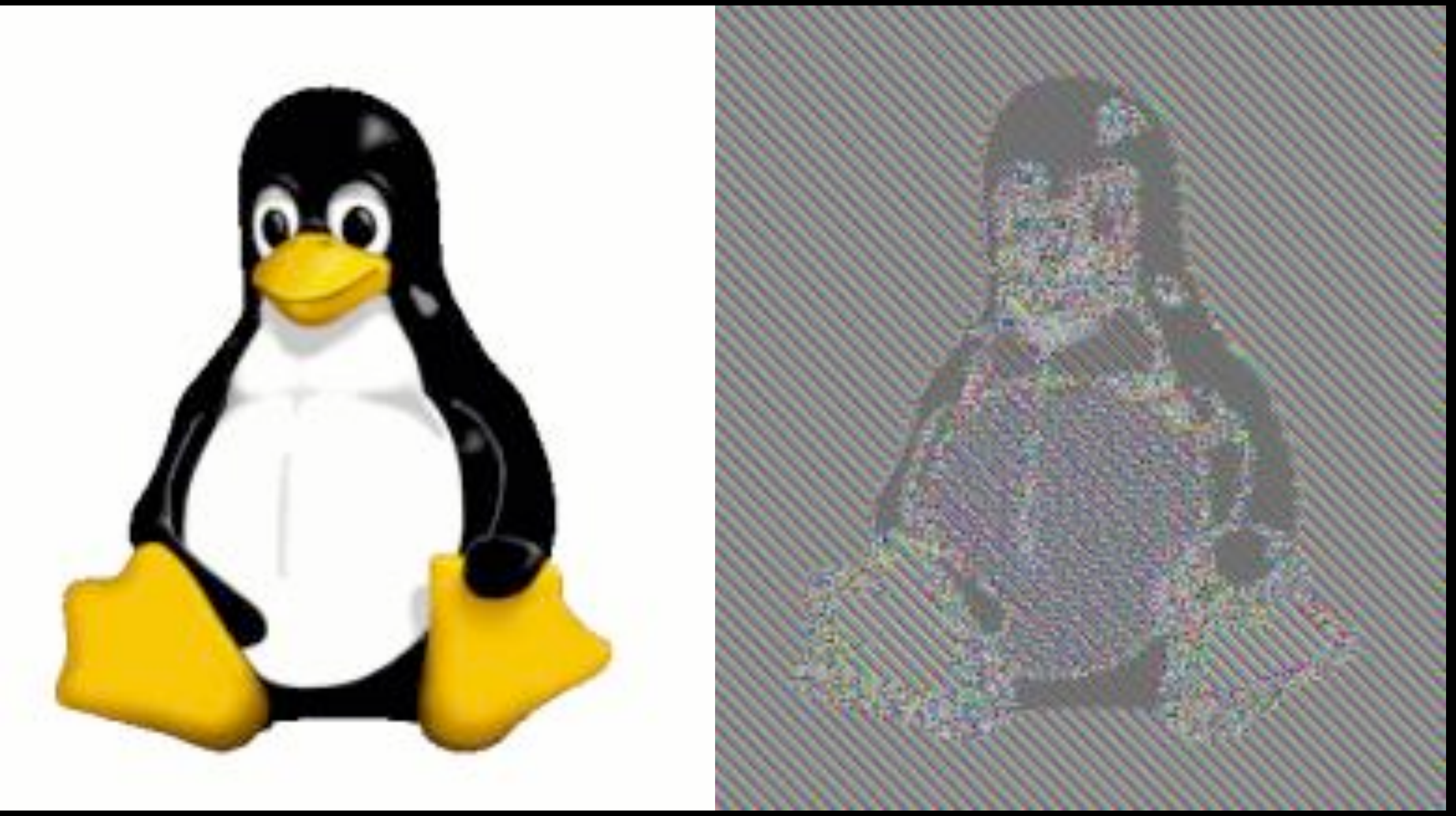
Image from Wikipedia, used under GFDL

How to use a block cipher?

- ECB Mode: Encrypt each block separately
  - Problems?







ECB Mode

- ECB is deterministic
  - Leads to problems, e.g.,:

