

601.445/601.645

Practical Cryptographic Systems

Symmetric Cryptography

Instructor: Alishah Chator

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

Personal Introduction



News?

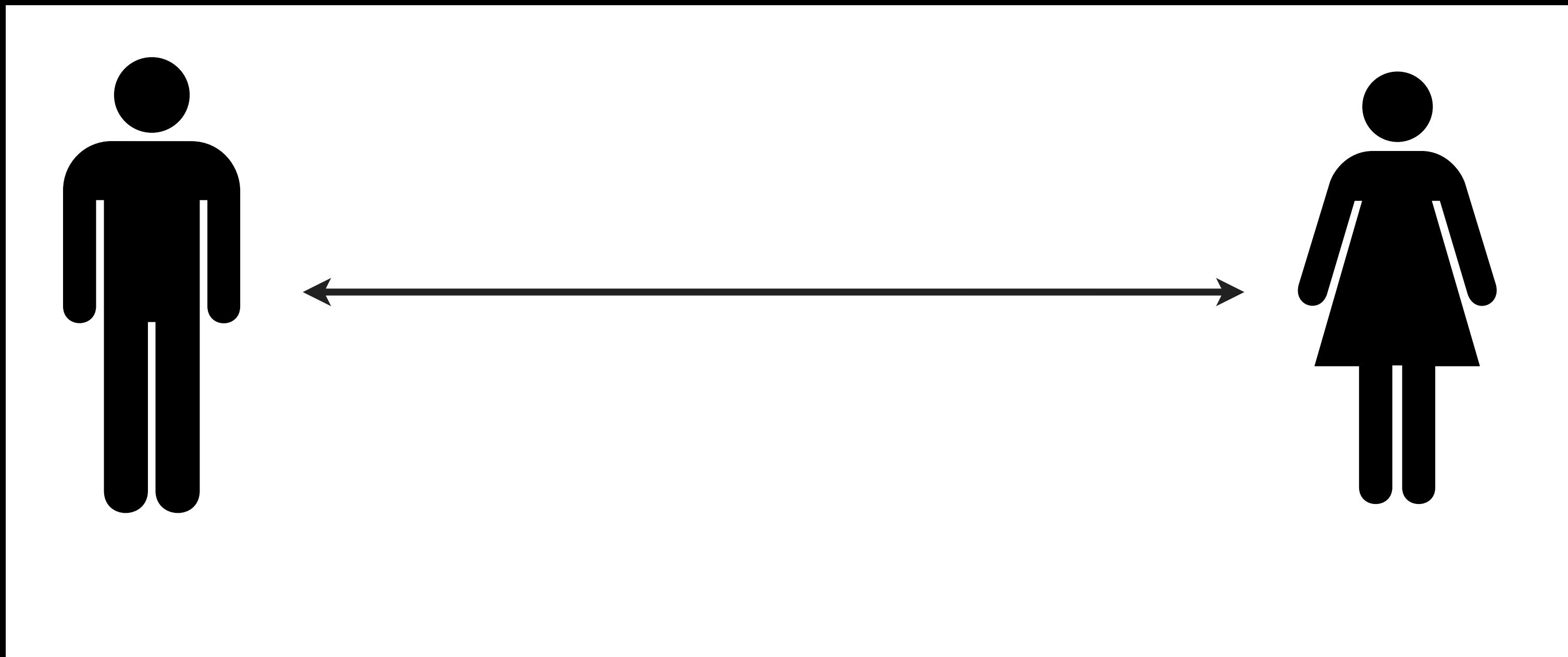
Security/crypto news

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

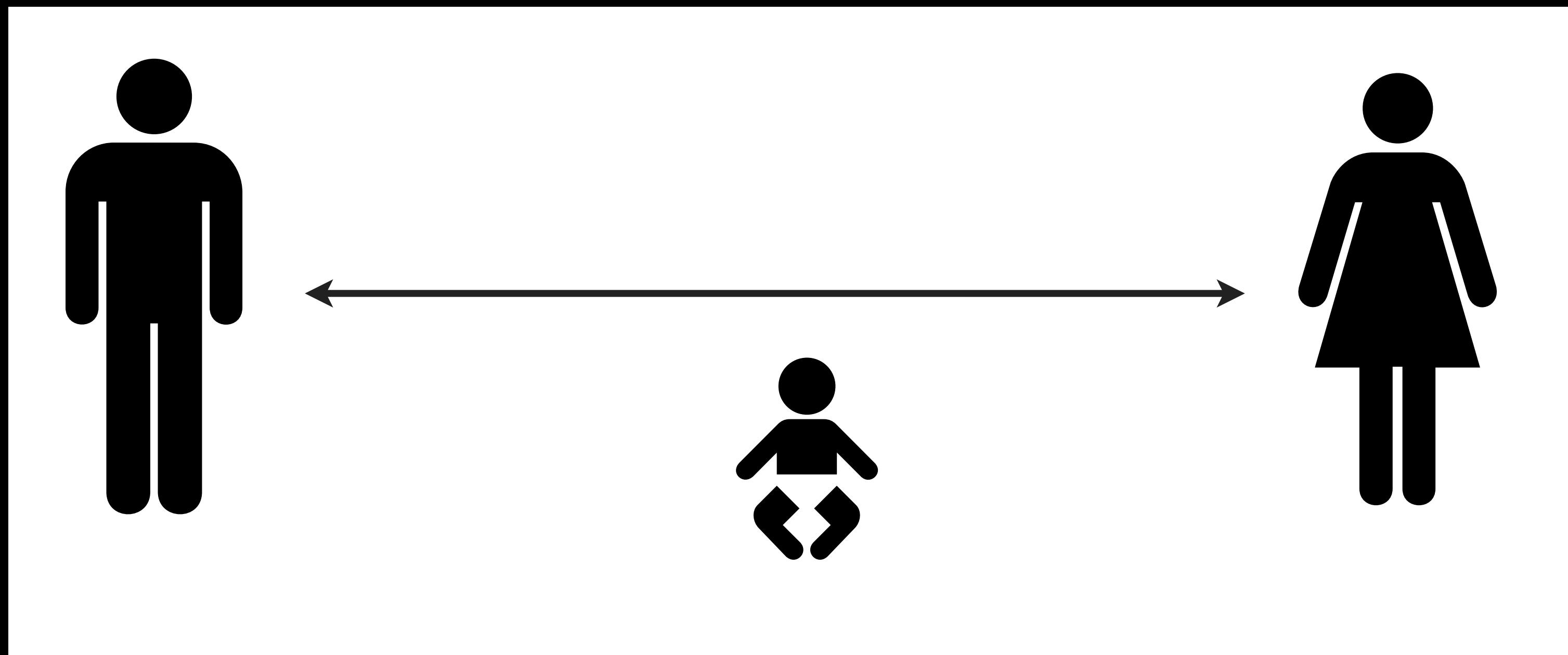
Review

- 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

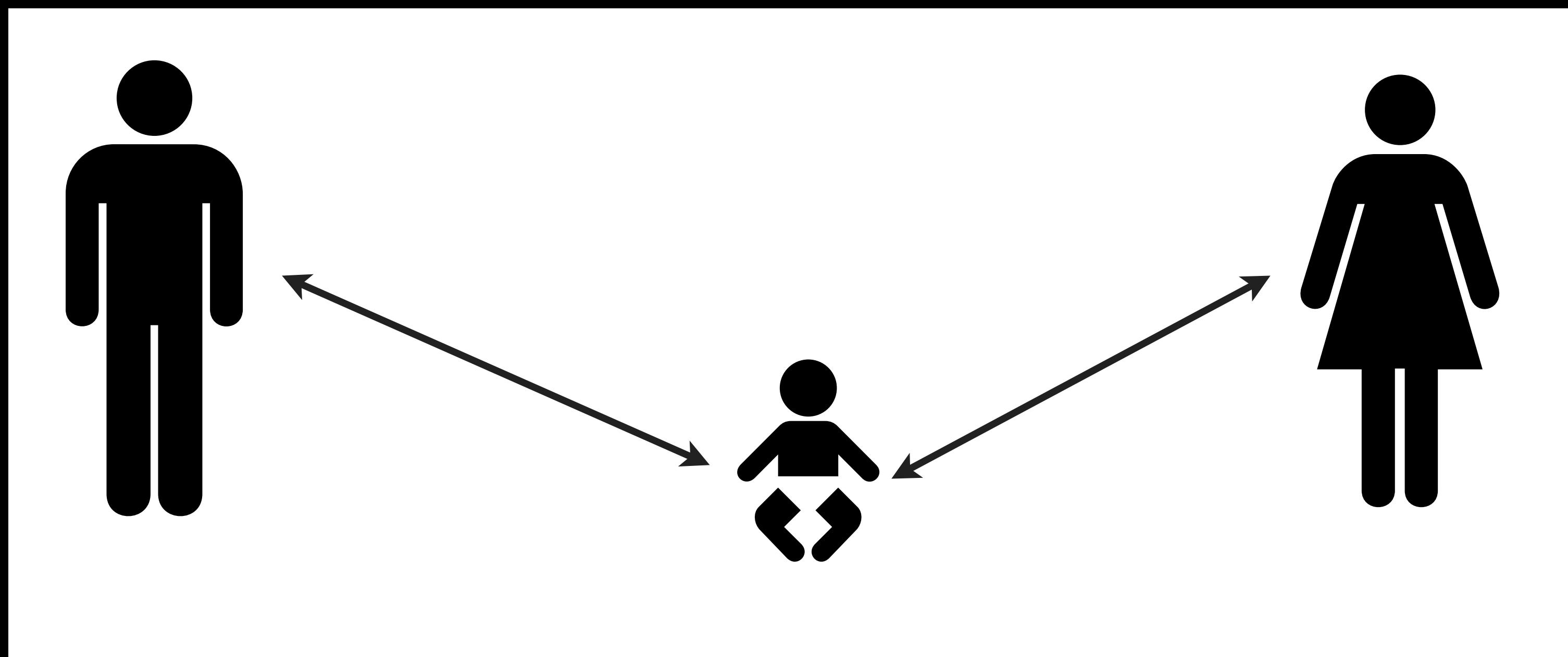
Communication Model



Communication Model



Communication Model



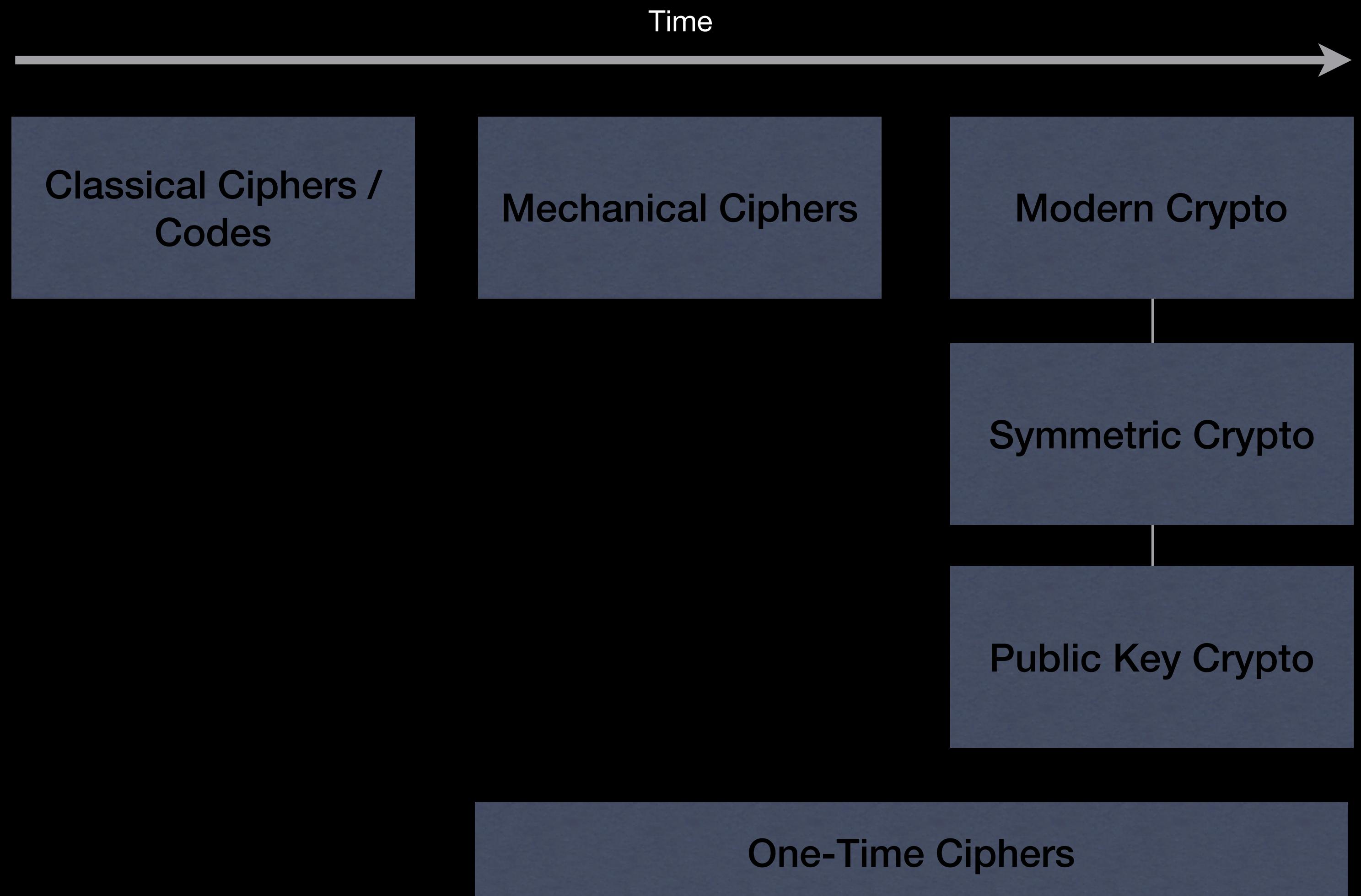
Secure Communication

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

Secure Communication

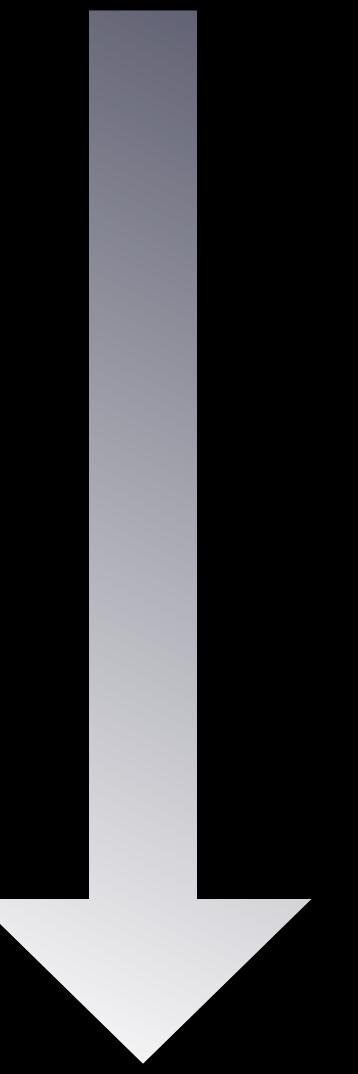
- Two basic properties we like to achieve:
 - Data confidentiality
 - Data authenticity (“integrity”)
- Tools:
 - Encryption / Key exchange
 - Message Authentication Codes (MACs)
 - Digital Signatures

