

**601.445/600.454**

**Practical Cryptographic**

**Systems**

**Symmetric Cryptography**

**Instructor: Matthew Green**

# Housekeeping

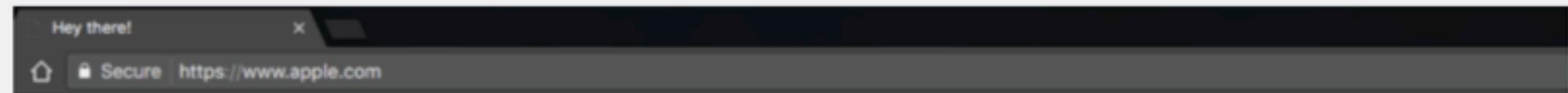
- Syllabus updated
  - <https://github.com/matthewdgreen/practicalcrypto/wiki>
  - Slides up as we go (<https://github.com/matthewdgreen/practicalcrypto>)
  - Reading assignment today (for Weds)  
Anderson chap 5.7
  - Office Hours Weds 2-3:30pm \*\*
  - Assignment 1 out last week

*ALWAYS PRONOUNCED YOU ARE ELL —*

# Google wants to get rid of URLs but doesn't know what to use instead

Their complexity makes them a security hazard; their ubiquity makes replacement nigh impossible.

PETER BRIGHT - 9/5/2018, 10:04 AM



## Hey there!

This may or may not be the site you are looking for! This site is obviously not affiliated with Apple, but rather a demonstration of a flaw in the way unicode domains are handled in browsers.

[See what this is about](#)

The New York Times

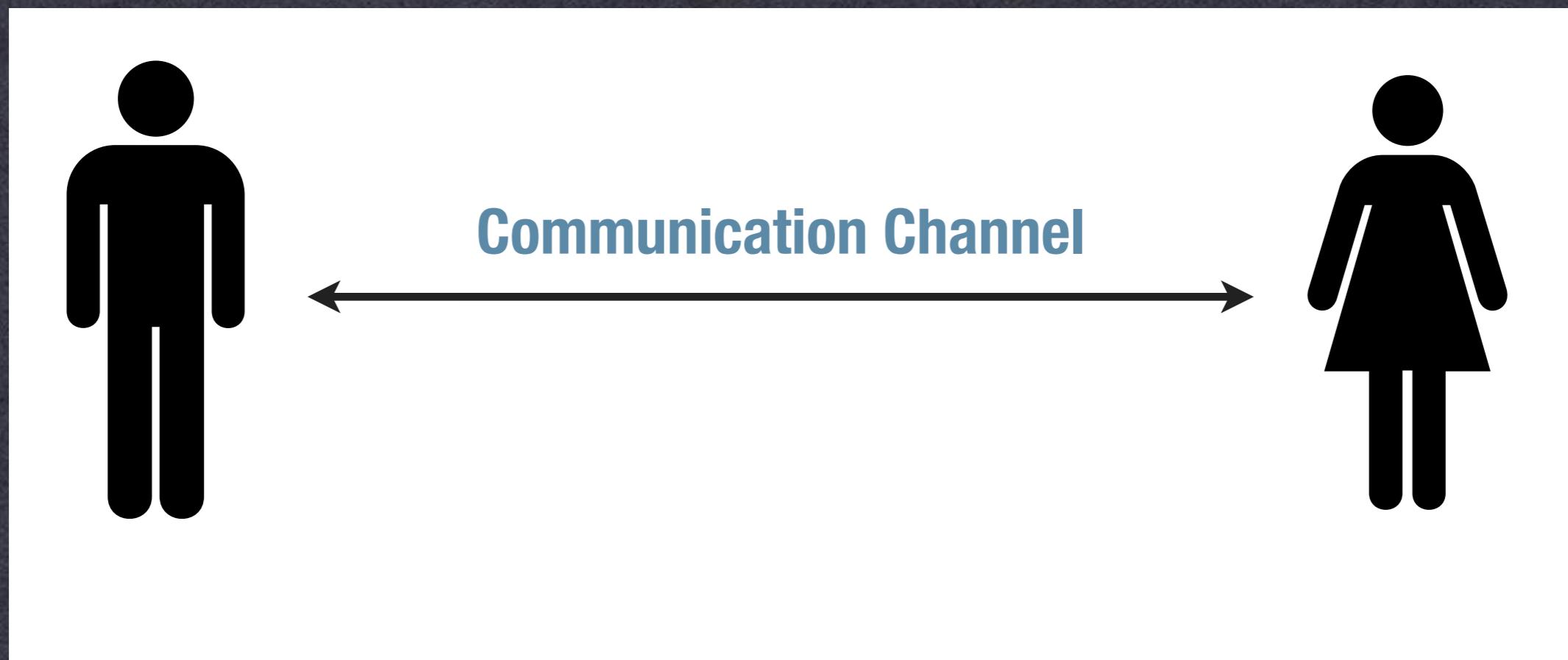
# *'Five Eyes' Nations Quietly Demand Government Access to Encrypted Data*