Game server

Game client

Definitions

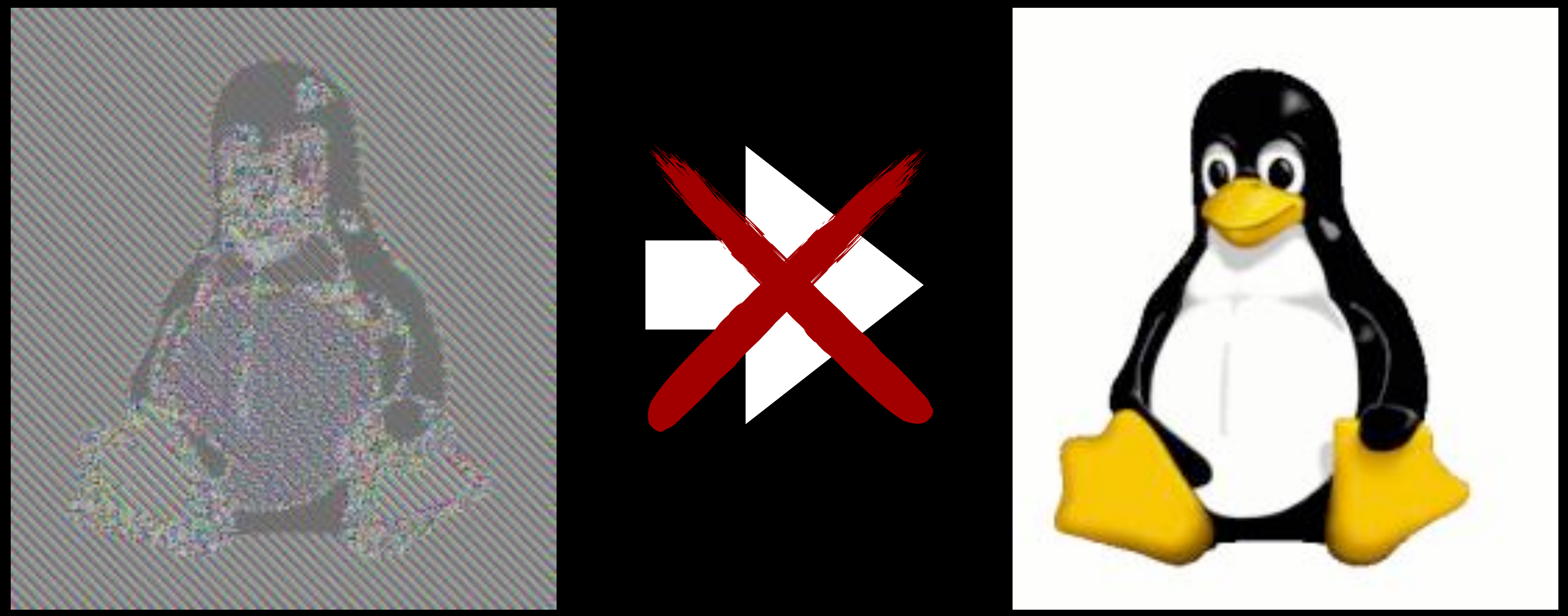
- What does it mean to securely encrypt something?

Historical attempts

- Given a ciphertext, can’t recover the plaintext

Historical attempts

- Given a ciphertext, can’t recover the plaintext



Security of Encryption

- Semantic Security
  - Due to Goldwasser & Micali (1980s)
  - Informally: An encryption scheme is secure if <u>adversary who sees ciphertext</u> “learns as much” as <u>adversary who doesn’t see ciphertext.</u>
- Even if adversary can request chosen plaintexts
  - How do we state this formally?

Semantic security

- Semantic Security (IND-CPA)