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

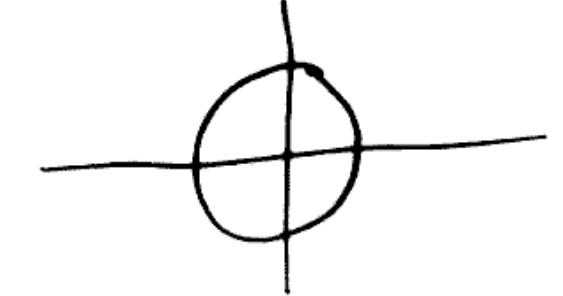
A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	
'	P	I	G	C	G	M	N	N	U	J	C	Y	L	I	P	G	T	Y	T	L	P	I	Y	T	L	
V	Y	K	K	N	G	M	L	G	Y	H	P	I	M	P	U	F	E	R	T	F	O	U	F	E	'	NN
F	E	P	F	J	Y	P	.	.	-	K	F	C	Y	H	K	M	U									

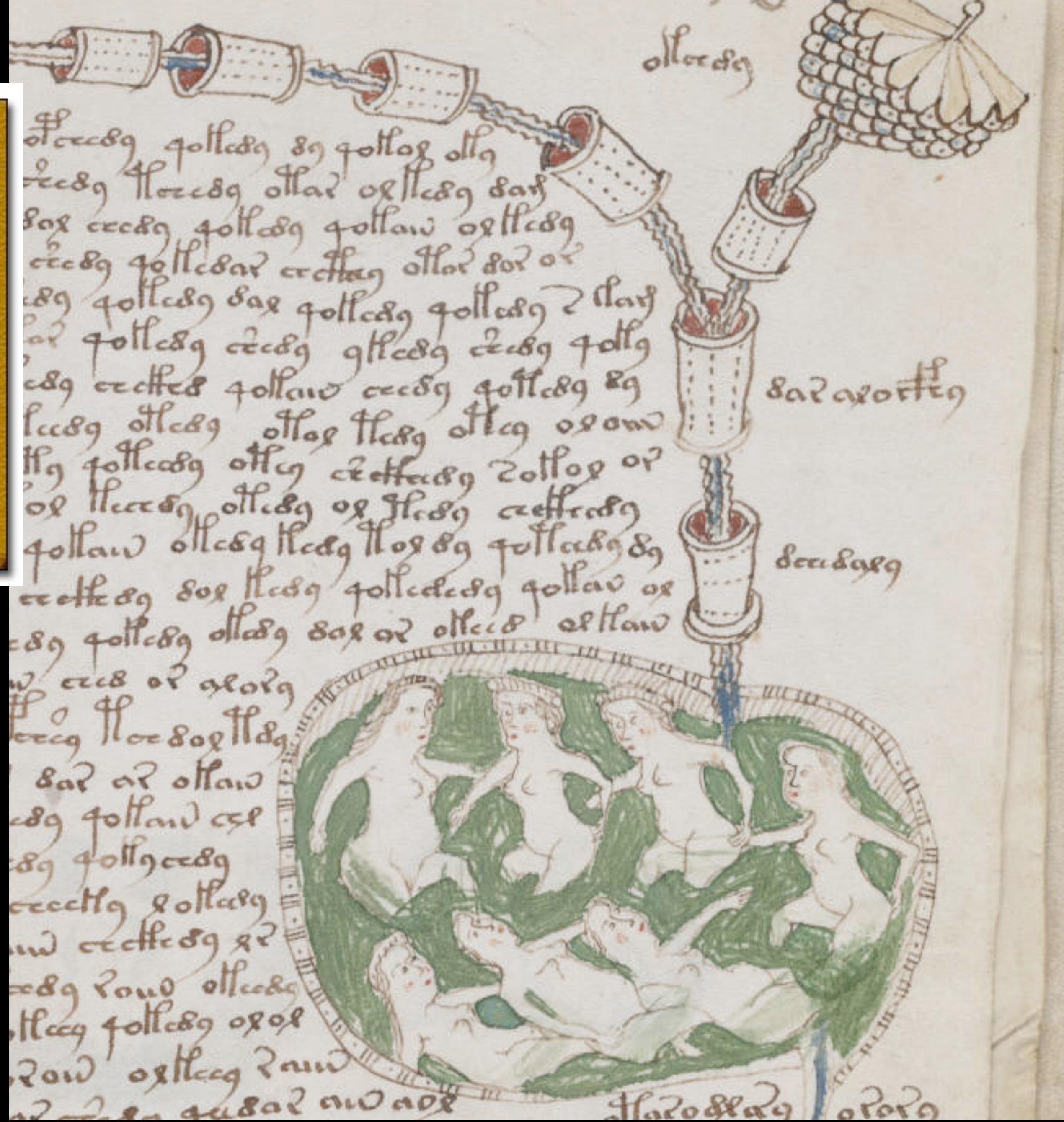
bafaixvola-5//5n1200&+aavifjalkif3415108#l+do0oqfjotnae
a-vf&fvcnna#fem&ofgaxevfocav&fif&fotnaiafala
ofgaitfrova-ic-a-#hjkfj&fca&fem&fotnaia
mogfna&fca&fem&fotnaia&fif&fotnaia&fif&fotnaia
-&fif&fotnaia&fif&fotnaia&fif&fotnaia&fif&fotnaia
ca-15f&fotnaia&fif&fotnaia&fif&fotnaia&fif&fotnaia
##ga22w&fotnaia&fif&fotnaia&fif&fotnaia&fif&fotnaia

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								
V	I	G	E	N	E	R	V	I	G	E	N	E	R	V	I									
N	M	T	H	E	I	Z	R	A	W	X	G	R	Q	V	R	O	A							

H E R > p l v P k i o l t g o d
N q + B φ ■ o □ D w y . < □ K f □
B x I c M + u z G w φ □ L □ H J
S q q □ A l □ A □ V o 9 o + + R K o
□ □ M + □ T □ D □ I □ F P + P o K /
9 □ R □ F □ O - □ D C □ F > o D φ
■ e + K φ □ I e n c X G V . □ L i
φ G o J f t □ o + □ N Y □ + □ L □
D < M + 8 + Z R o F B □ X A o o K
- □ J u v + □ J + 0 9 A < F B x -
U + R / o l E i D y B 9 8 T M K o
o < c l R J i □ o T o M . + P B F
□ o A S Y □ + N i o F B □ o I □ A R
J G F N A □ 7 o o B . □ V o T + +
X B X o □ I o A C E > V U Z o - +
I C . o □ B K f o 9 A . f M o 6 o
R □ T + L □ o C < + F J W B i □ L
+ + o W C □ W C P o S H T / o o q
I F K o W < A l B □ Y o B □ - C o
> M D H N 9 K 5 □ Z o □ A i K I +





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
<hr/>																	
N	M	T	H	E	I	Z	R	A	W	X	G	R	Q	V	R	O	A

One-Time Ciphers

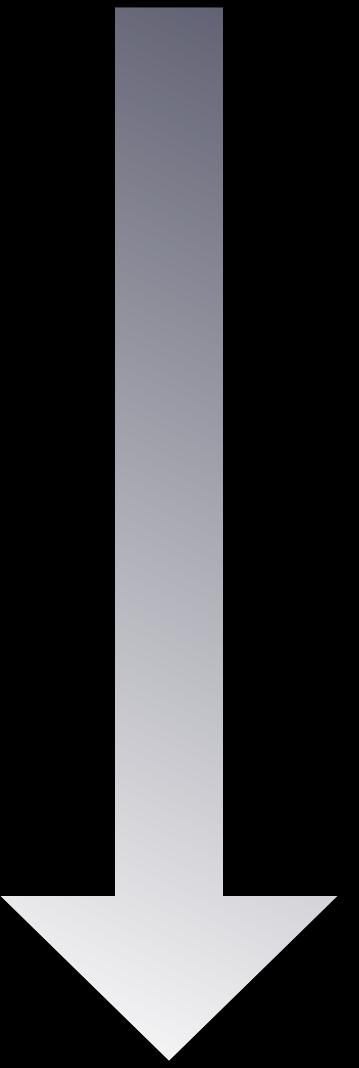
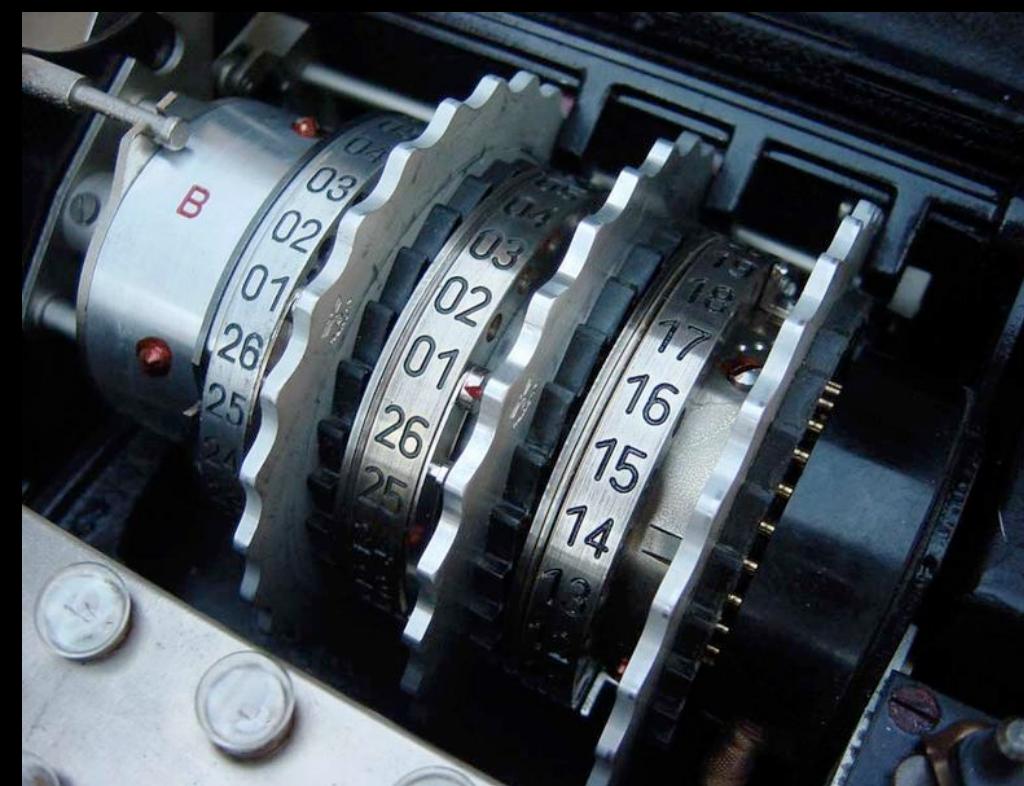
- 1900s
 - Vernam & Mauborgne's "Unbreakable" cipher
- Based on Baudot code for Teletypes
- Added (XORed) a random Key (sequence of bits) to a binary message
 - Perfectly secure, provided:
 - key is perfectly random
 - key is at least as long as the message
 - key is never re-used