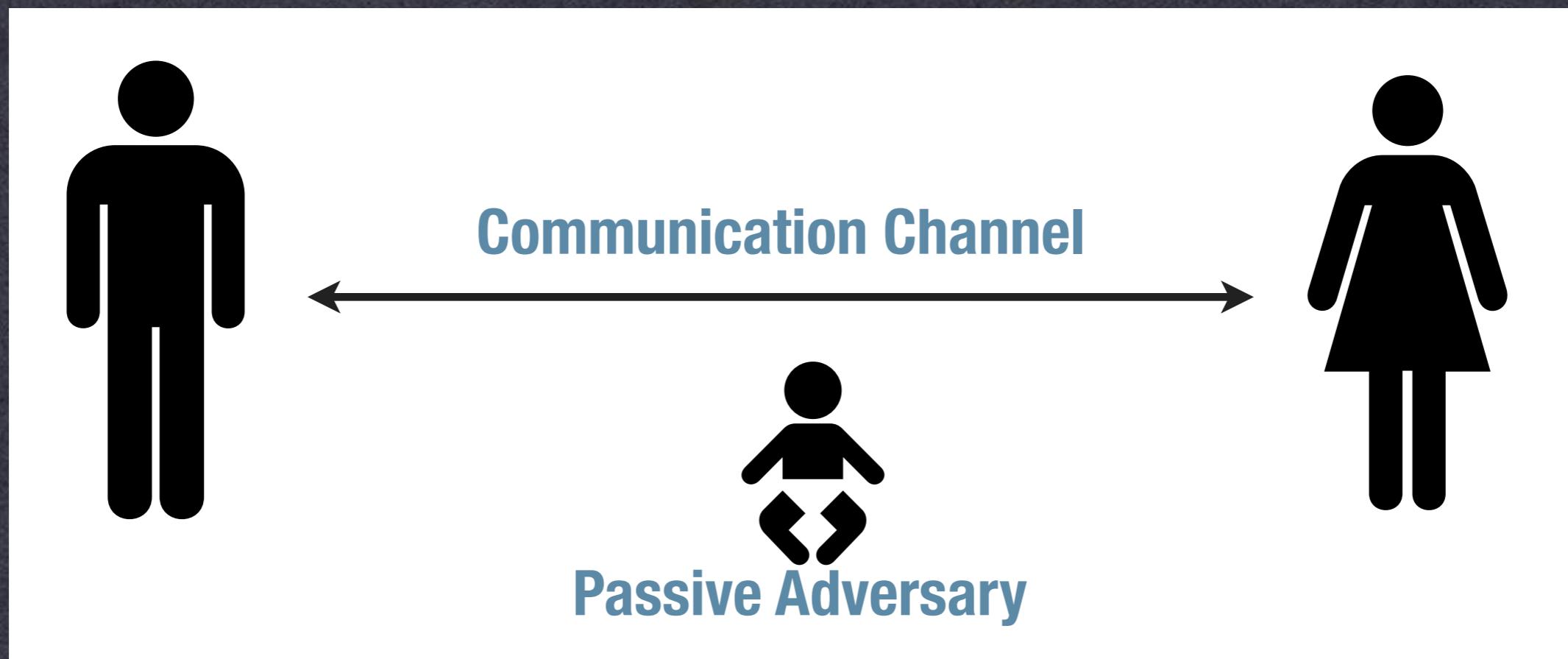
# Review

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

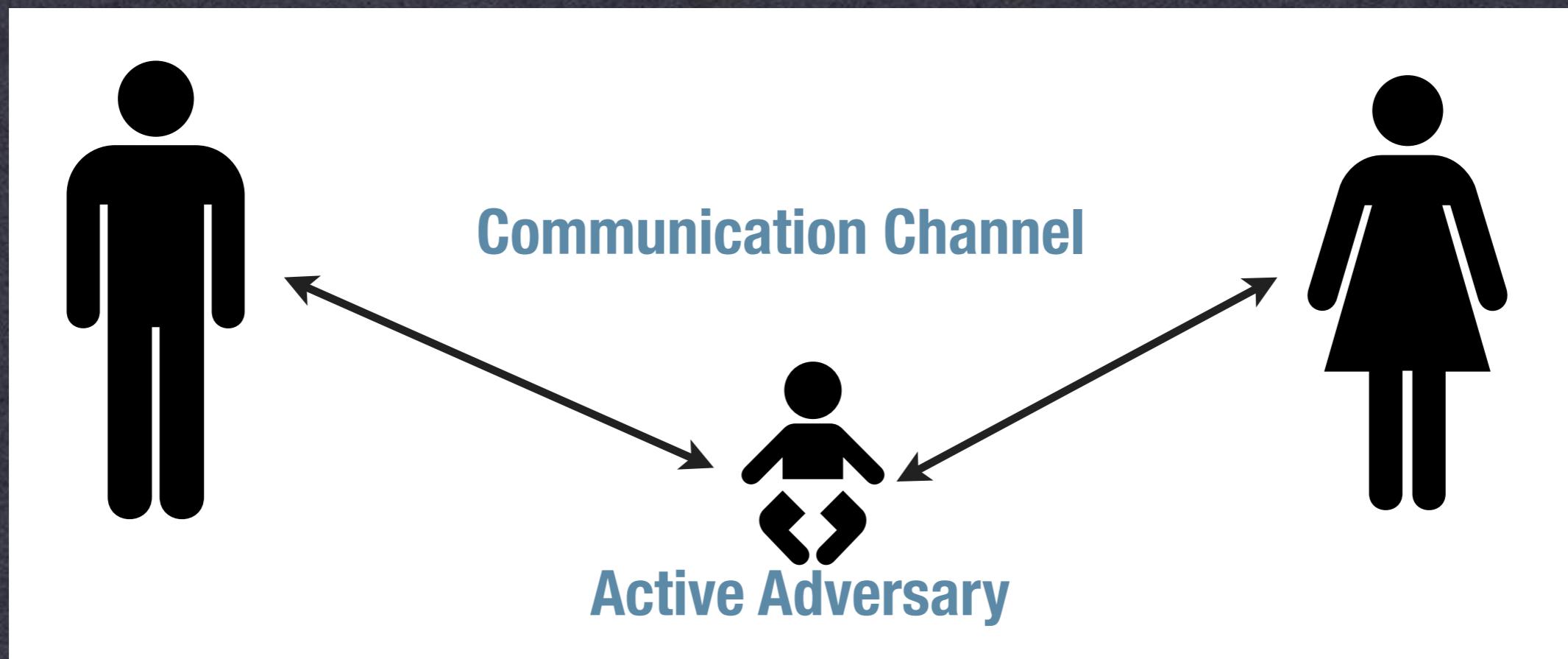
# Communication Model



# 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

Time

The diagram illustrates the historical progression of encryption methods over time. A horizontal arrow points from left to right, labeled 'Time' above it. Five rectangular boxes are arranged along this timeline, each containing a category of encryption:

- Classical Ciphers / Codes
- Mechanical Ciphers
- Modern Crypto
- Symmetric Crypto
- Public Key Crypto
- One-Time Ciphers

The 'Modern Crypto' box is positioned above the 'Symmetric Crypto' and 'Public Key Crypto' boxes, indicating its historical context relative to them.

Classical  
Ciphers / Codes

Mechanical  
Ciphers

Modern Crypto

Symmetric  
Crypto

Public Key  
Crypto

One-Time Ciphers

# 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 K	L C F O
[ ] [ ] [ ] [ ] [ ]	[ ] [ ]	[ ] [ ]	[ ] [ ] [ ] [ ]	[ ] [ ] [ ]	[ ] [ ] [ ]	[ ] [ ] [ ]	[ ] [ ]	[ ] [ ] [ ] [ ]
F E P	F J	Y P	.	- K F C Y H	K M U			
[ ] [ ] [ ] [ ]	[ ] [ ]	[ ] [ ]	.	- [ ] [ ] [ ] [ ]	[ ] [ ] [ ]			

βοραίσσωνται // σημιαώνεται φάλαγξ 341 ε 1108 η απόφθασ  
ανθράκων καταπέλτης οφεγαλεύθερος φοντούρα παλα  
οφεγανταρνούσαντη μηχανή διασφέντης πολεμάνεται  
μεριγμένης + βραχιόνων φρίσονας αγριότερης από την περιοχή  
από την πολιορκία της Ηονίας Χειρεύσιου σφίλου γαν  
καταστρατηγός φαντα 1108 η απόφθασ η απόφθασ  
η γαλανοφάσια φάσια φέρεται

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

Н Е Р > 9 Л В У Р К 1 0 Л Т 6 0  
N 9 + B φ ■ O ■ D W Y . < □ K F 0  
B Y I Z M + 4 Z G W φ ■ L ■ □ H J  
S 9 9 A L U □ V 0 9 0 + + R K E  
□ A M + □ T D I ● F P + P e K /  
9 □ R A F L O - □ O C □ F > □ D ♦  
■ 0 + K D ■ E 0 4 C X G V . □ L I  
φ 6 0 3 7 T ■ O + D N Y ♦ + □ L A  
D < M + B + Z R 0 F B C K A O 0 K  
- □ U V + A J + 0 9 A < F B Y -  
U + R / 0 1 E I D Y B 9 8 T M K O  
0 < C L R J I □ 0 T 0 M . + P B F  
♦ 0 A S X ■ + N I ● F B C ♦ E □ R  
L G F N A 7 0 0 0 B . C V 0 T + +  
Y B X 0 ■ E 0 4 C E > V U Z 0 - +  
I D . 0 4 B K φ 0 9 A . 7 M 0 6 0  
R C T + L 0 0 C < + F J W B I □ L  
+ □ W C ♦ W D P O S H T / φ 0 9  
I F D K W < D T B D Y 0 B ■ - C  
> M D H N 9 S □ Z O A A I K E +





# 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

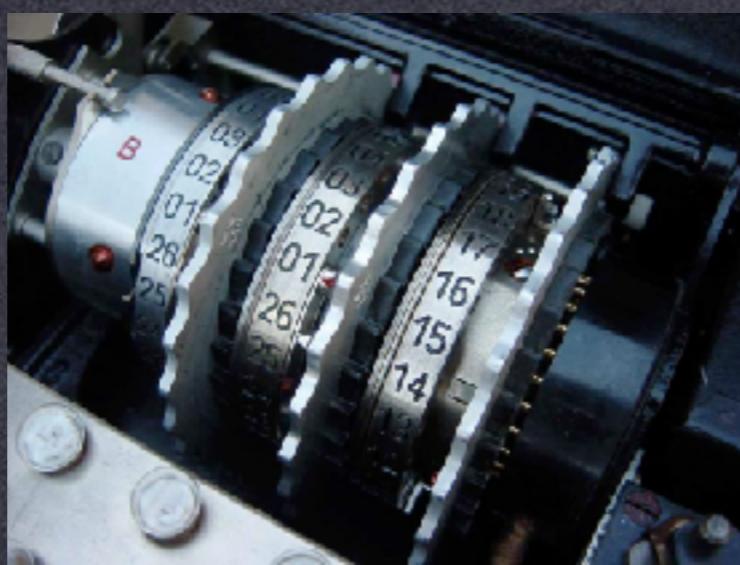
- 1900s
  - Vernam & Mauborgne's "Unbreakable" cipher
    - Based on Baudot code for Teletypes
    - Added (XORed) a random Key (sequence of bits) to a binary message
      - Perfectly secure, provided:
        - key is perfectly random
        - key is at least as long as the message
        - key is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

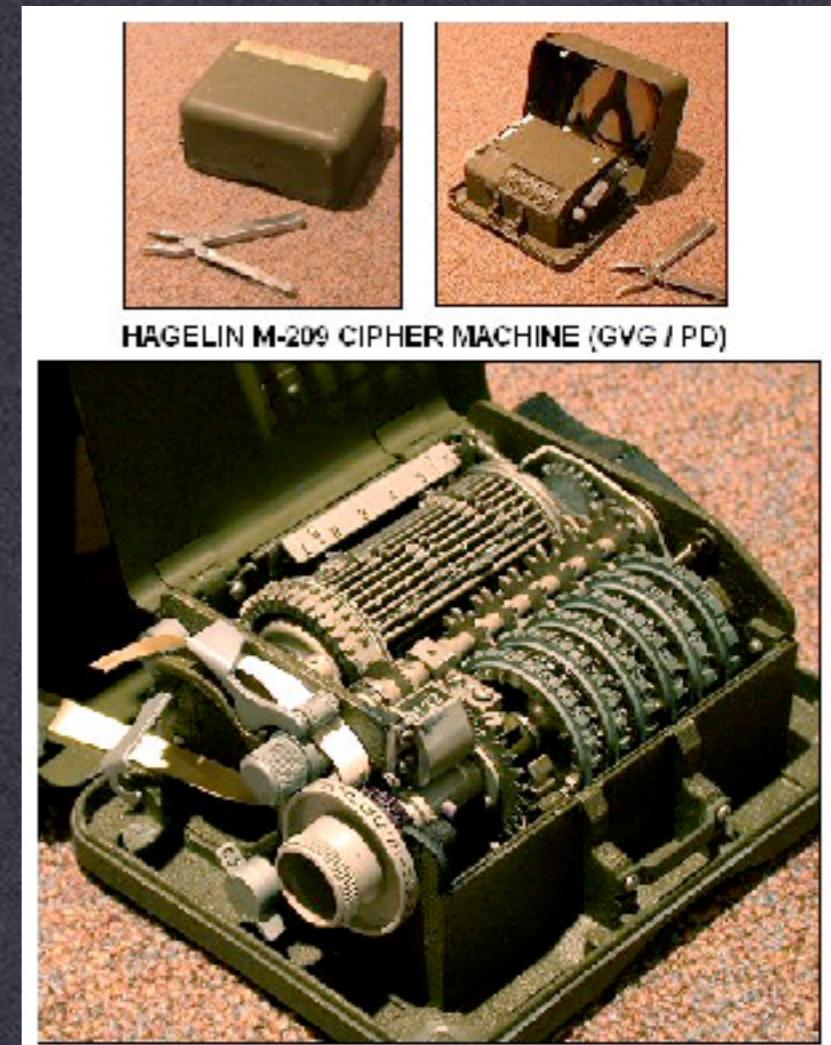


# Mechanical Cryptography

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

Increasing  
Complexity





HAGELIN M-209 CIPHER MACHINE (GVG / PD)