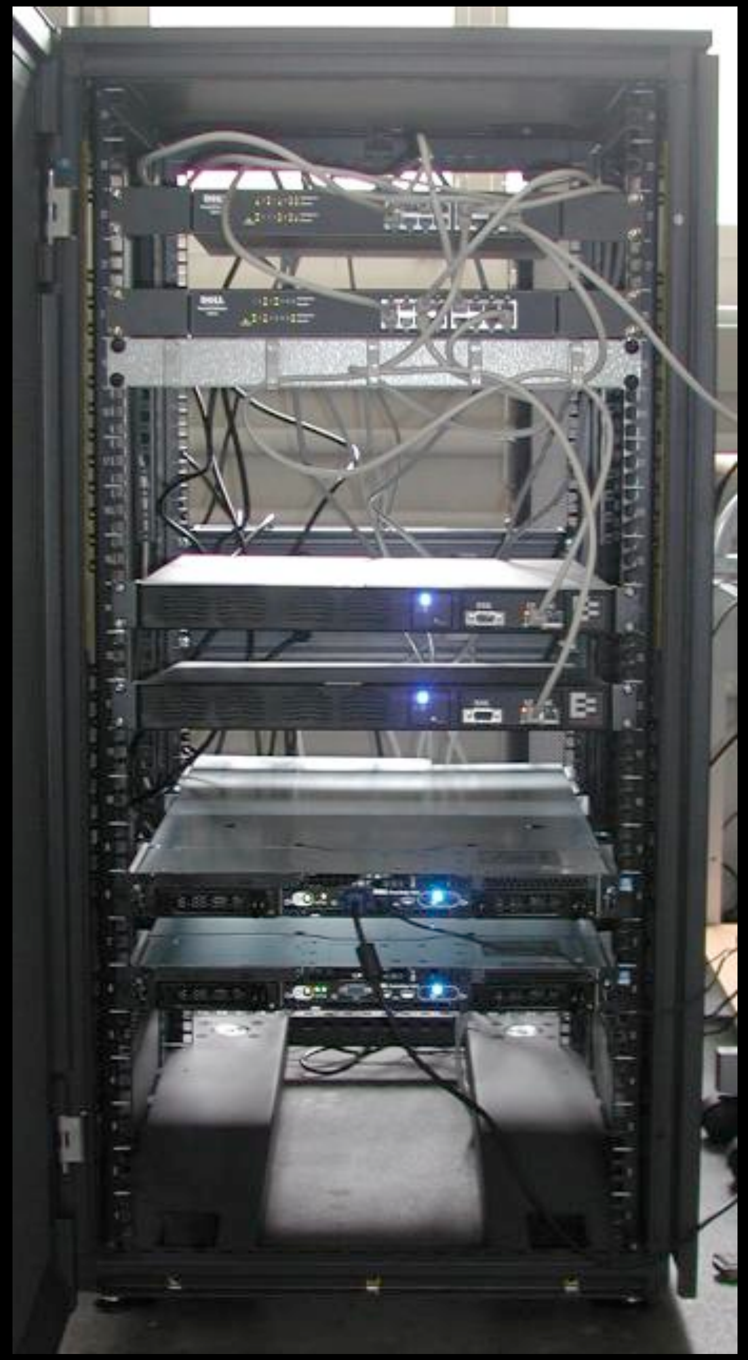
$$b \xleftarrow{\$} \{0, 1\}$$

$|M_0| = |M_1|$

Adversary

M_0, M_1 →

$E(M_b)$ ←



k

b?

Semantic security

- Semantic Security (IND-CPA)