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

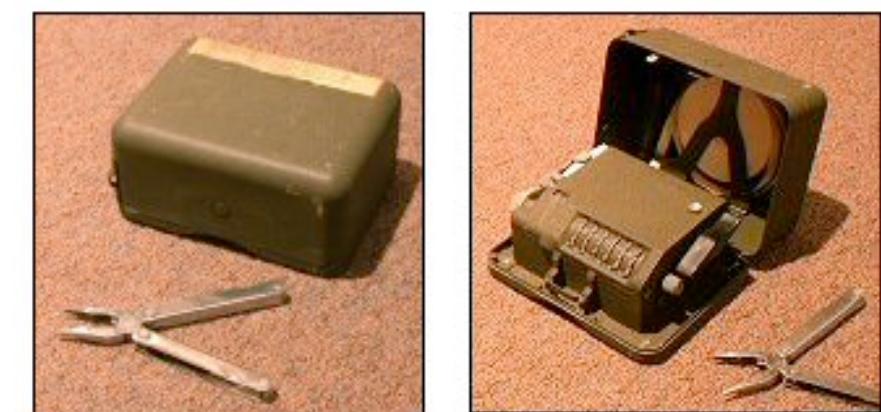
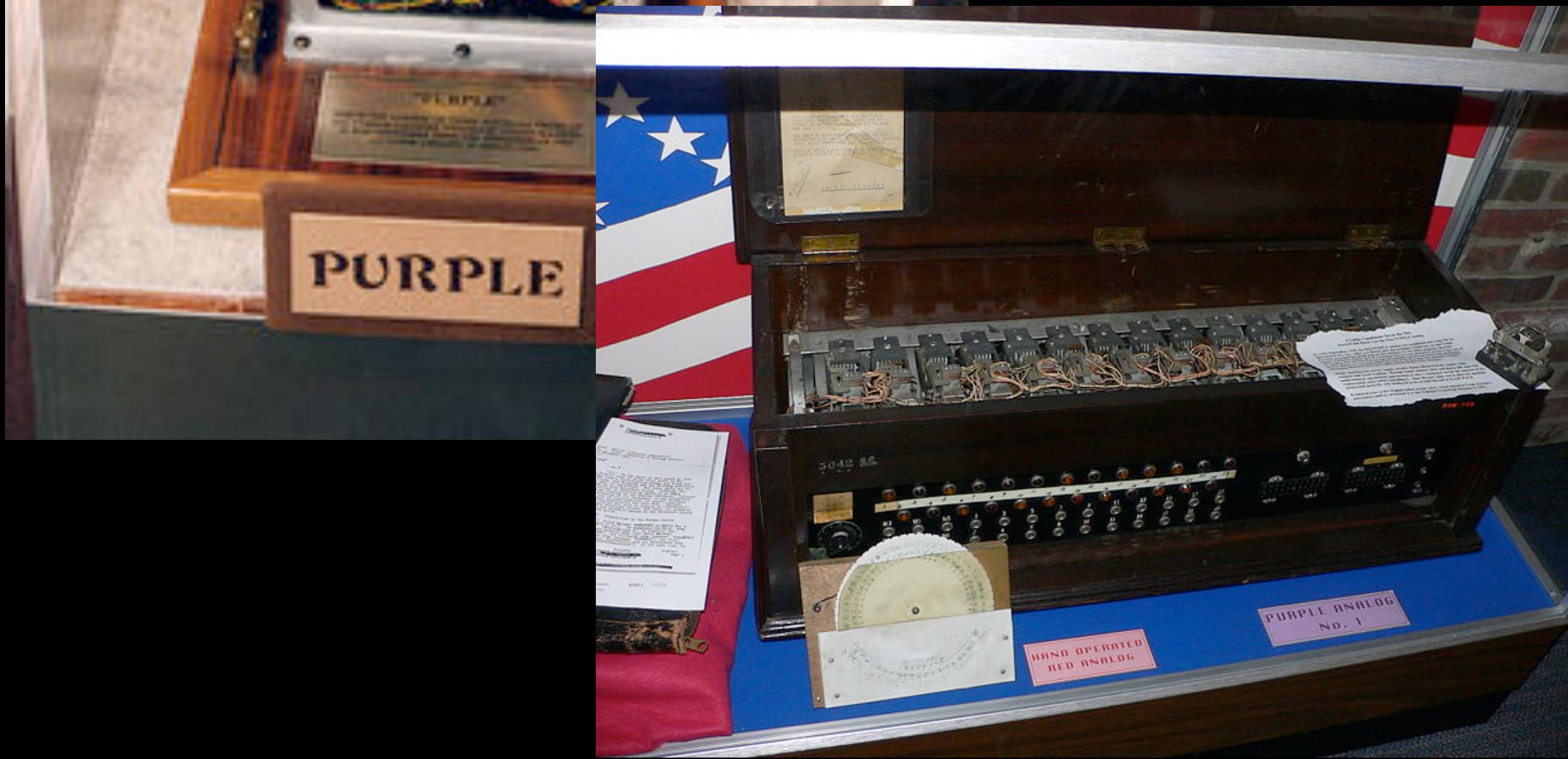
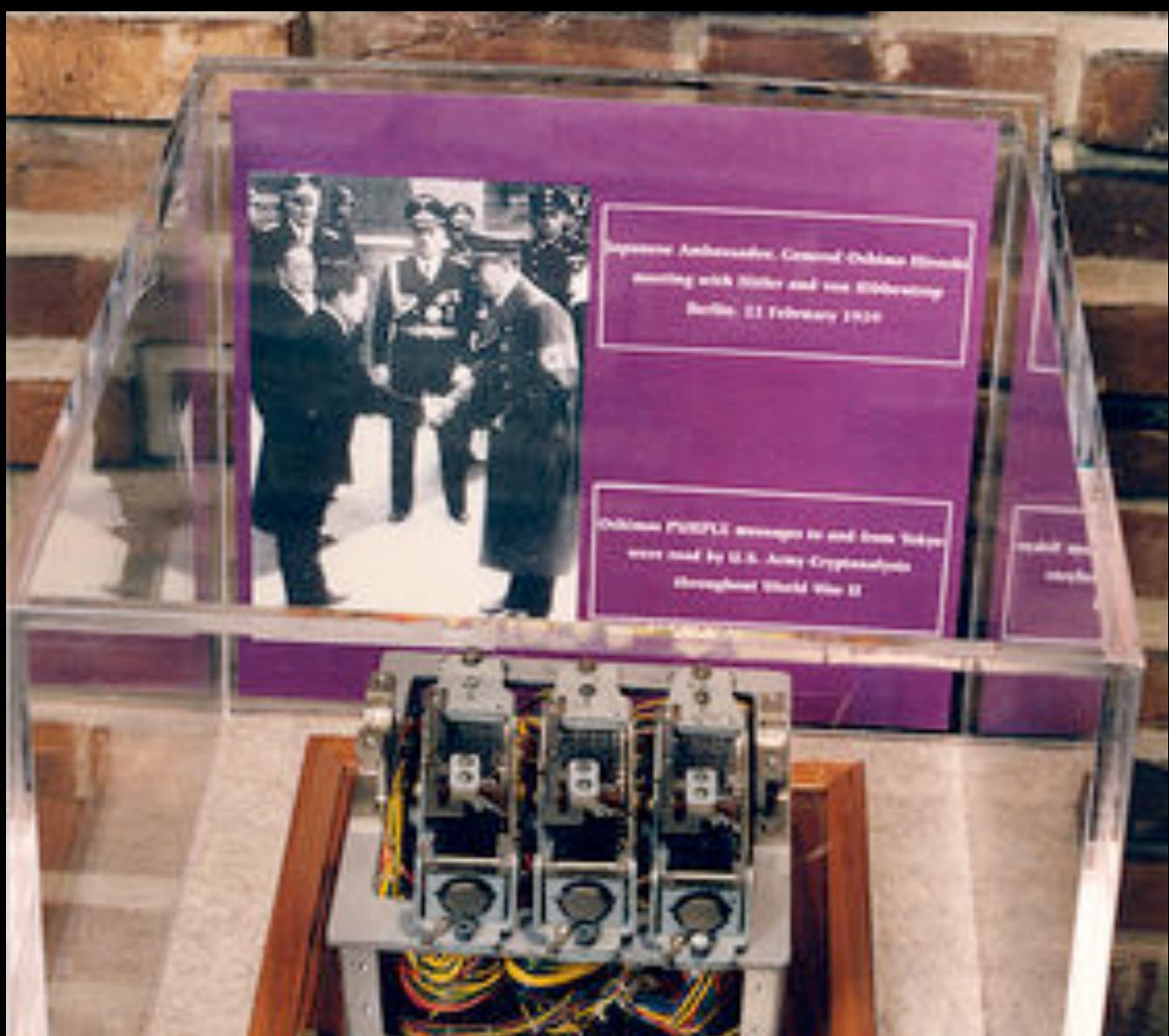
Mechanical Cryptography

- 1900s
 - Mass production and usage of cipher devices
 - Rotor ciphers
 - Electro-mechanical cipher machines

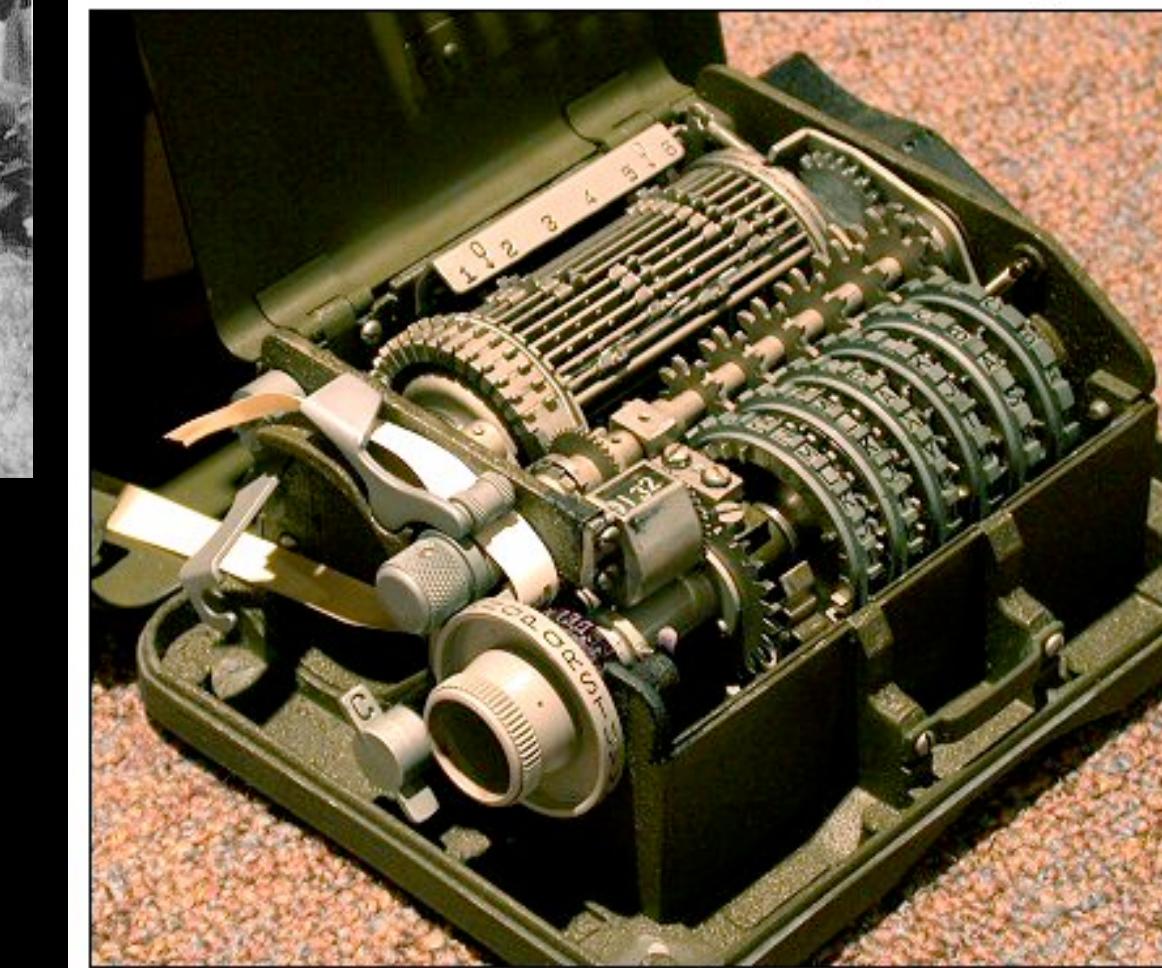


Increasing
Complexity

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



HAGELIN M-209 CIPHER MACHINE (GVG / PD)



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



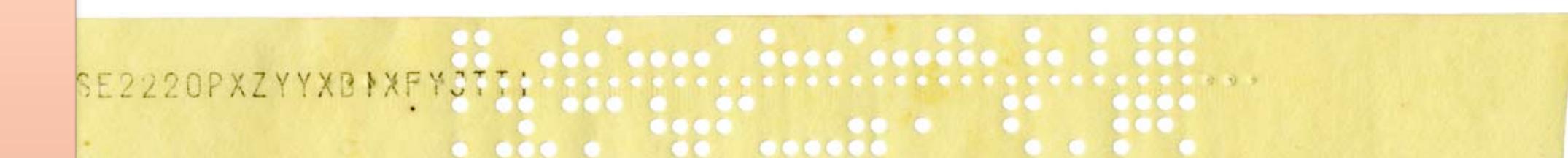
Swedish AB Transvertex HC-9.
Commercial devices used for low-level communications until 1970s.



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}



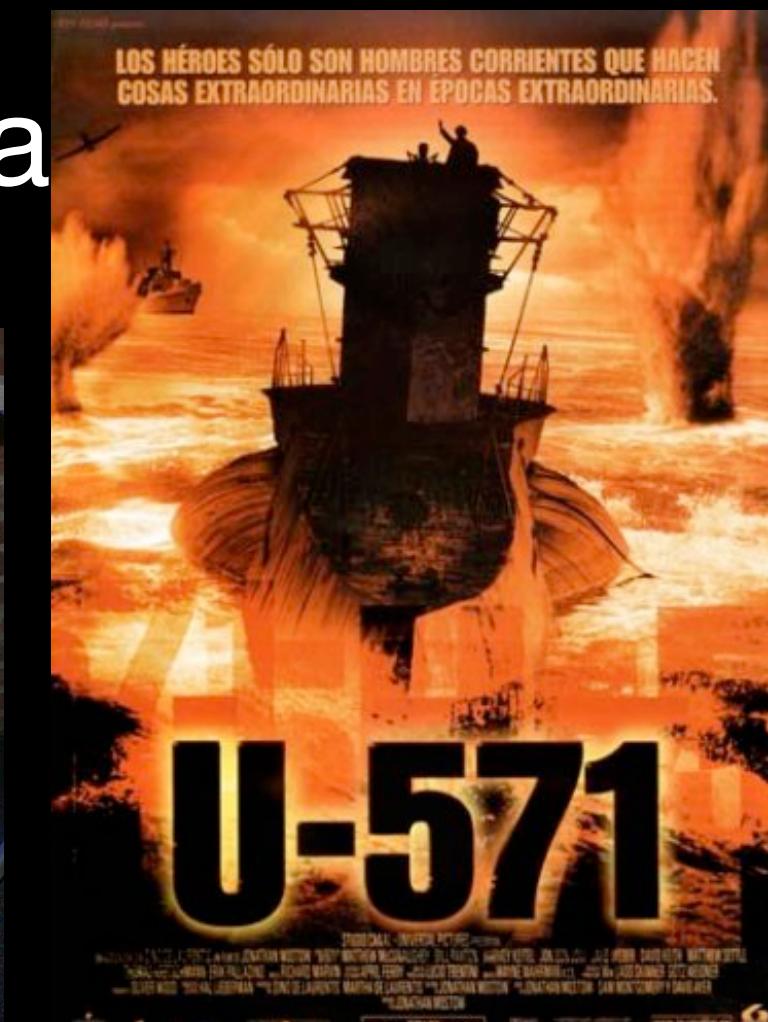
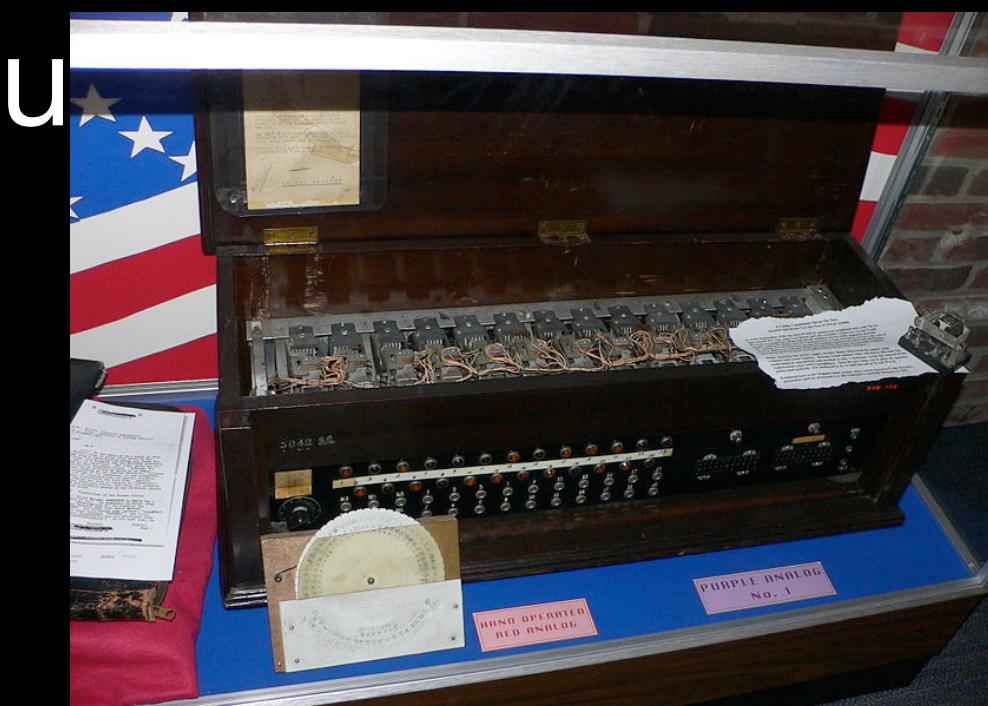
Russian Fialka
used from 1965-1990s
10 rotors, reads and writes to