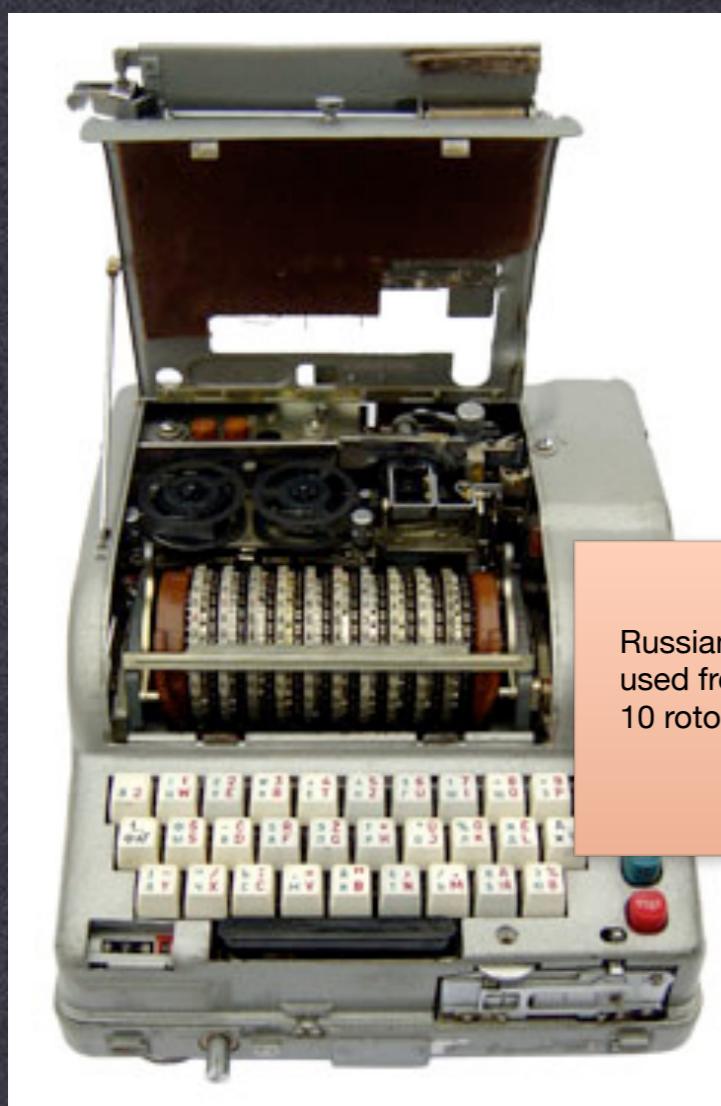
US M-209, broken by  
Germans in 1943 but still used



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 =  $2^{41}$



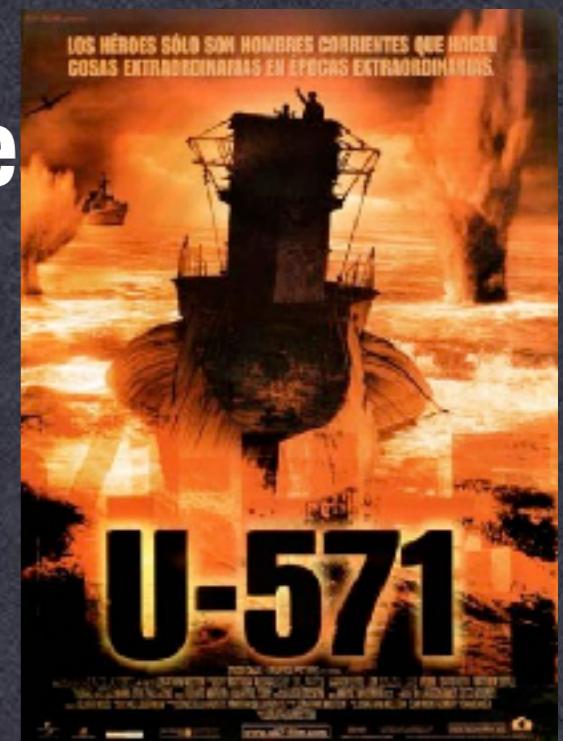
Russian Fialka  
used from 1965-1990s  
10 rotors, reads and writes to



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.

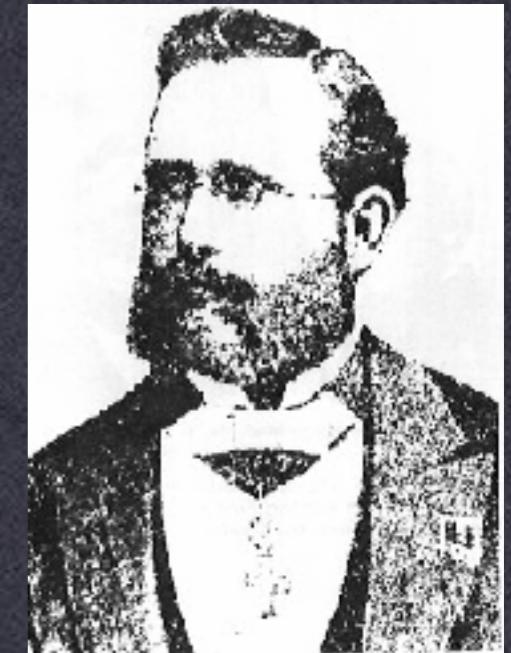
# Summary

- 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 procedure
  - 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

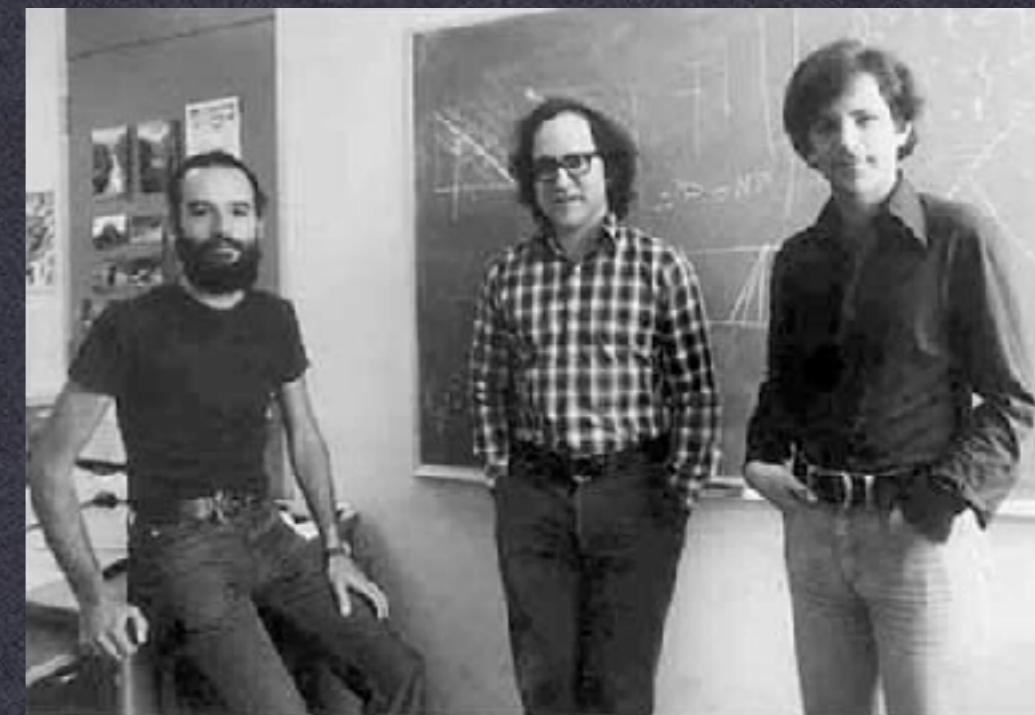


1972



1976

(1974) ← U.K. GCHQ → (1973)