$$b \xleftarrow{\$} \{0, 1\}$$

Adversary

$M_1, ..., M_n$ →

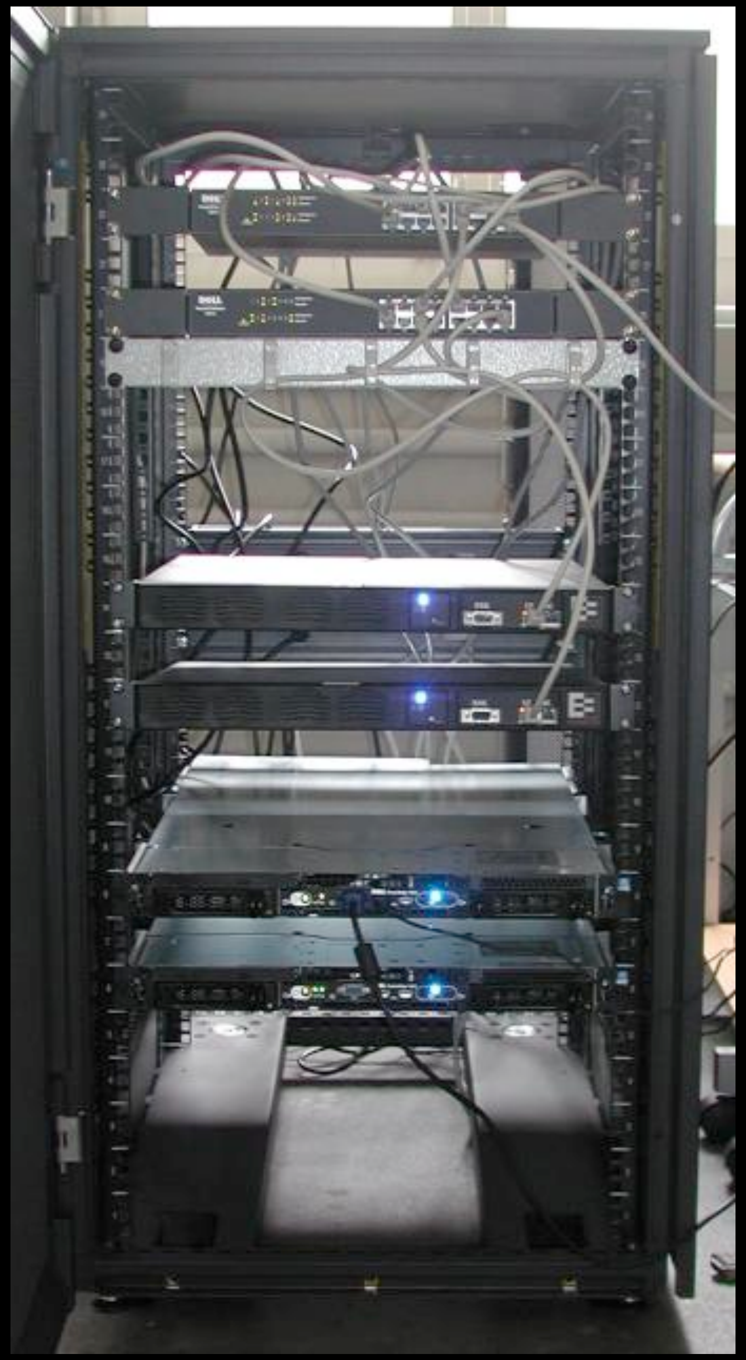
$E(k, M_1), ..., E(k, M_n)$ ←

M_0, M_1 →

$E(M_b)$ ←

$M_1, ..., M_n$ →

$E(k, M_1), ..., E(k, M_n)$ ←



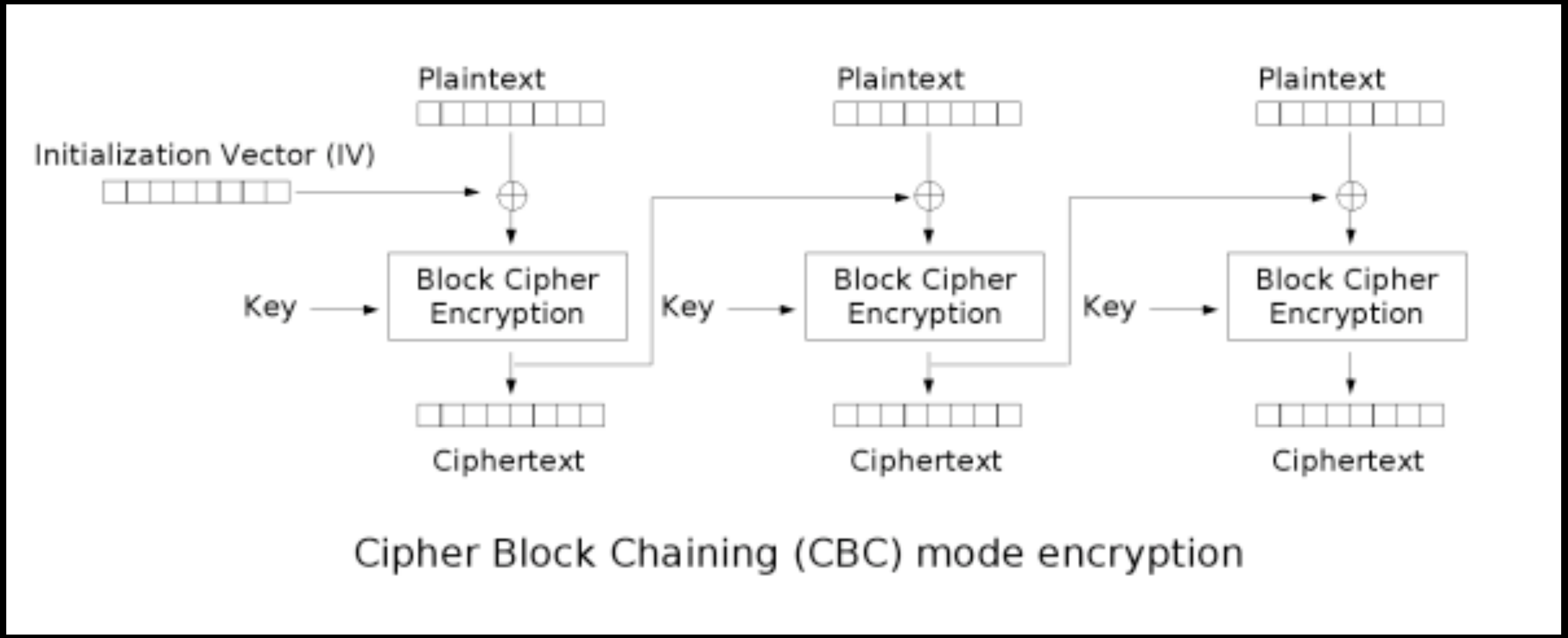
k

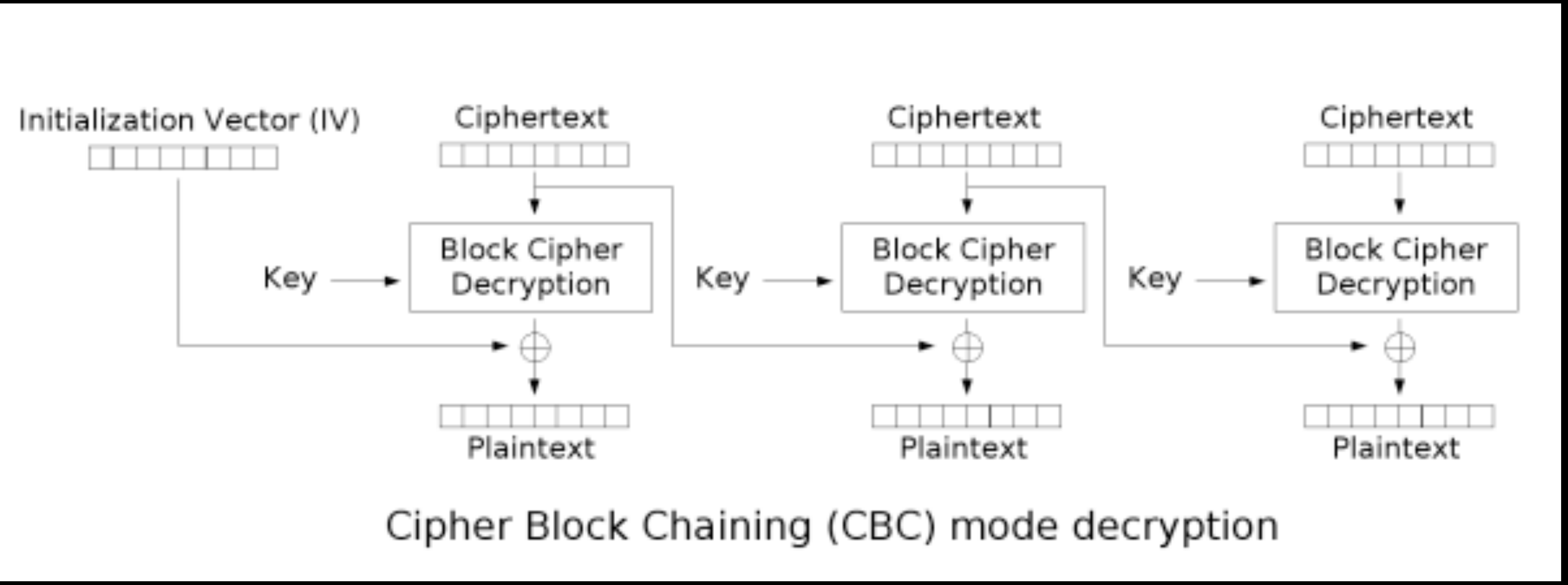
b?