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

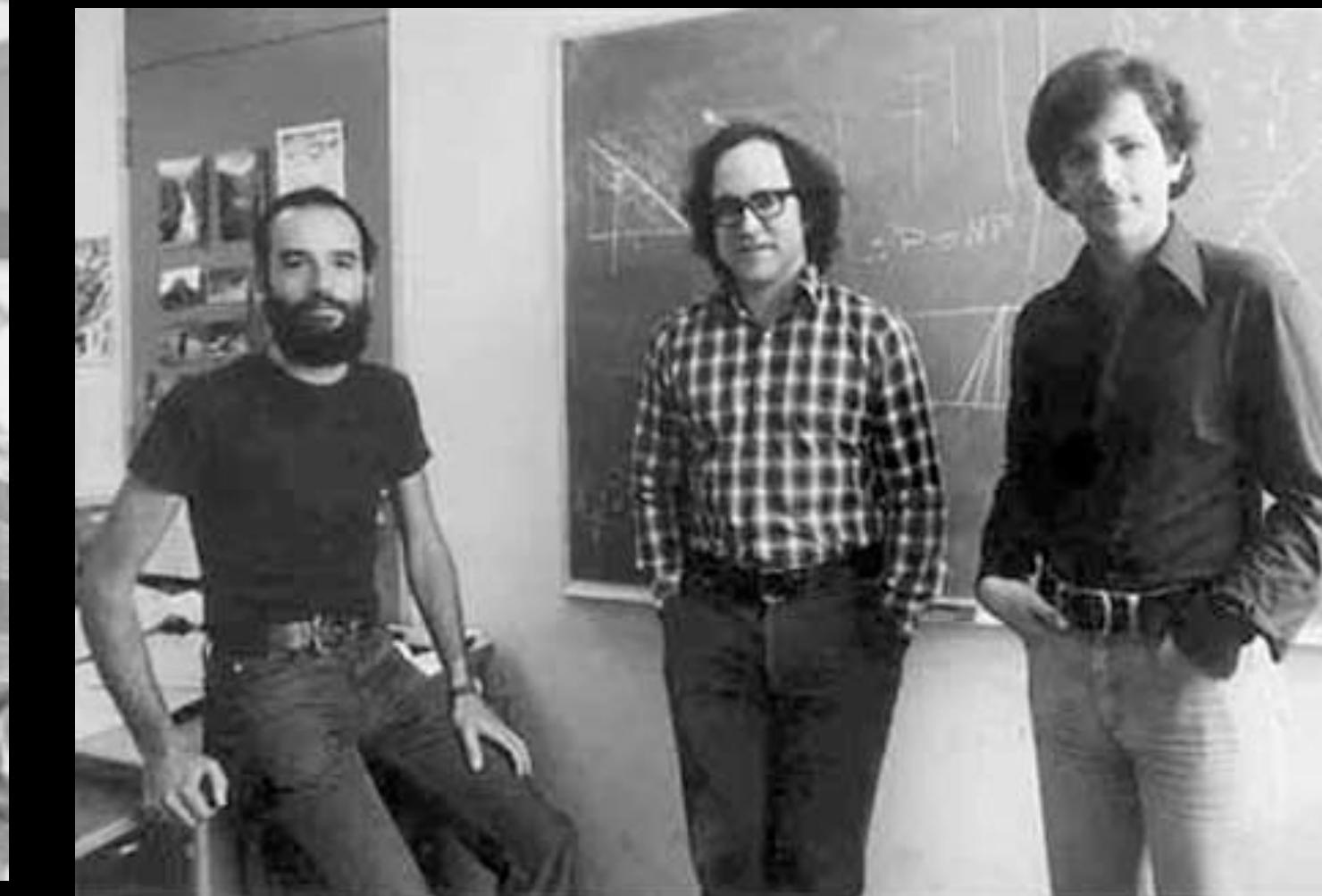
The 1970s



1972



1976
(1974)



1977
(1973)

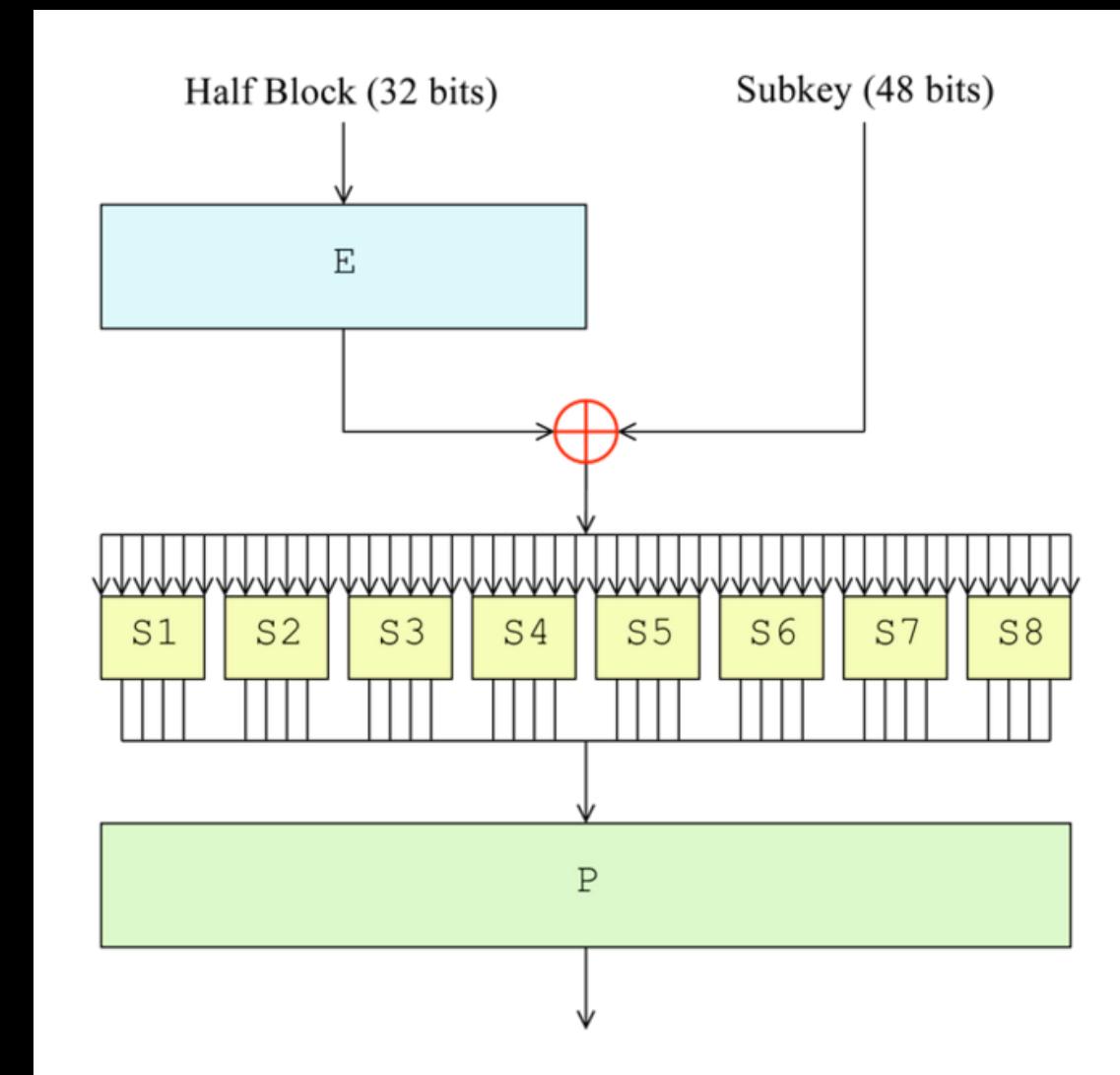
← U.K. GCHQ →

The Implications

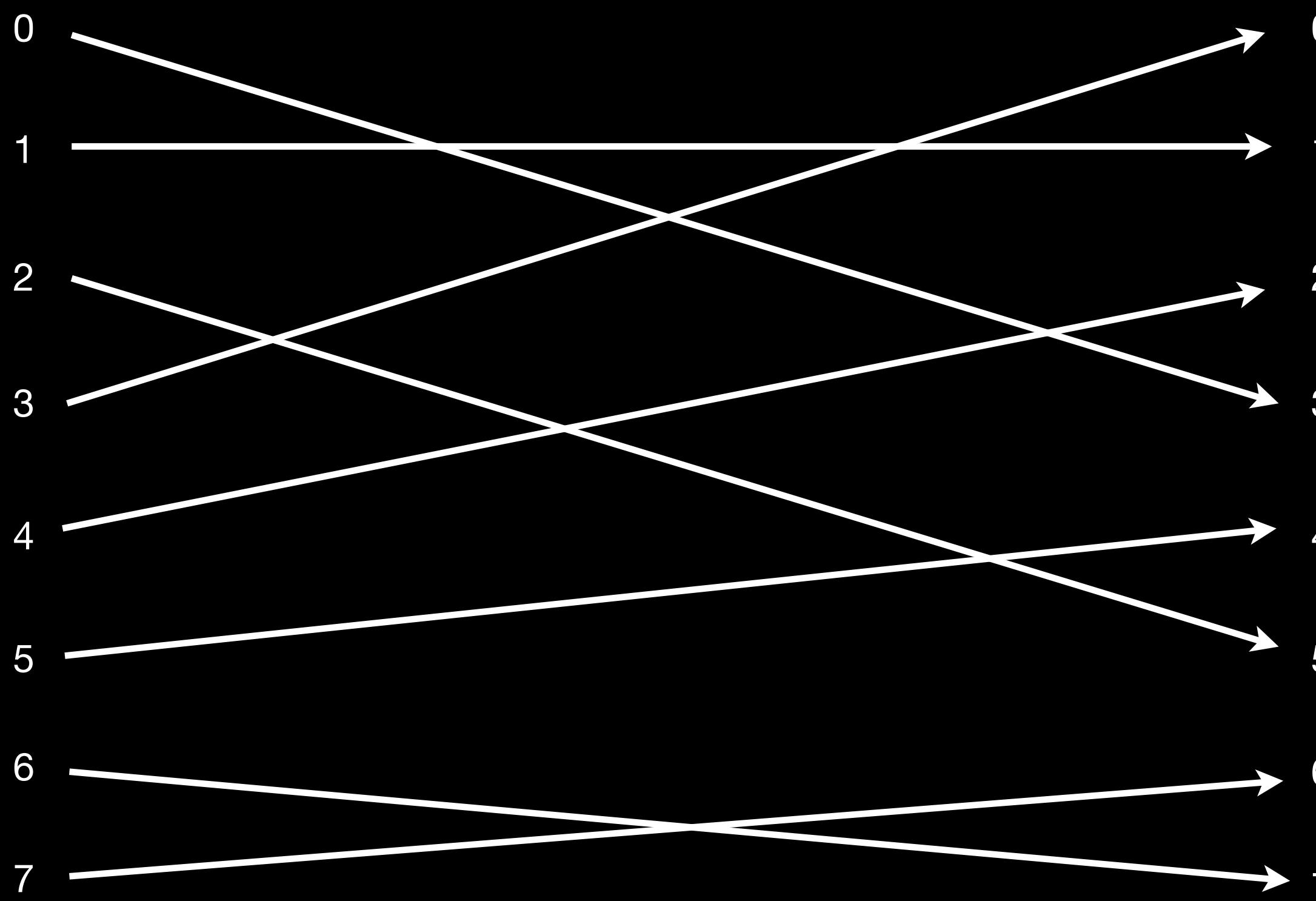
- Exponential increase in study & usage of cryptography in industry, academia
- Wide-scale deployment of cryptographic systems
- Provable Security
 - Cryptographic Systems can be reduced to some hard mathematical problem

Data Encryption Standard

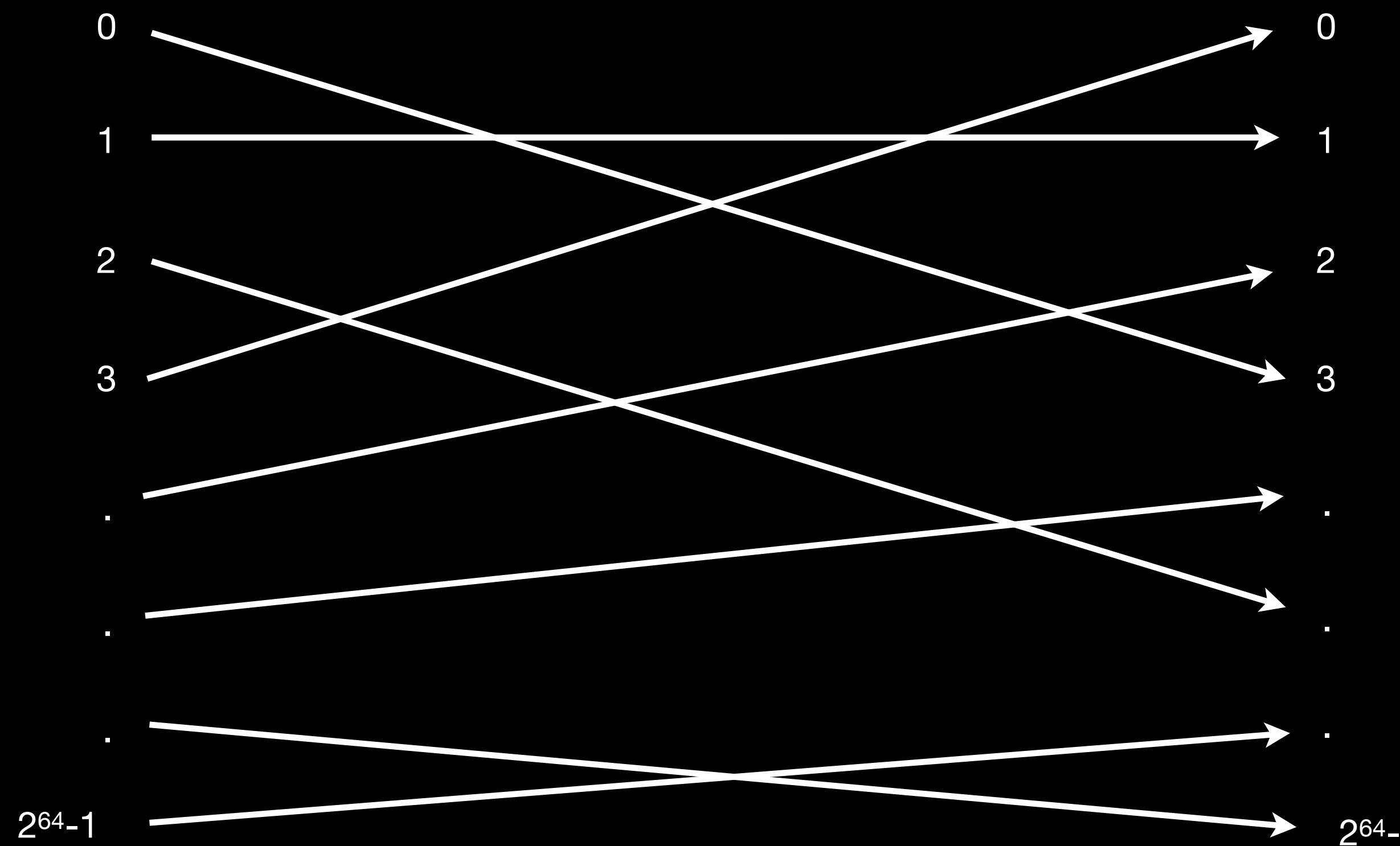
- Commercial-grade Block Cipher
 - 64-bit block size
 - 56 bit key (+ 8 bits parity)
 - “Feistel Network” Construction