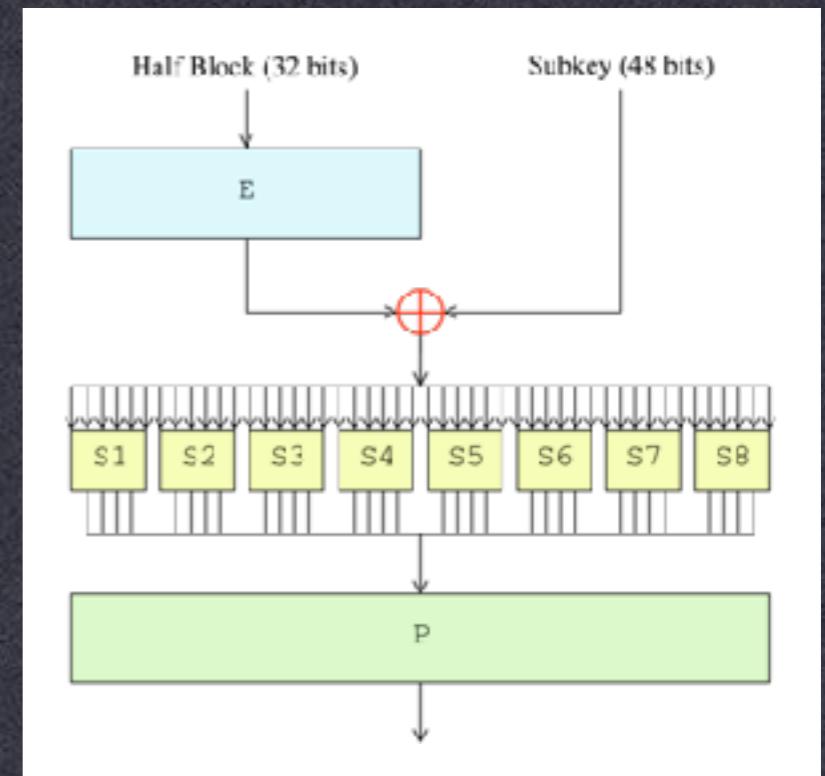
1977

# The Implications

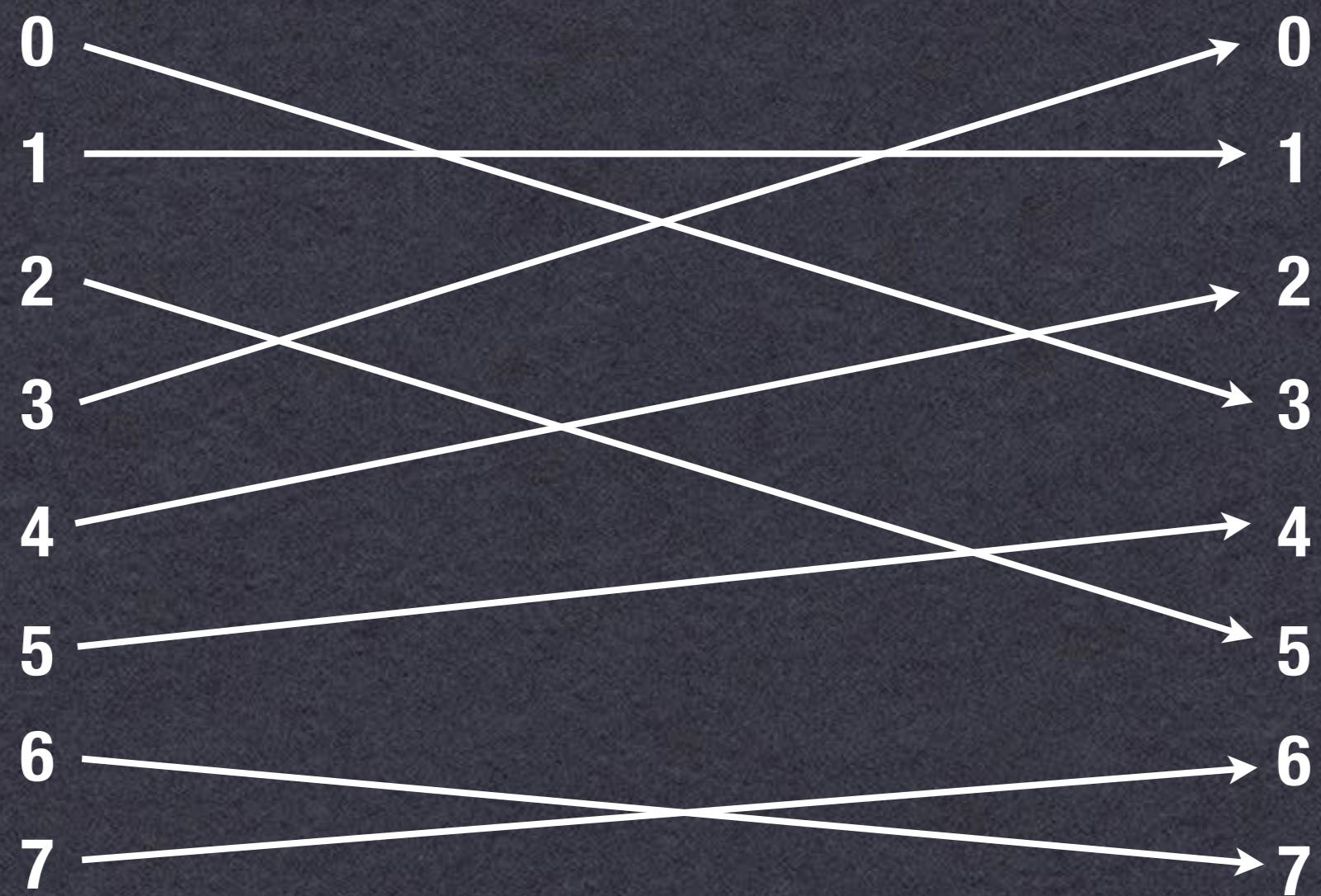
- Exponential increase in study & usage of cryptography in industry, academia
- Wide-scale deployment of cryptographic systems
- Provable Security
  - Cryptographic Systems can be reduced to some hard mathematical problem

# Data Encryption Standard

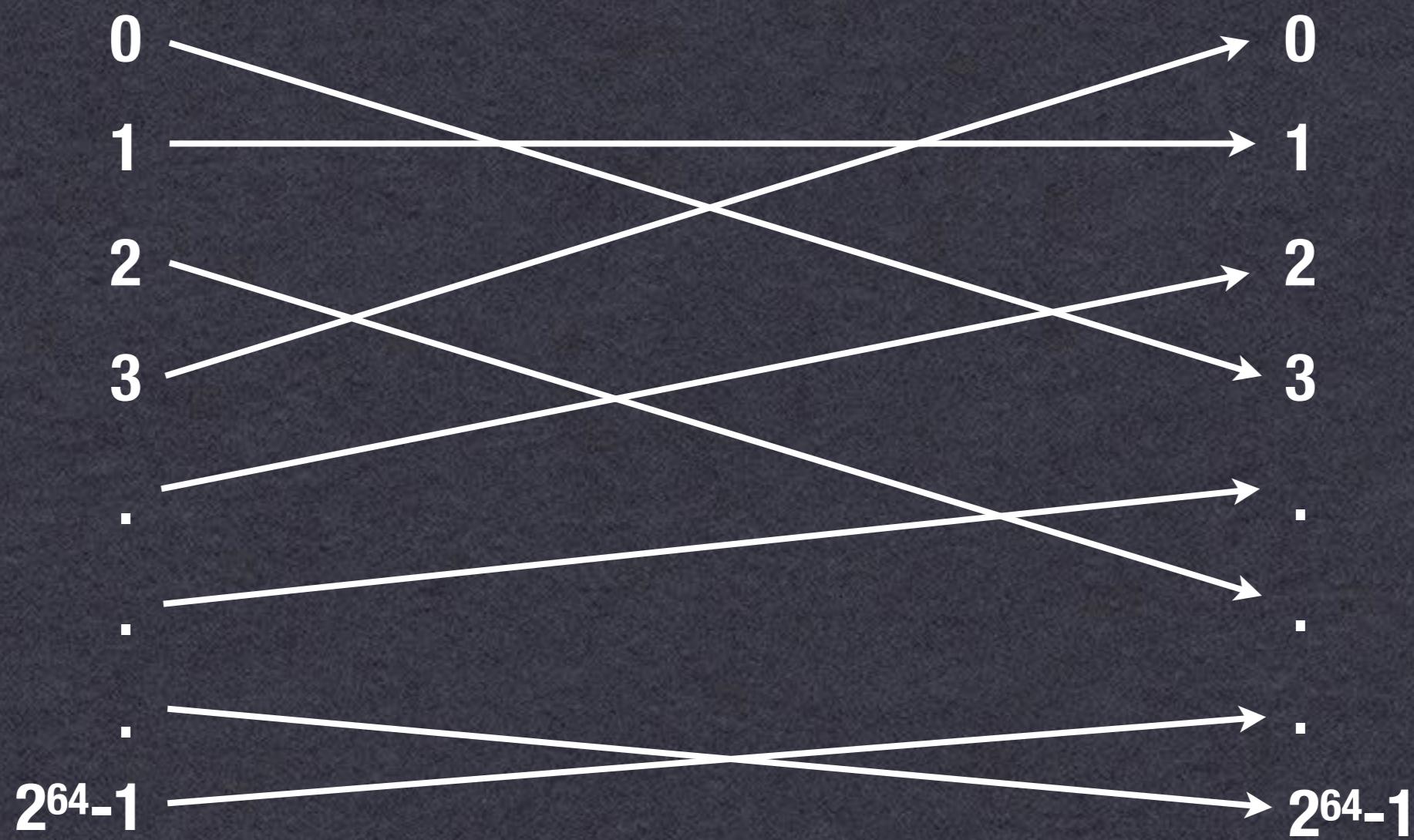
- Commercial-grade Block Cipher
  - 64-bit block size
  - 56 bit key (+ 8 bits parity)
  - “Feistel Network” Construction