Using Block Ciphers

- ECB is not semantically secure, hence we use a “mode of operation”
  - e.g., CBC, CTR, CFB, OFB (and others)
- These provide:
  - Security for multi-block messages
  - Randomization (through an Initialization Vector)

CBC Mode





Public domain image courtesy Wikipedia.

Security of CBC

- Is CBC a secure encryption scheme?
  - Yes, assuming a secure block cipher
  - Correct (random) IV generation
  - Can <u>prove</u> this under assumption that
    block cipher = Pseudo-Random Permutation (PRP)
- Bellare, Desai, Jokipii & Rogaway (2000)
- Easy to use wrong...
  - Most important: use a unique & random IV!

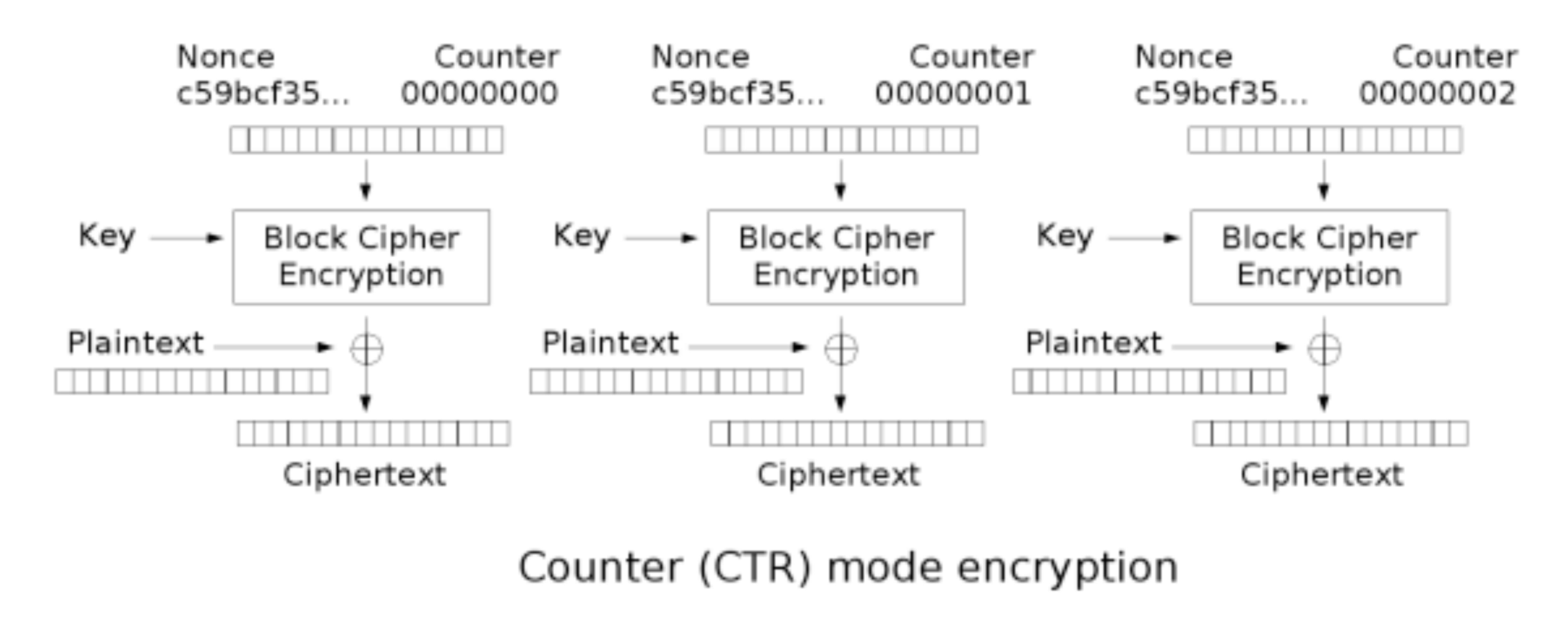
The size of the frame of data to be encrypted or decrypted (i.e. how often a new CBC chain is started) depends on the particular application, and is defined for each in the corresponding format specific books of this specification. Unless otherwise specified, the Initialization Vector used at the beginning of a CBC encryption or decryption chain is a constant, $iv_{0,}$ which is:

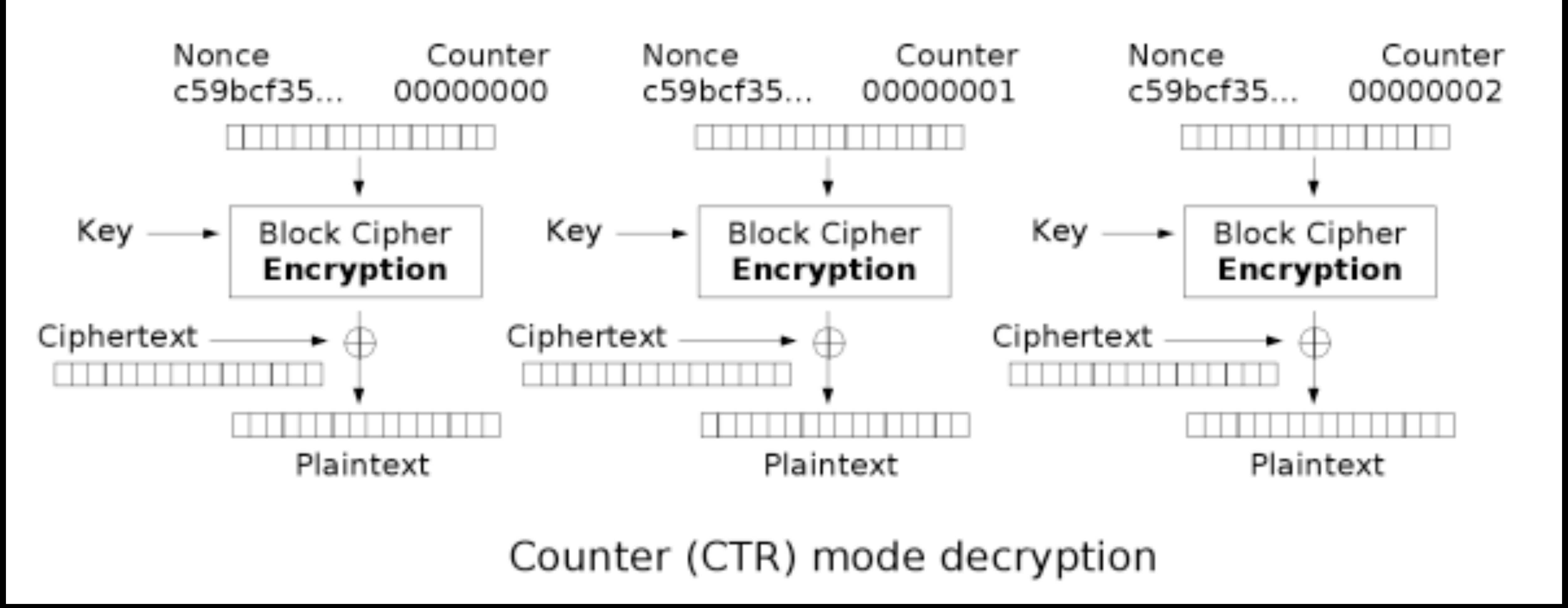
$$0BA0F8DDFEA61FB3D8DF9F566A050F78_{16}$$

Advanced Access Content System (AACS)

Introduction and Common Cryptographic Elements

CTR Mode





Public domain image courtesy Wikipedia.