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)

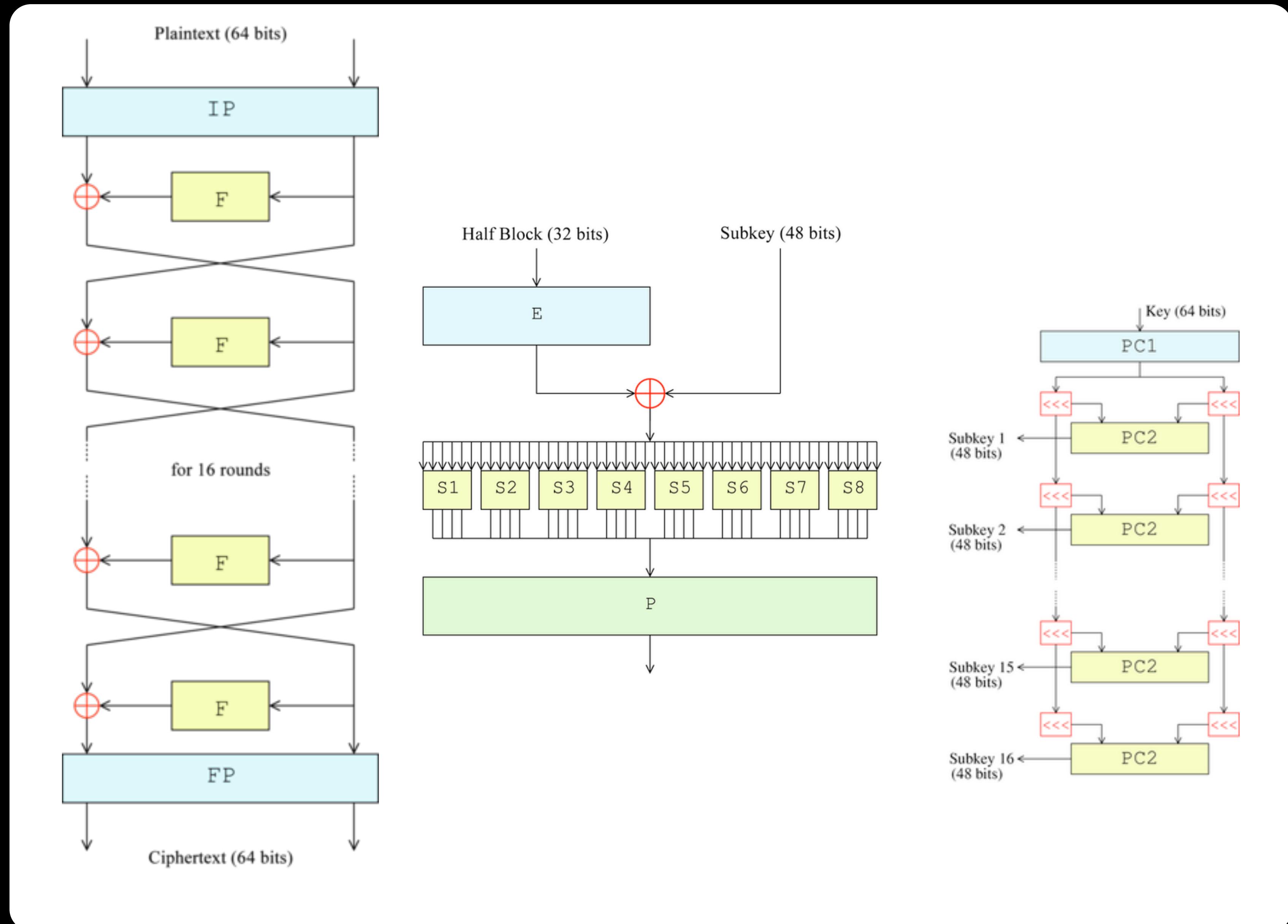
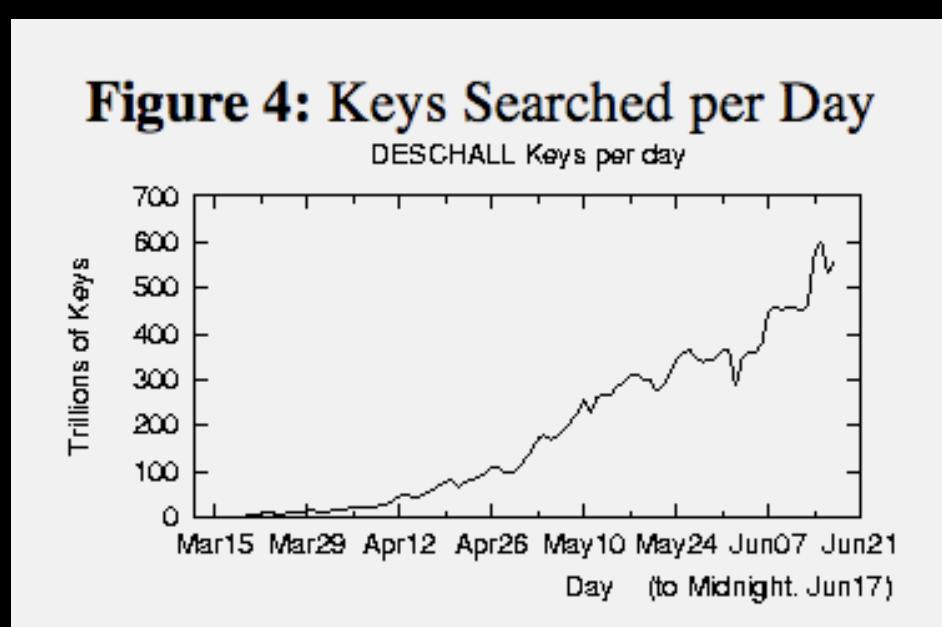


Image from Wikipedia, used under GFDL

DES

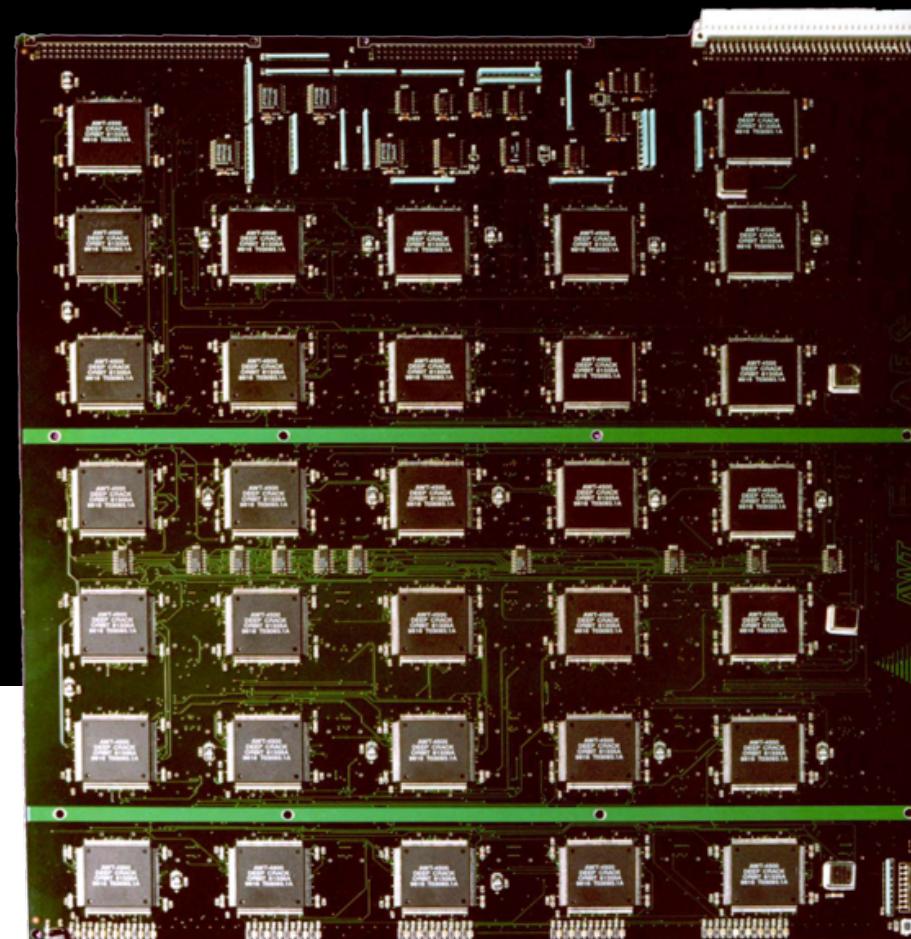
- Some “clever” attacks on DES
 - However: practical weakness = 56 bit key size
 - Practical solution: 3DES (now being deprecated)



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 (200s):
 - Fast in software & hardware
 - Larger block size (128 bit)
 - Longer keys (128/192/256-bit)
- 5 finalists:
 - MARS, RC6, Rijndael, Serpent, and Twofish

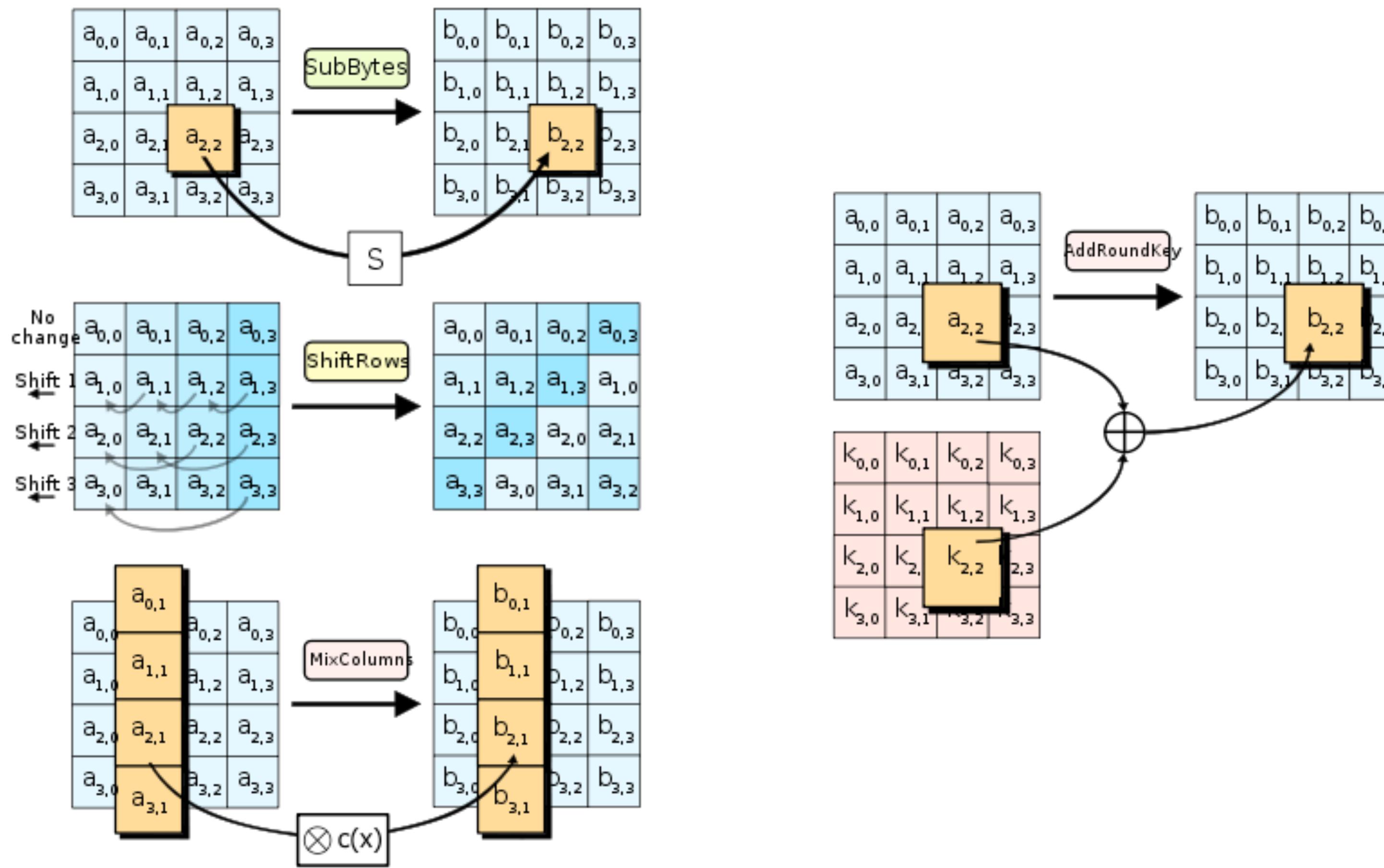
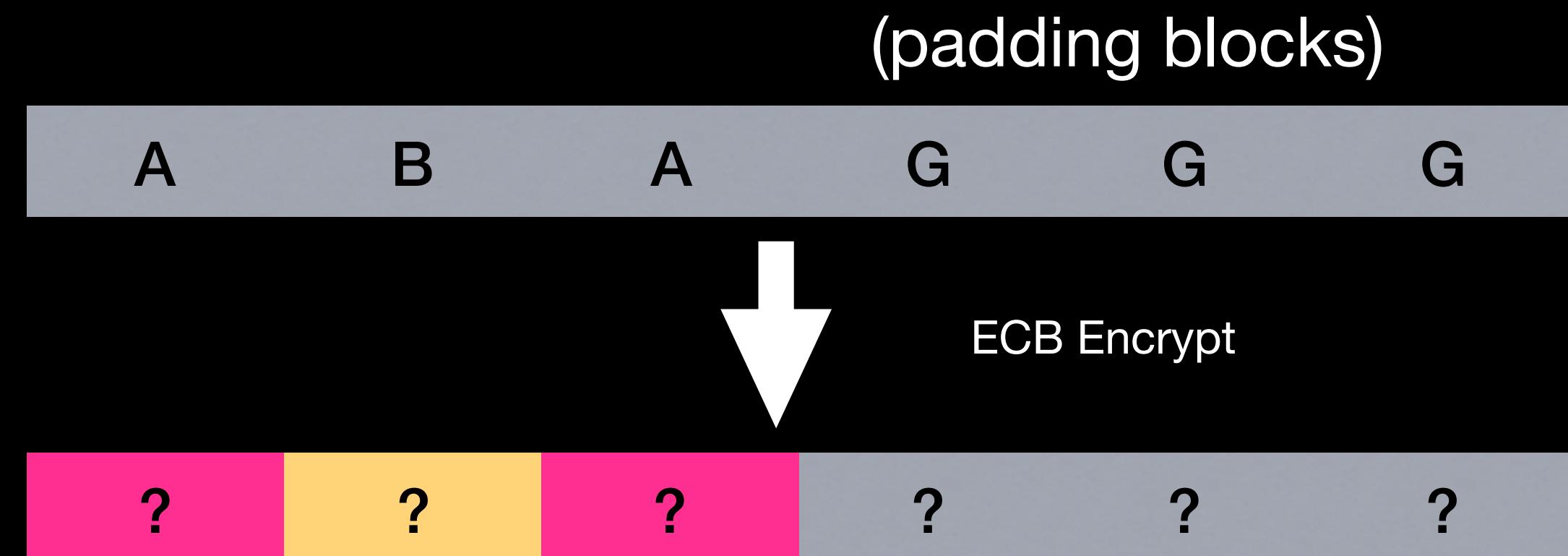
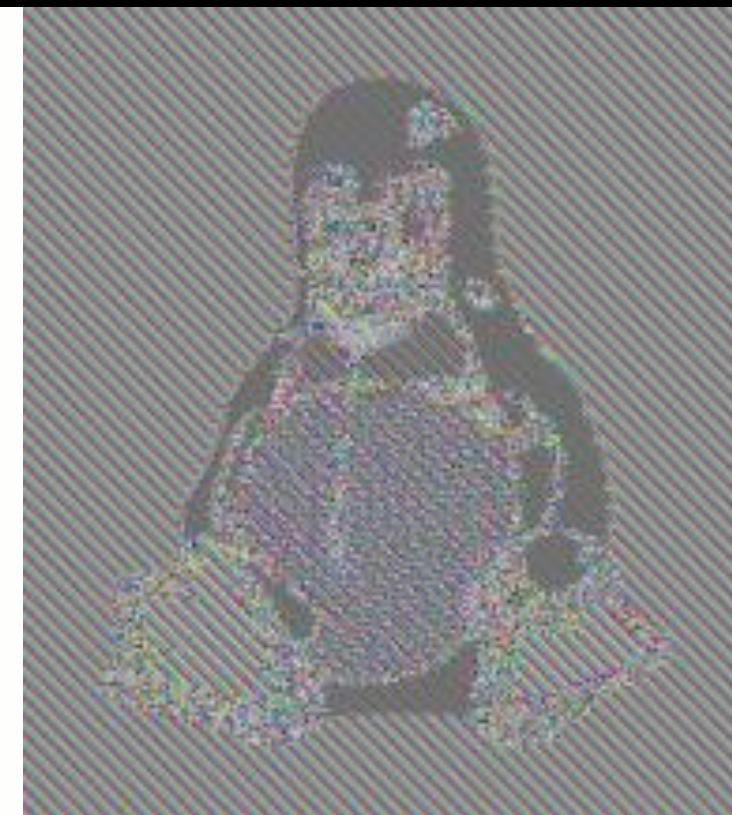
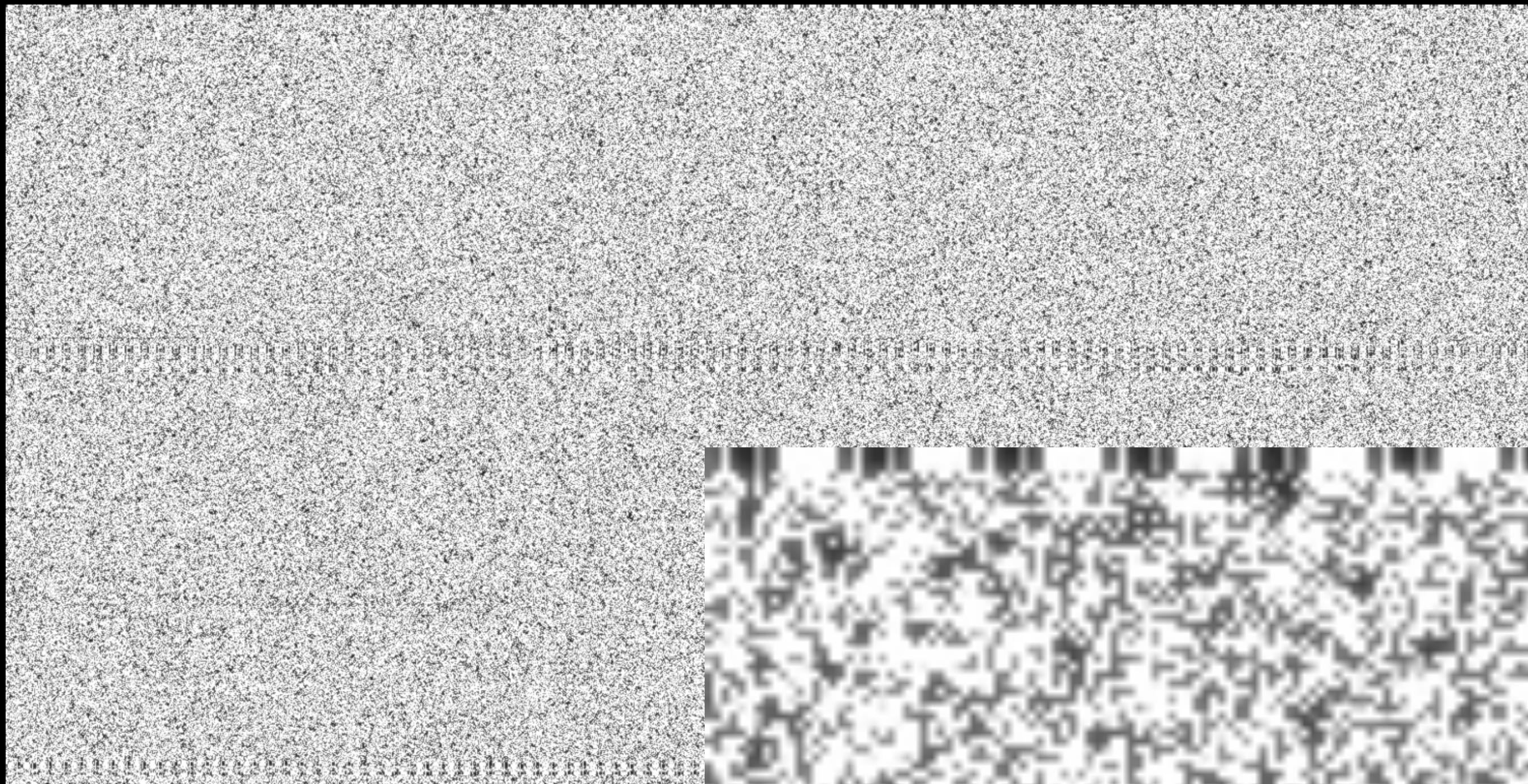