# 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...

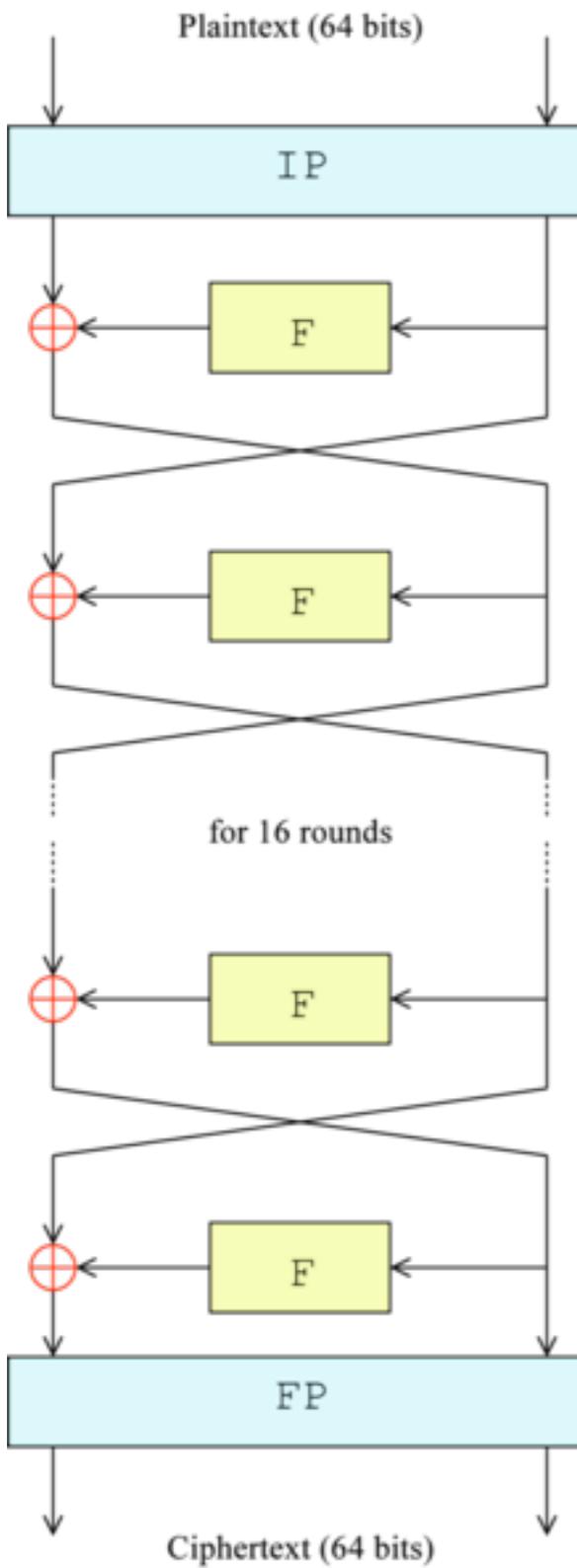
# Block Cipher

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

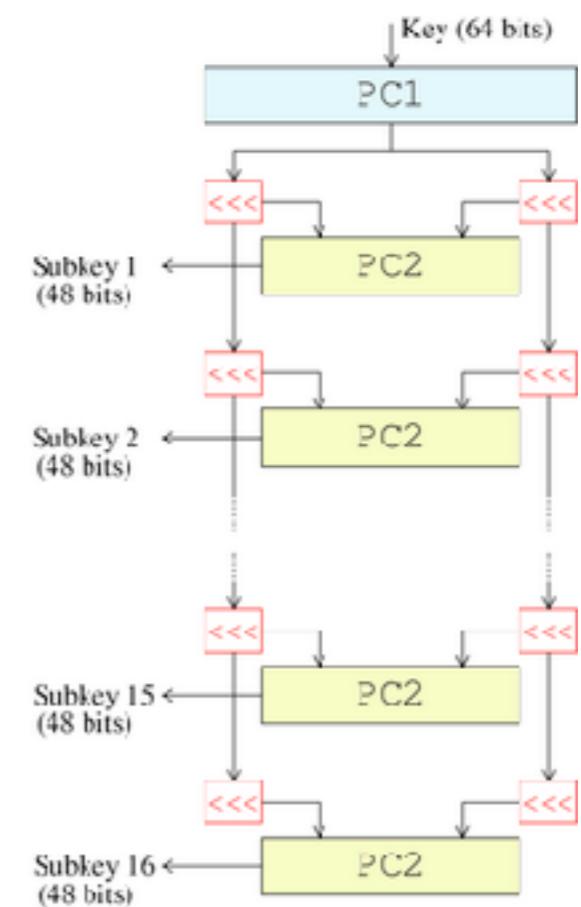
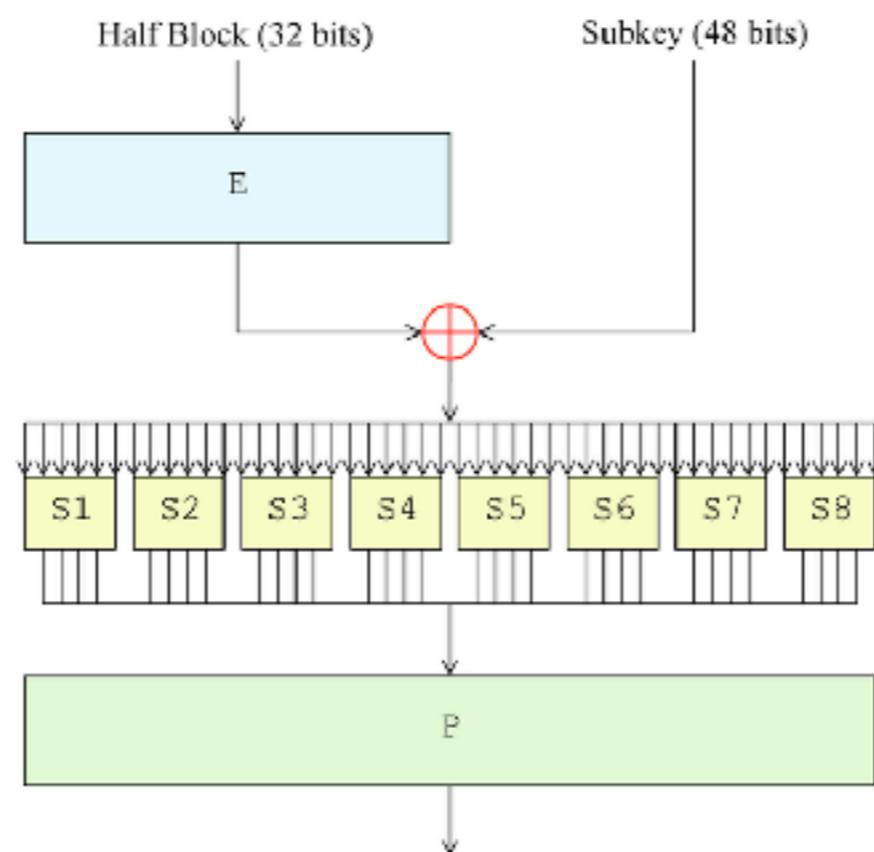
# Block Cipher

- 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)

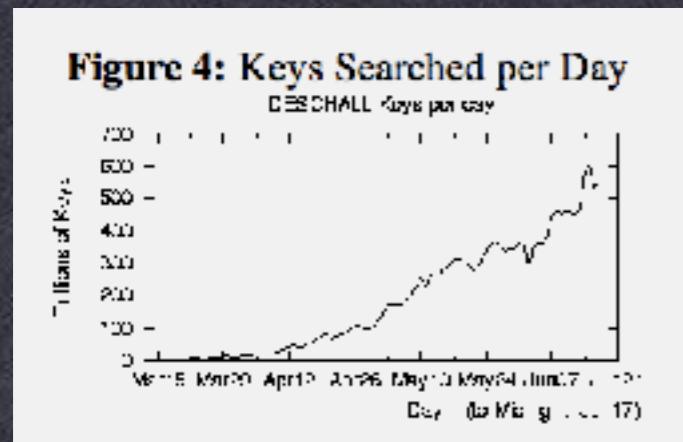


## DES: 64-bit Block, 56-bit Key



# DES

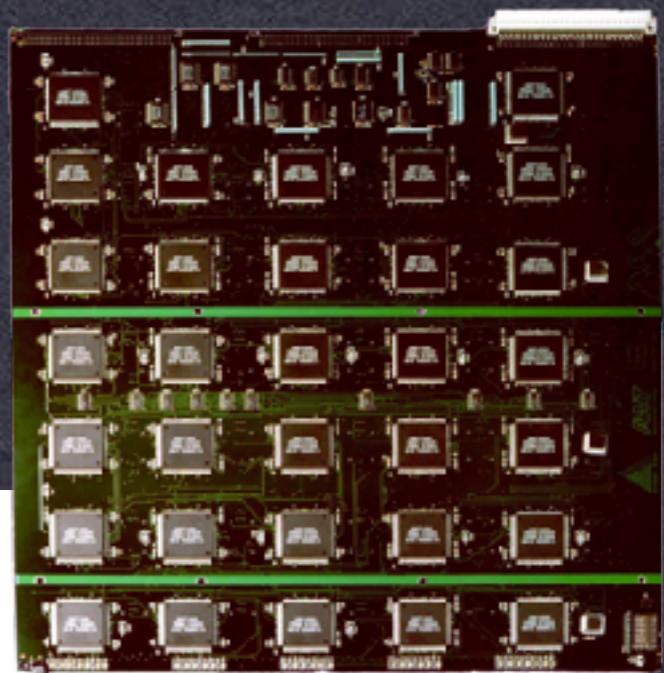
- Some “clever” attacks on DES
  - However: practical weakness = 56 bit key size
  - Practical solution: 3DES (now being deprecated)