Security of CTR

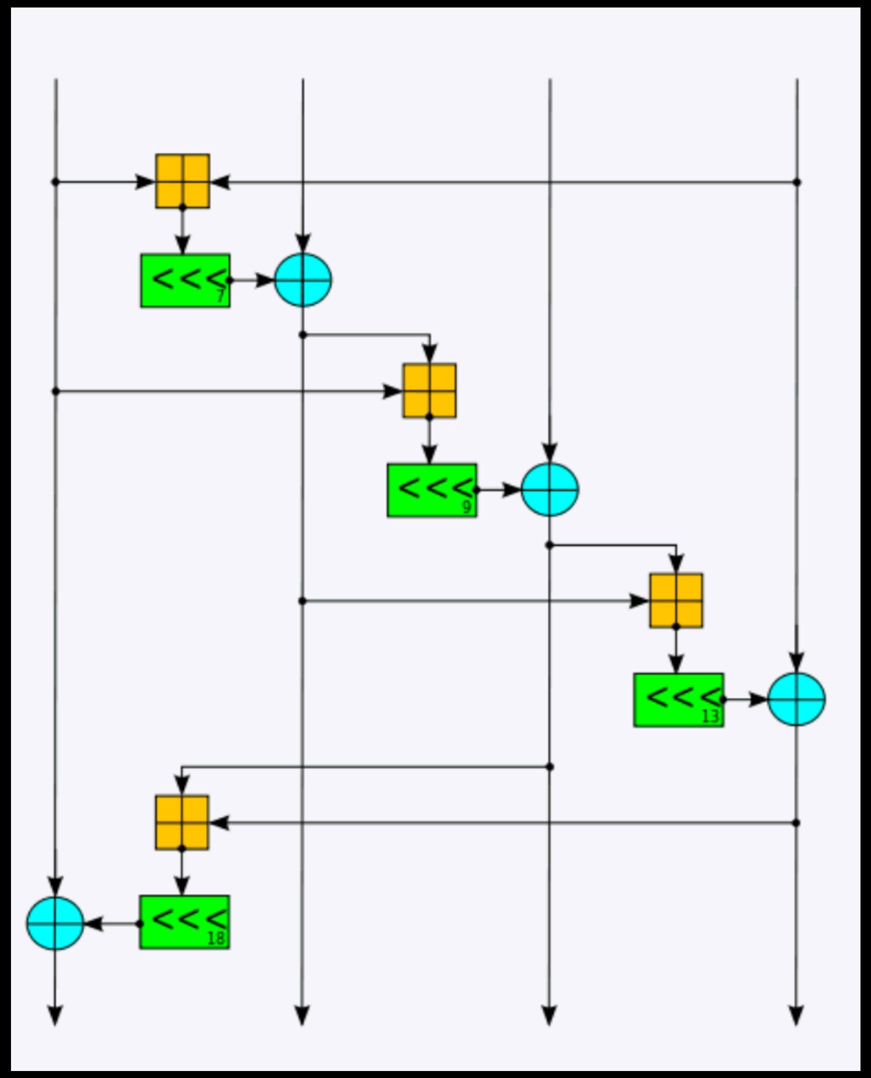
- Yes, assuming secure block cipher (PRP)
- However, counter range must never be re-used

$$(\text{Plaintext 1} \oplus \cancel{\text{Keystream}}) \oplus (\text{Plaintext 2} \oplus \cancel{\text{Keystream}}) = \text{Plaintext 1} \oplus \text{Plaintext 2}$$

- Similar example: MS Word 2003
  - (they used RC4, but same problem)

Alternative ciphers

- Salsa20, ChaCha (Bernstein)
  - These are not block ciphers
  - Designed as *non-invertible pseudorandom* functions
  - Salsa20(k, n) -> {output}
  - Can use these to implement a stream cipher (i.e. CTR mode)



Point of order

- Proofs of security:
  - We <u>don't</u> know how to prove that DES or AES or Salsa20 are secure block ciphers
  - But if we assume that the block ciphers <u>are</u> secure PRPs (resp PRFs) then:

•We can prove that CBC & CTR & OFB & CFB etc.
are secure encryption modes.

http://www.cs.ucdavis.edu/~rogaway/papers/sym-enc-abstract.html

Point of order

In 2008, Bernstein published the closely related "**ChaCha**" family of ciphers, which aim to increase the diffusion per round while achieving the same or slightly better performance.[17] The Aumasson et al. paper also attacks ChaCha, achieving one round fewer: for 256 bits ChaCha6 with complexity 2^{139} and ChaCha7 with complexity 2^{248}. 128 bits ChaCha6 within 2^{107}, but claims that the attack fails to break 128 bits ChaCha7.[3]

- Proofs
  - We c… block ciph…
  - But if we assume that the block ciphers <u>are</u> secure PRPs (resp PRFs) then:

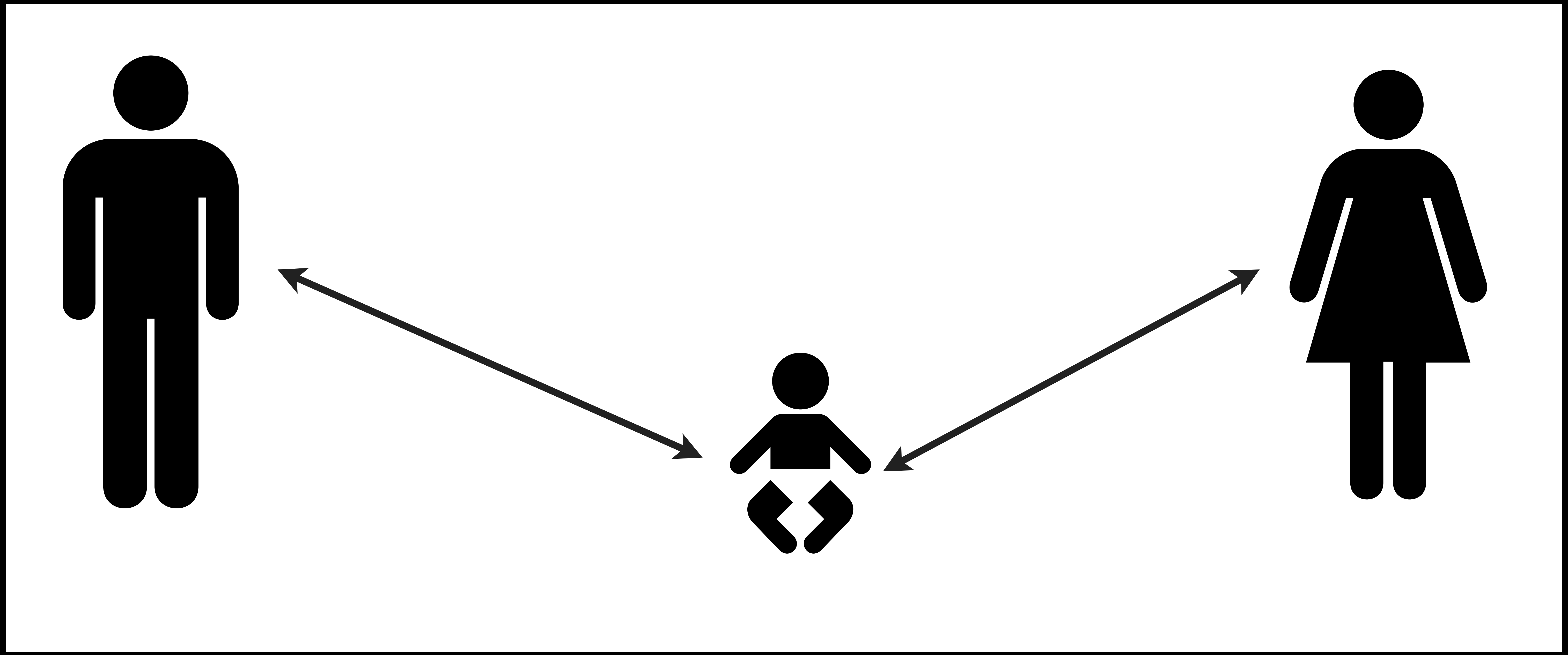
- We can prove that CBC & CTR & OFB & CFB etc. are secure encryption modes.