Image from Wikipedia, used under GFDL

How to use a block cipher?

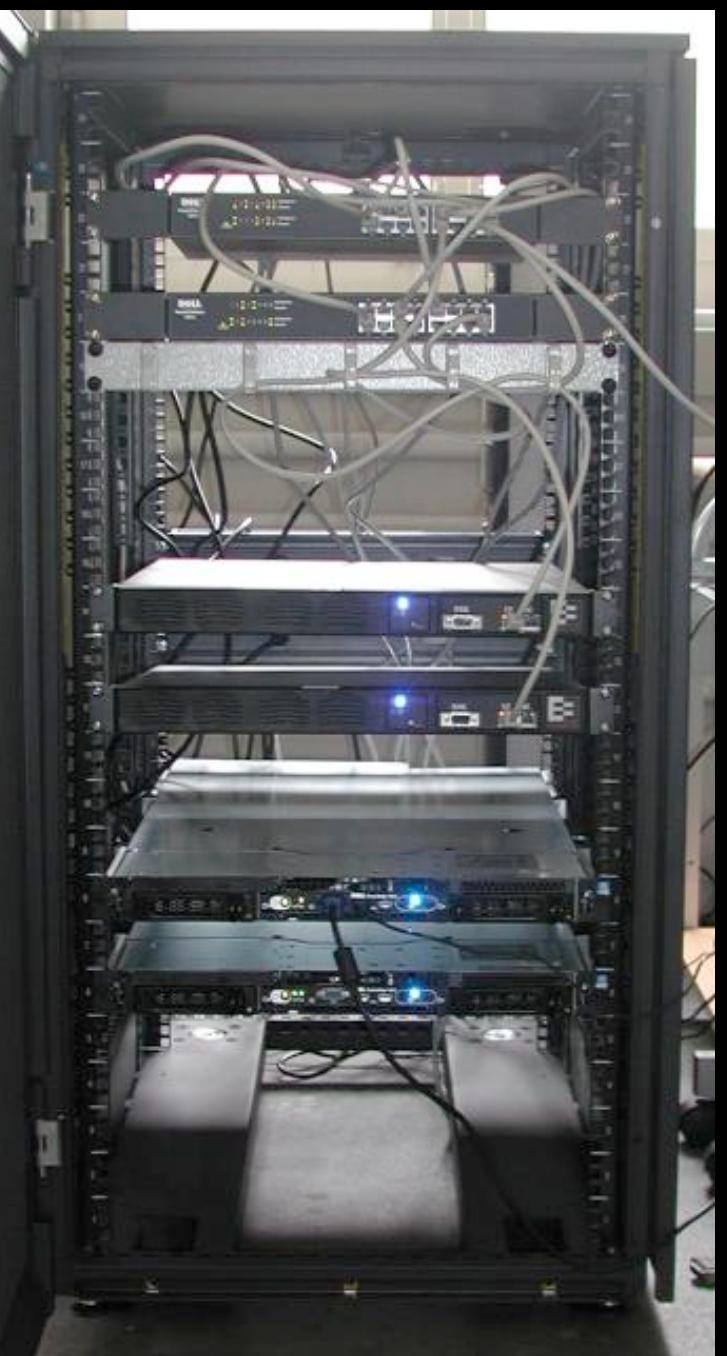
- ECB Mode: Encrypt each block separately
 - Problems?





ECB Mode

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



Game server

E(Attack Monster)
E(Monster Attacks)



Game client

Definitions

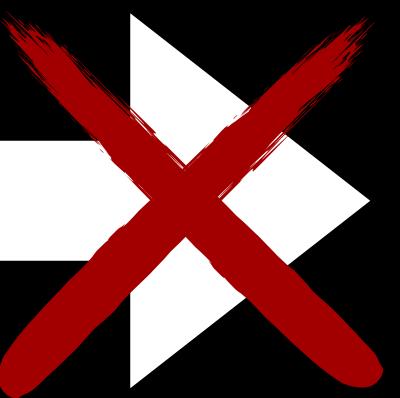
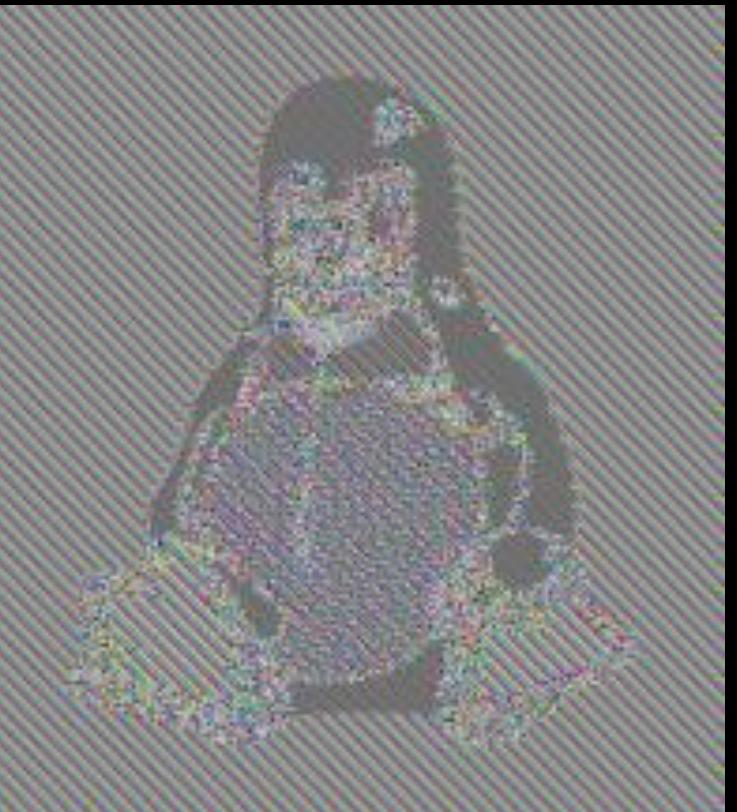
- What does it mean to securely encrypt something?

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 adversary who sees ciphertext “learns as much” as adversary who doesn’t see ciphertext.
- Even if adversary can request chosen plaintexts
 - How do we state this formally?

Semantic security

- Semantic Security (IND-CPA)

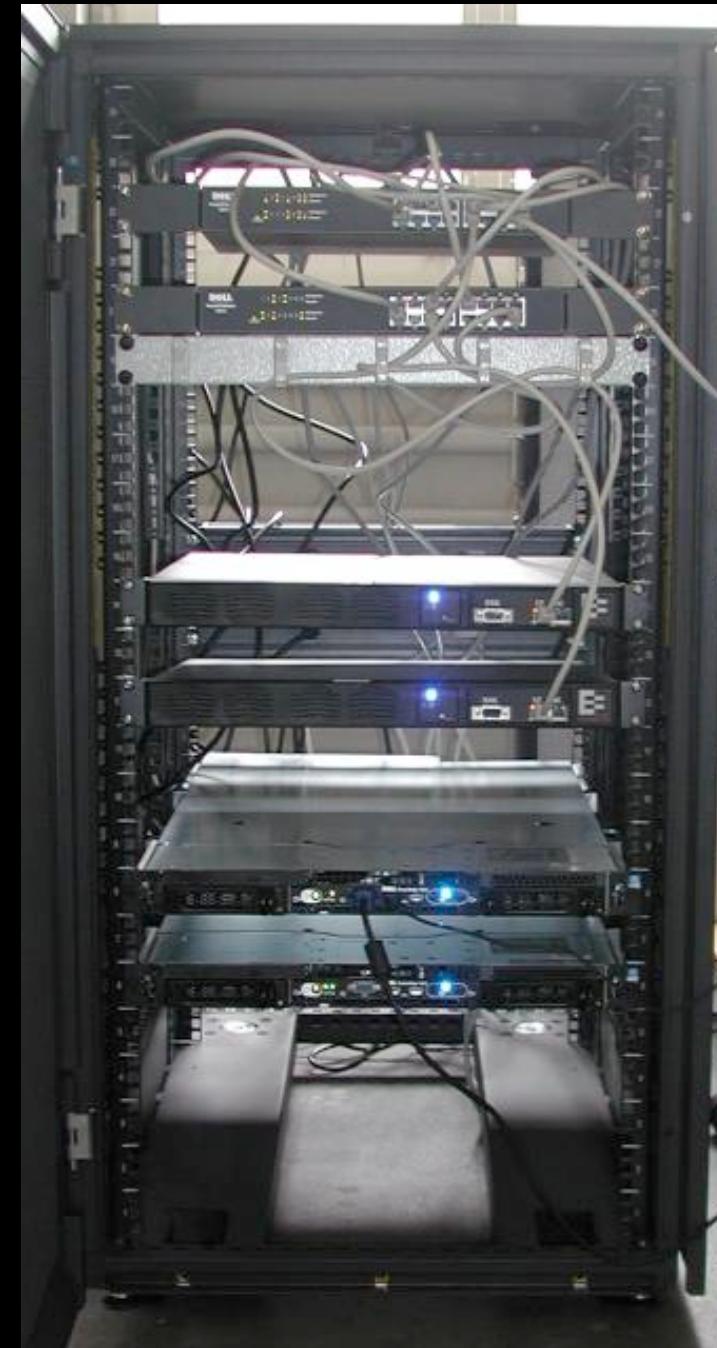
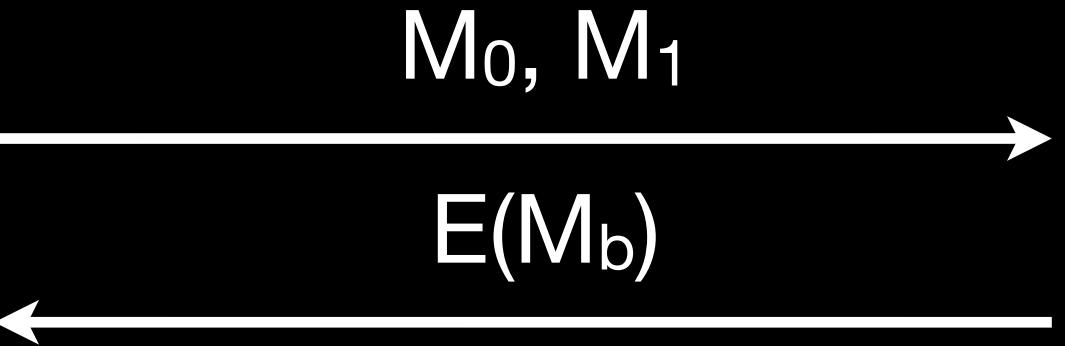
$$b \xleftarrow{\$} \{0, 1\}$$

$$|M_0| = |M_1|$$



Adversary

b?