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

By JOHN MARKOFF

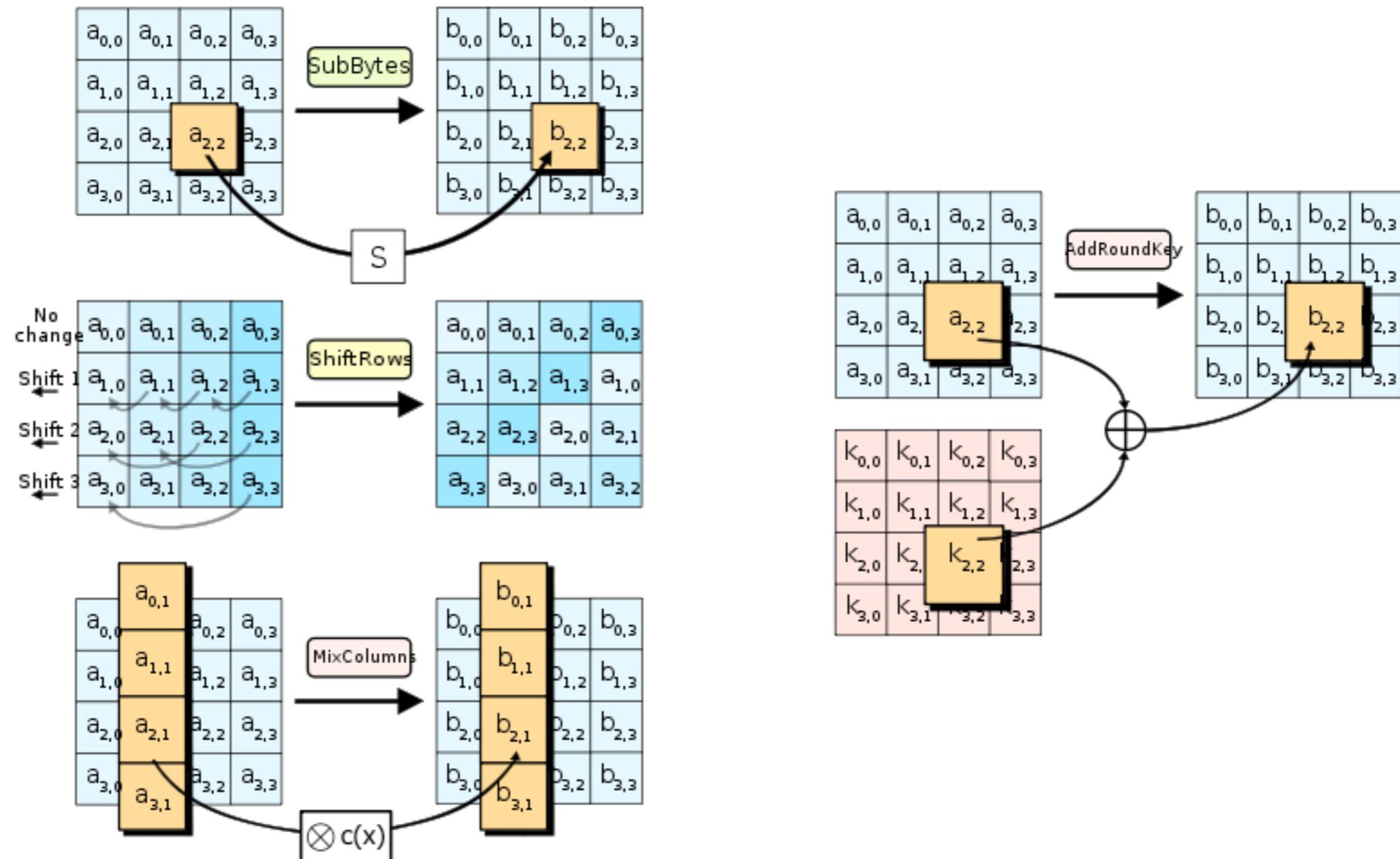
**S**AN FRANCISCO -- In a 1990s variant of a John Henry-style competition between man and machine, researchers using a homemade supercomputer have cracked the government's standard data-scrambling code in record time -- and have done it by out-calculating a team that had harnessed thousands of computers,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

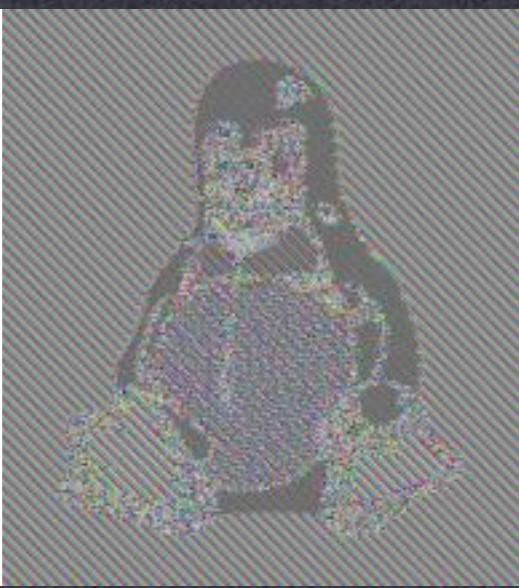
# AES: 128-bit Block, 128/192/256-bit Key



# 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

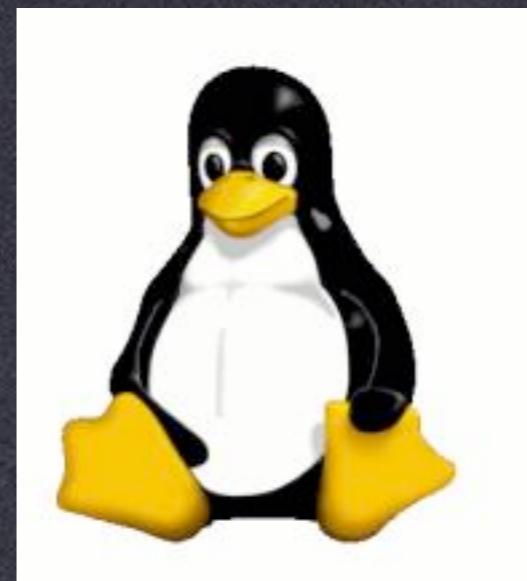
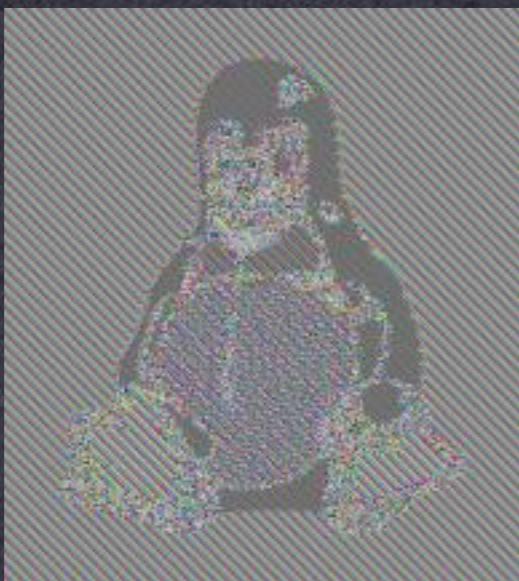
- What does it mean to securely encrypt something?

# 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 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

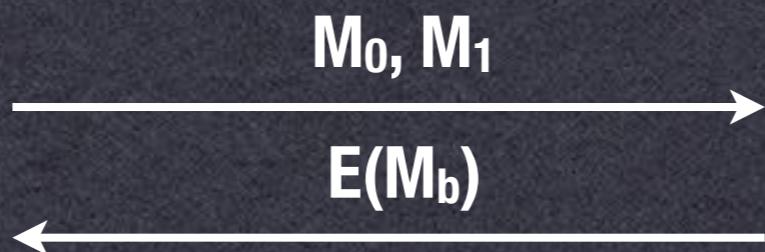
- Semantic Security (IND-CPA)

$$|M_0| = |M_1|$$



Adversary

b?