http://www.cs.ucdavis.edu/~rogaway/papers/sym-enc-abstract.html

Malleability

- The ability to modify a ciphertext
  - Such that the plaintext is meaningfully altered
  - CTR Mode (bad)
  - CBC Mode (somewhat bad)

Authenticated Encryption



MACs

- Symmetric-key primitive
  - Given a key and a message, compute a “tag”
  - Tag can be verified using the same key
  - Any changes to the message detectable
- To prevent malleability:
  - Encrypt <u>then</u> MAC
  - Under separate keys

MACs

- Definitions of Security
  - Existential Unforgeability under Chosen Message Attack (EU-CMA)
- Examples:
  - HMAC (based on hash functions)
  - CMAC/CBC-MAC (block ciphers)

Authenticated Encryption

- Two ways to get there:
  - <u>Generic composition</u>
    Encrypt (e.g., CBC mode) then MAC

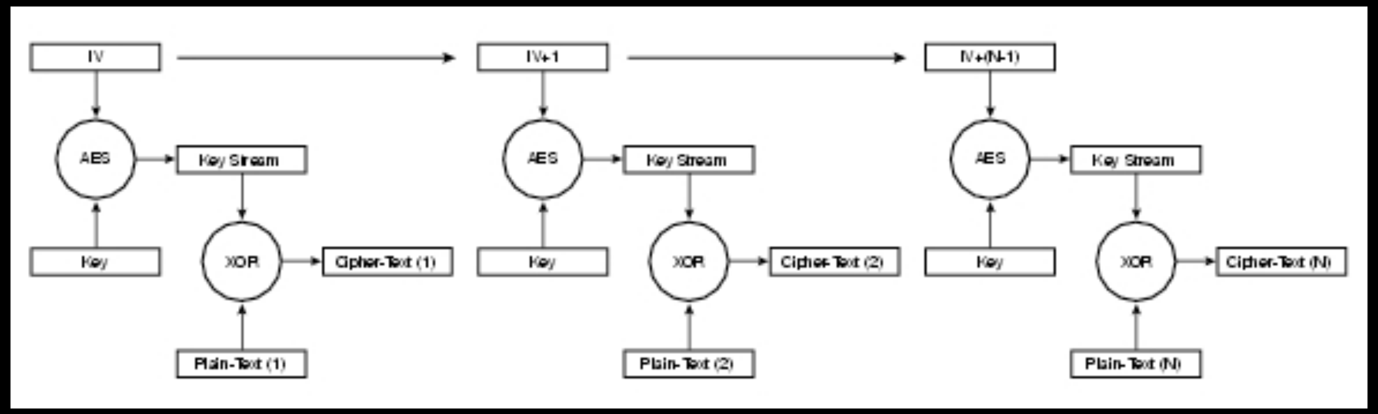
•two different keys, multiple primitives

- <u>Authenticated</u> mode of operation

•Integrates both encryption & authentication

•Single key, typically uses only one primitive (e.g., block cipher)

•Ex: CCM, OCB, GCM modes



Authenticated Encryption

- Two ways to get there:
  - <u>Generic composition</u>
    Encrypt (e.g., CBC mode) then MAC

•two different keys, multiple primitives

  - <u>Authenticated</u> mode of operation

•Integrates both encryption & authentication

•Single key, typically uses only one primitive (e.g., block cipher)

•Ex: CCM, OCB, GCM modes