k

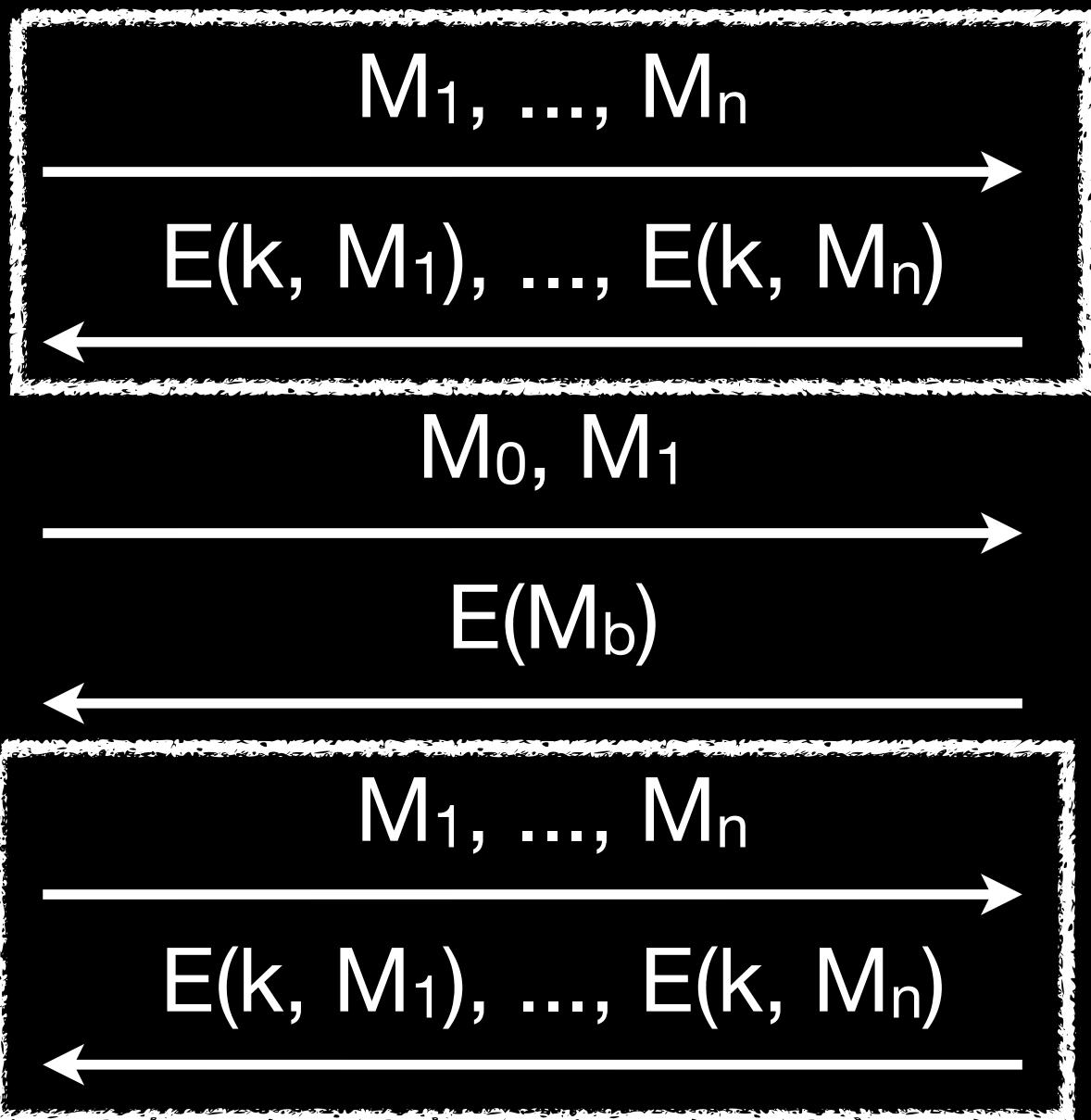
Semantic security

- Semantic Security (IND-CPA)

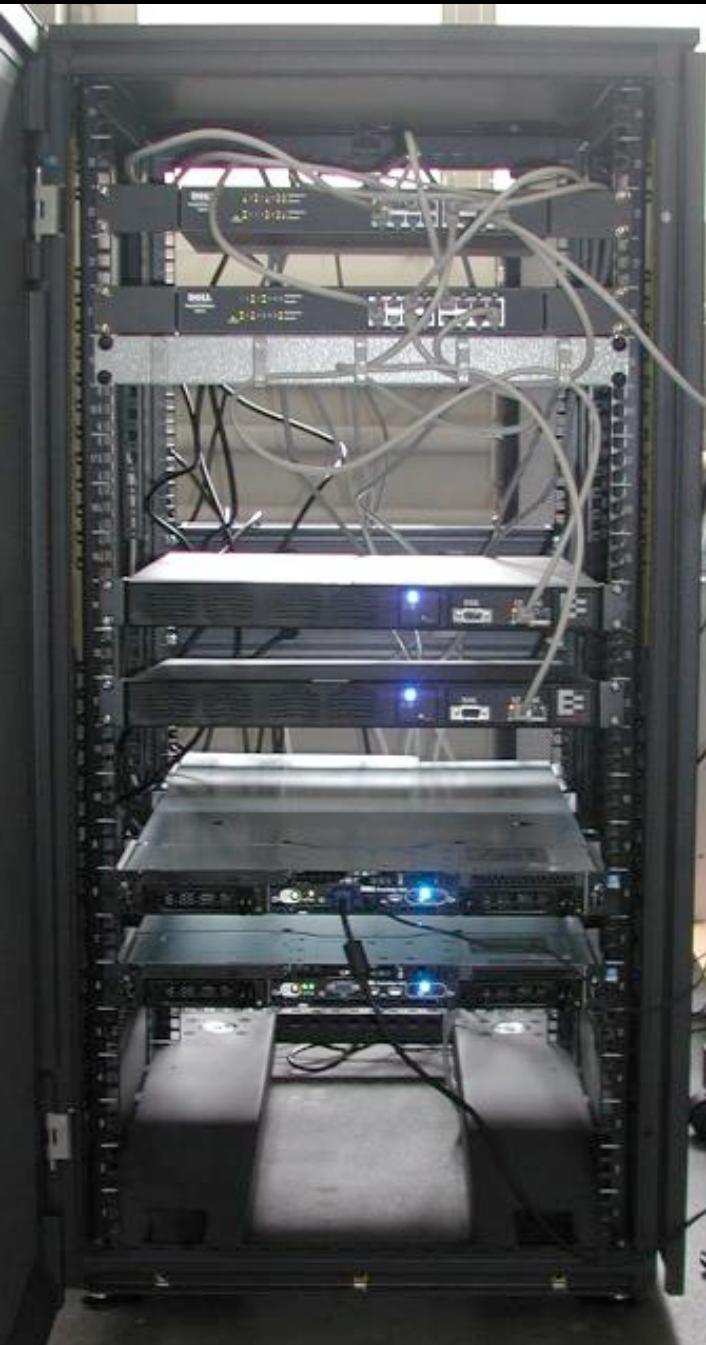
$$b \xleftarrow{\$} \{0, 1\}$$



Adversary



b?

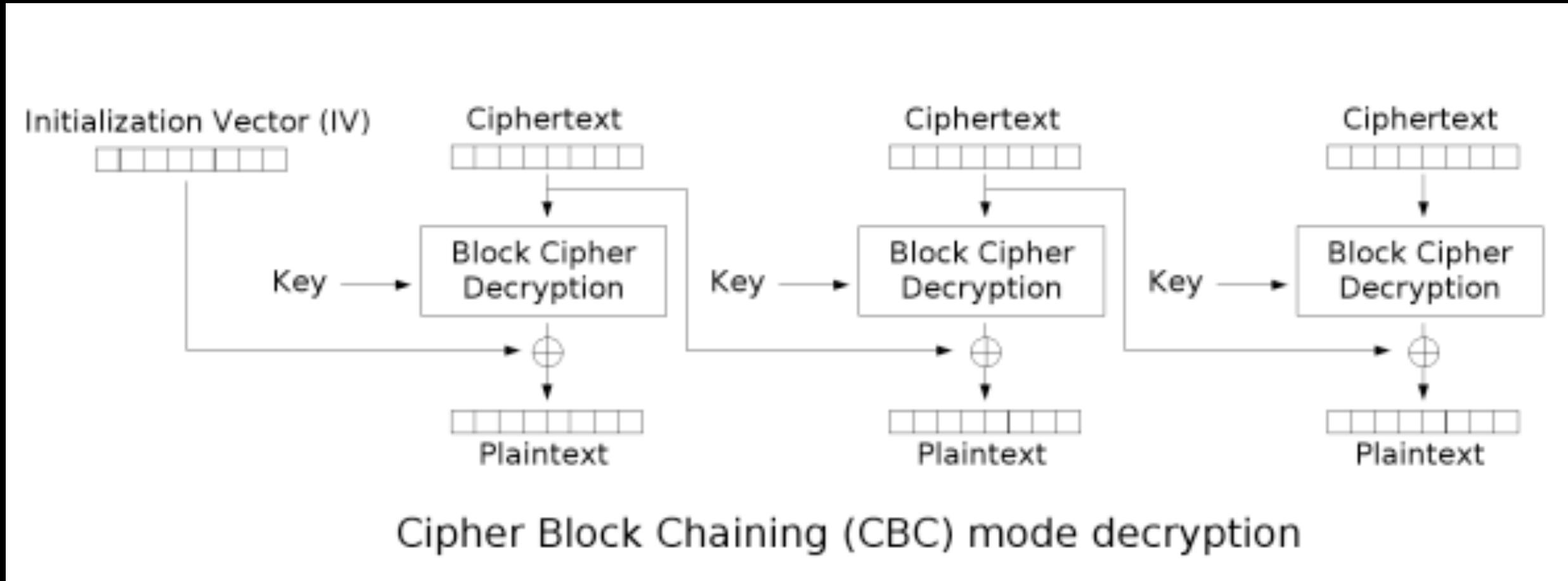
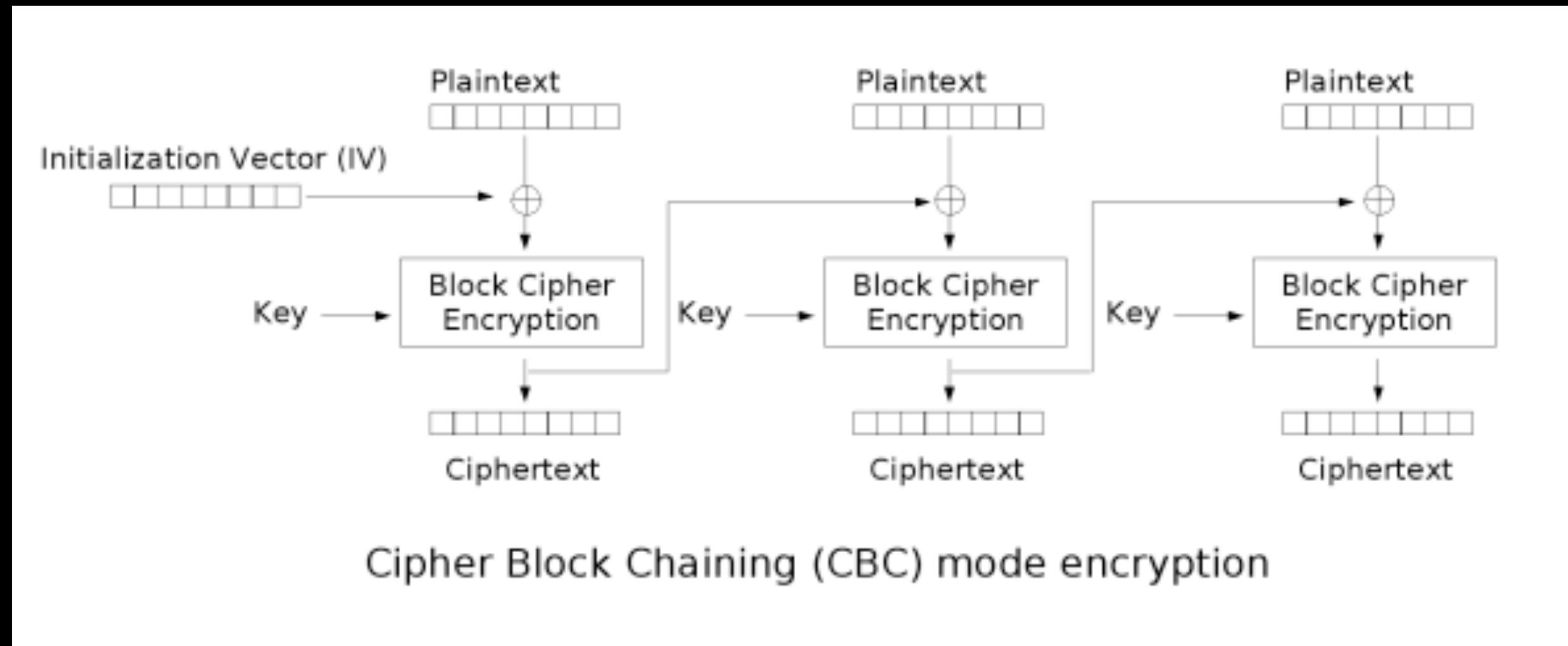


k

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



Security of CBC

- Is CBC a secure encryption scheme?
 - Yes, assuming a secure block cipher
 - Correct (random) IV generation
 - Can prove 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!