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



k

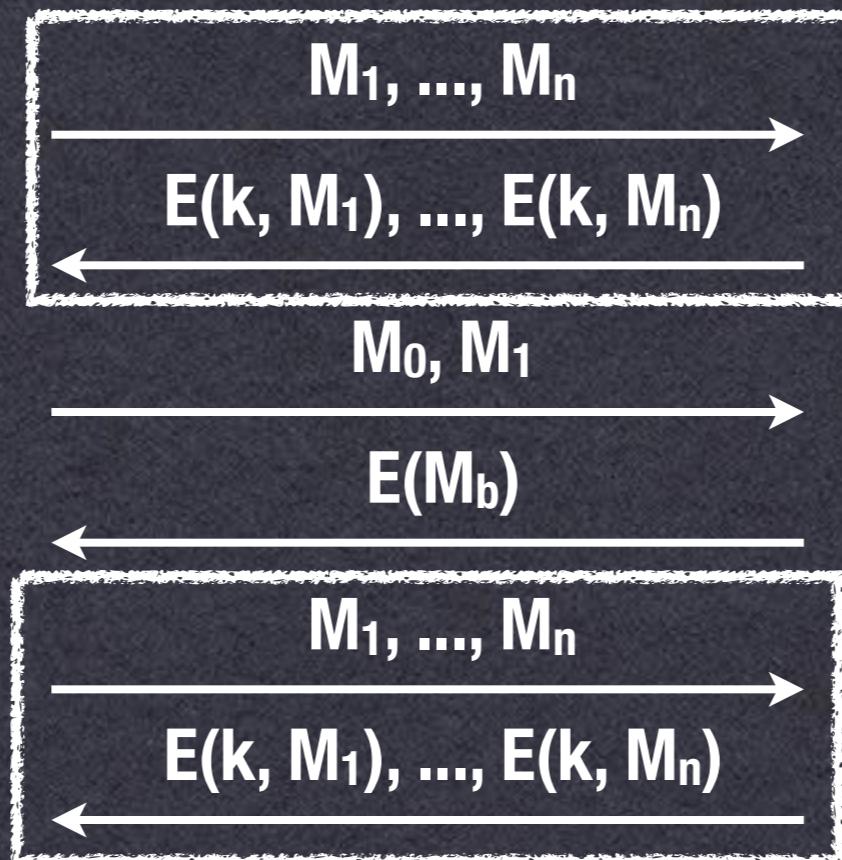
# Semantic security

- Semantic Security (IND-CPA)



Adversary

b?

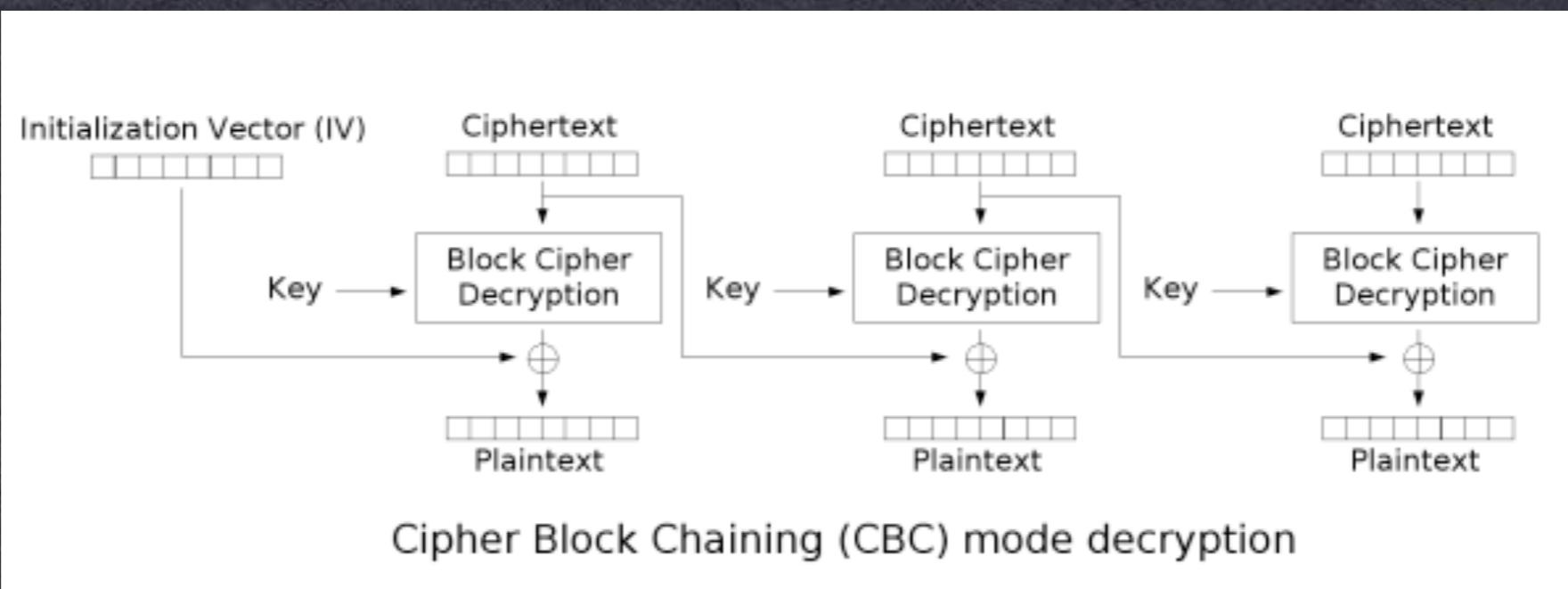
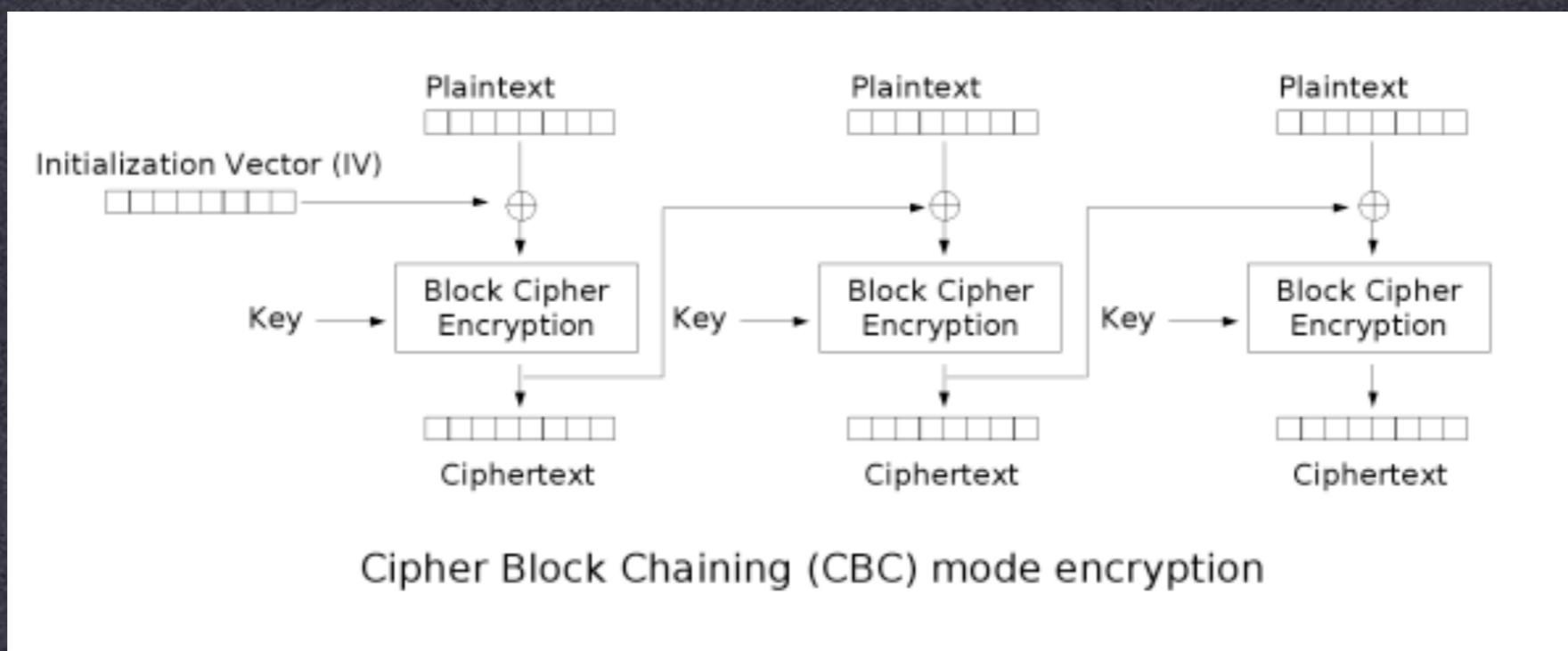


k

# 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!

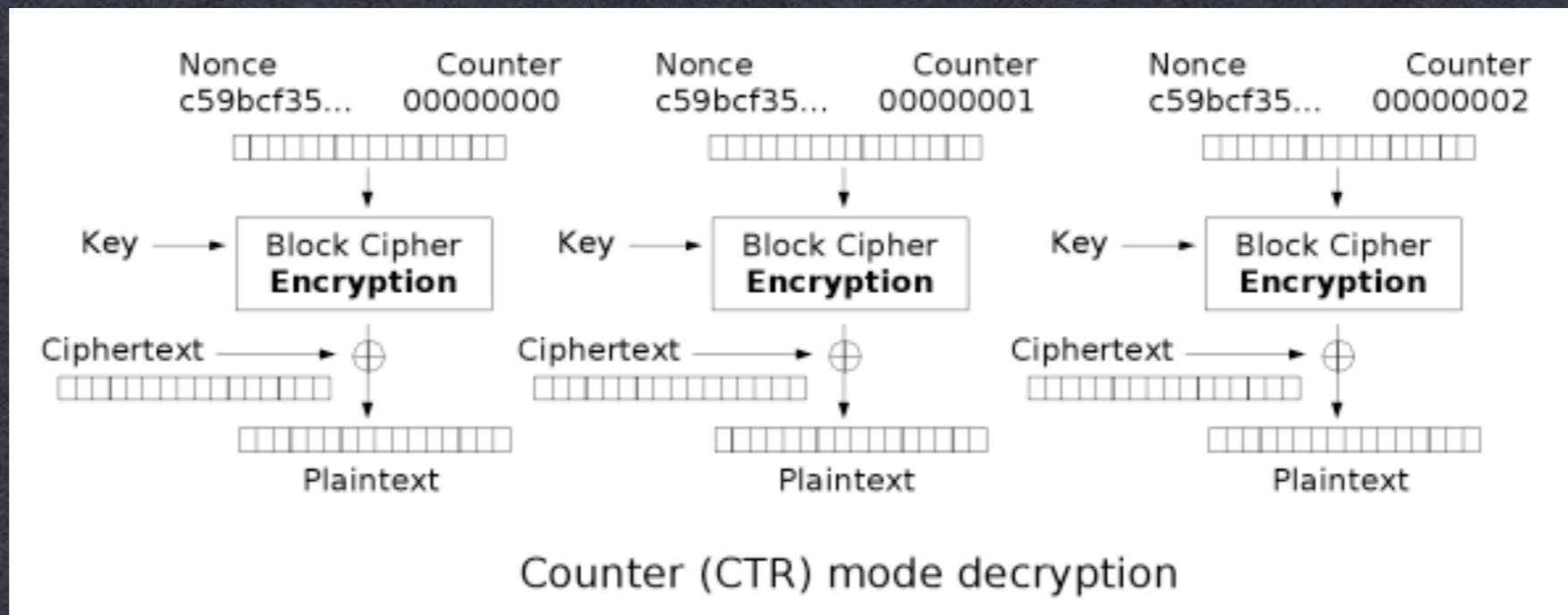
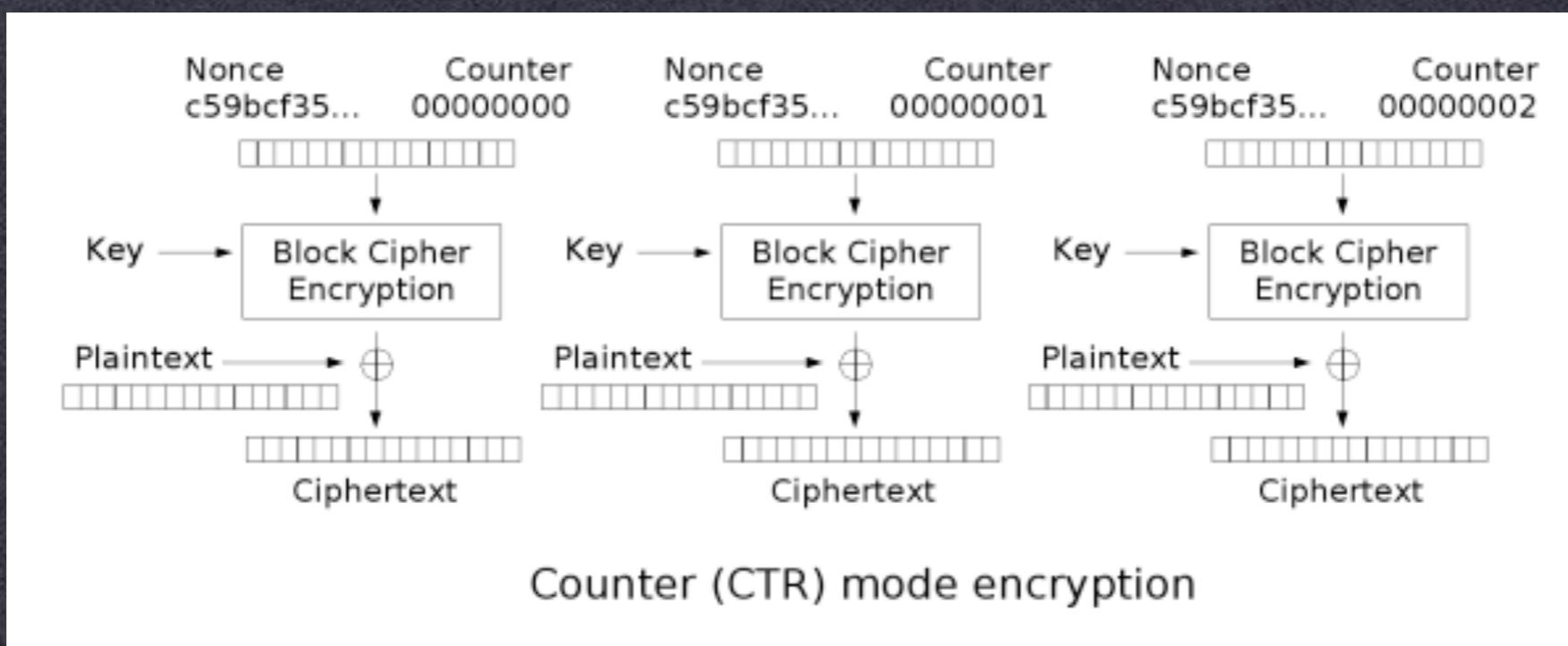
The size of the frame of data to be encrypted or decrypted (i.e. how often a new CBC chain is started) depends on the particular application, and is defined for each in the corresponding format specific books of this specification. Unless otherwise specified, the Initialization Vector used at the beginning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

0BA0F8DDFEA61FB3D8DF9F566A050F78<sub>16</sub>

## 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 reused



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

# Point of order

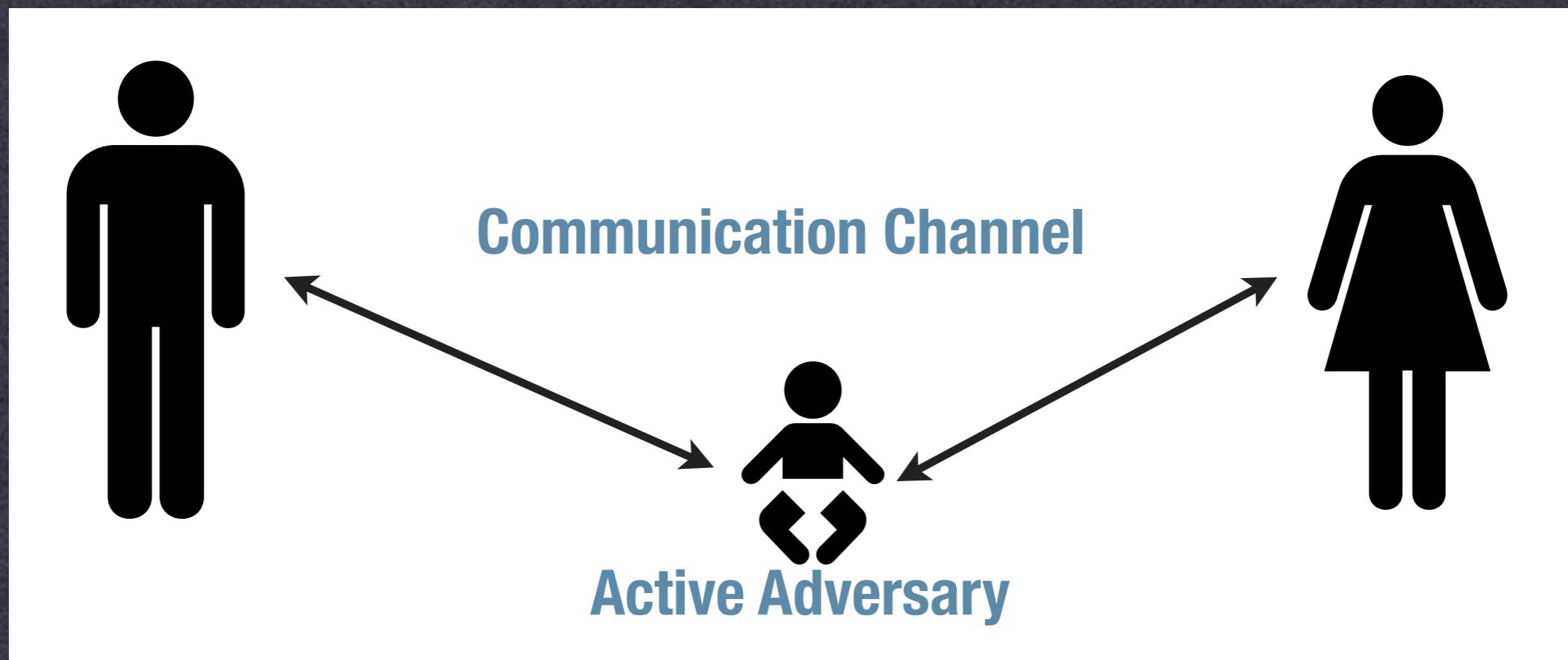
- Proofs of security:
  - We don't know how to prove that DES or AES are secure block ciphers
  - But if we assume that the block ciphers are secure PRPs then:
    - We can prove that CBC & CTR & OFB & CFB etc. are secure encryption modes.

<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 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
  - Authenticated mode of operation
  - Integrates both encryption & authentication
  - Single key, typically uses only one primitive (e.g., block cipher)
  - Ex: CCM, OCB, GCM modes