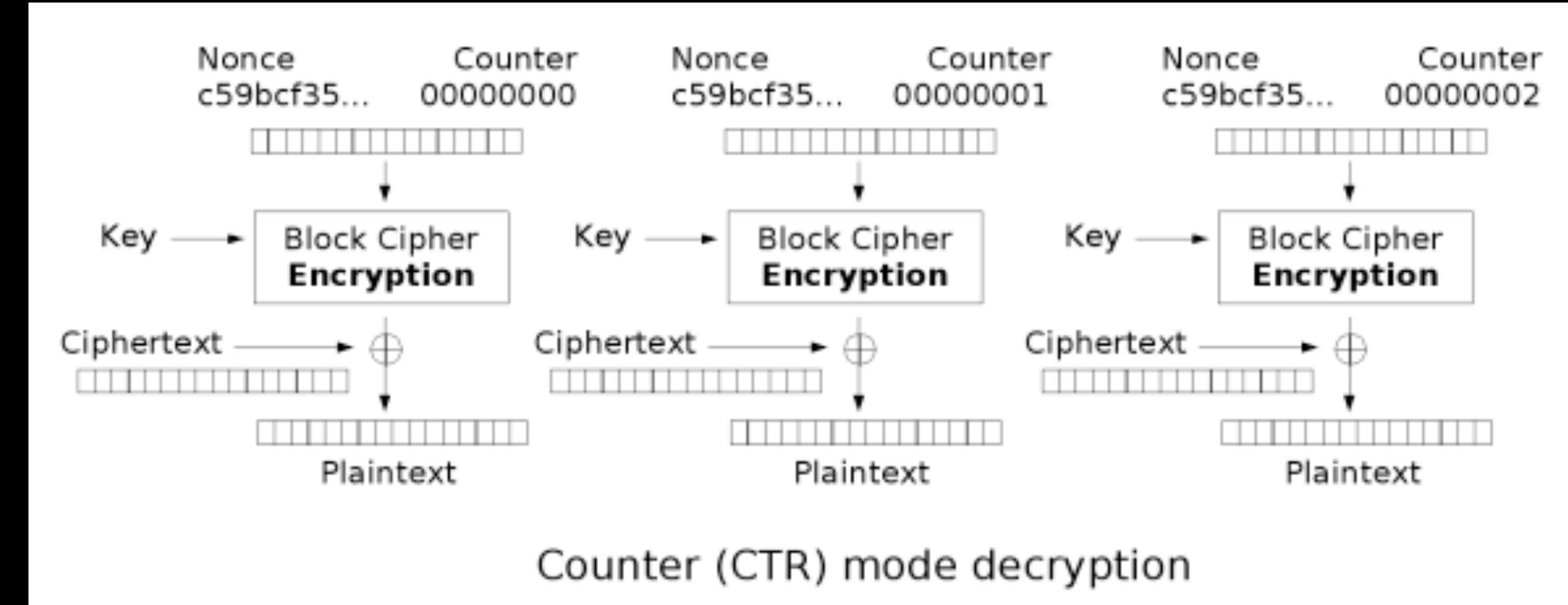
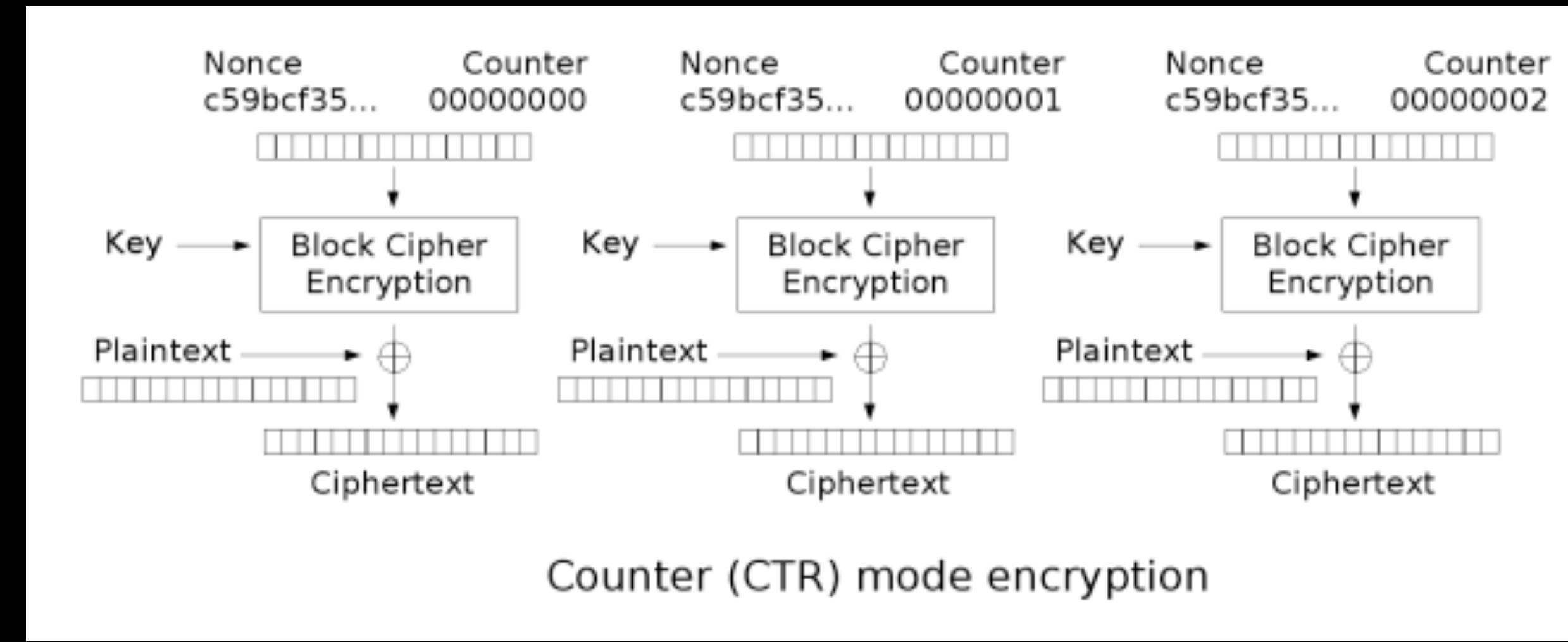
The size of the frame of data to be encrypted or decrypted (i.e. how often a new CBC chain is started) depends on the particular application, and is defined for each in the corresponding format specific books of this specification. Unless otherwise specified, the Initialization Vector used at the beginning of a CBC encryption or decryption chain is a constant, iv_0 , which is:

0BA0F8DDFEA61FB3D8DF9F566A050F78₁₆

Advanced Access Content System (AACS)

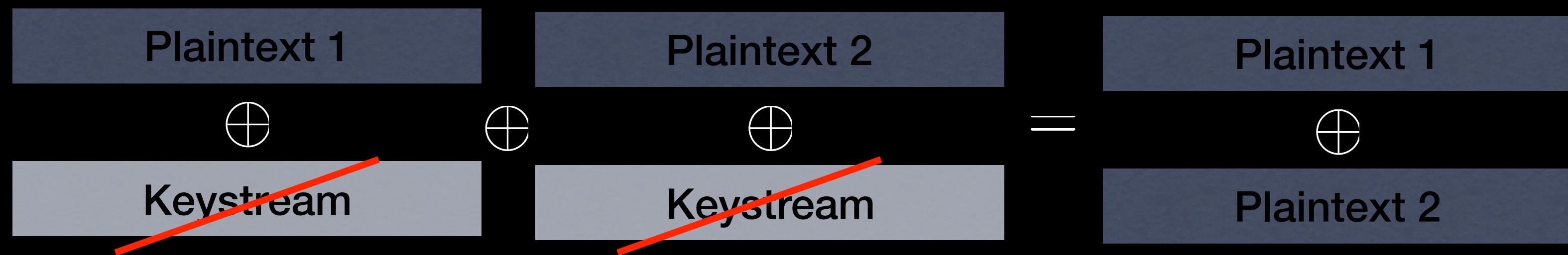
*Introduction and
Common Cryptographic Elements*

CTR Mode



Security of CTR

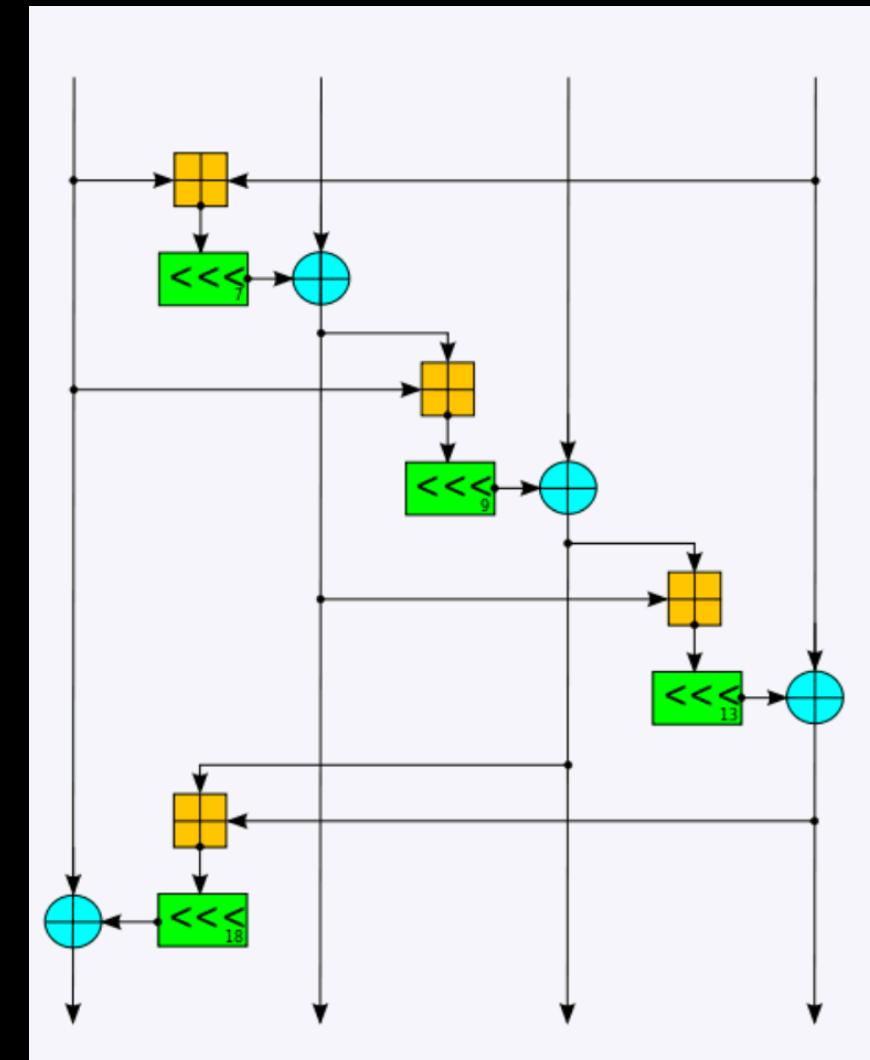
- Yes, assuming secure block cipher (PRP)
- However, counter range must never be re-used



- 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
 - $\text{Salsa20}(k, n) \rightarrow \{\text{output}\}$
 - Can use these to implement a stream cipher (i.e. CTR mode)



Point of order

- Proofs of security:
 - We don't know how to prove that DES or AES or Salsa20 are secure block ciphers
 - But if we assume that the block ciphers are 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

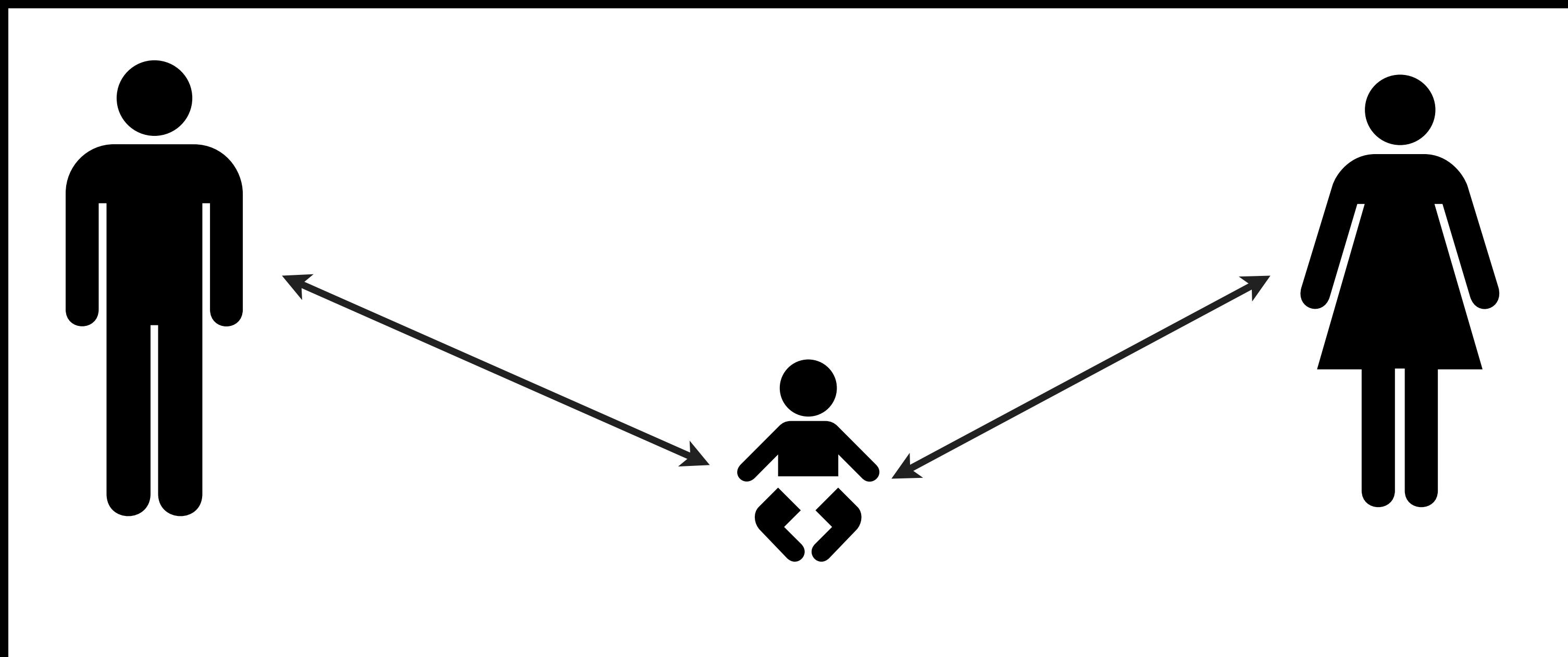
- Proofs of security for ChaCha20 and ChaCha20-Poly, showing that they are secure if the underlying block cipher is a PRP.
- We can prove that CBC & CTR & OFB & CFB etc. are secure encryption modes.
- We can prove that ChaCha20-Poly is a secure block cipher, achieving one round fewer: for 256 bits ChaCha6 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]
- But if we assume that the block ciphers are secure PRPs (resp PRFs) then:

<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 then 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:
 - Generic composition
Encrypt (e.g., CBC mode) then MAC
- two different keys, multiple primitives
 - Authenticated mode of operation
- Integrates both encryption & authentication
- Single key, typically uses only one primitive (e.g., block cipher)
- Ex: CCM, OCB, GCM modes

