Symmetric Cryptography
(Through the 1980s or so...)

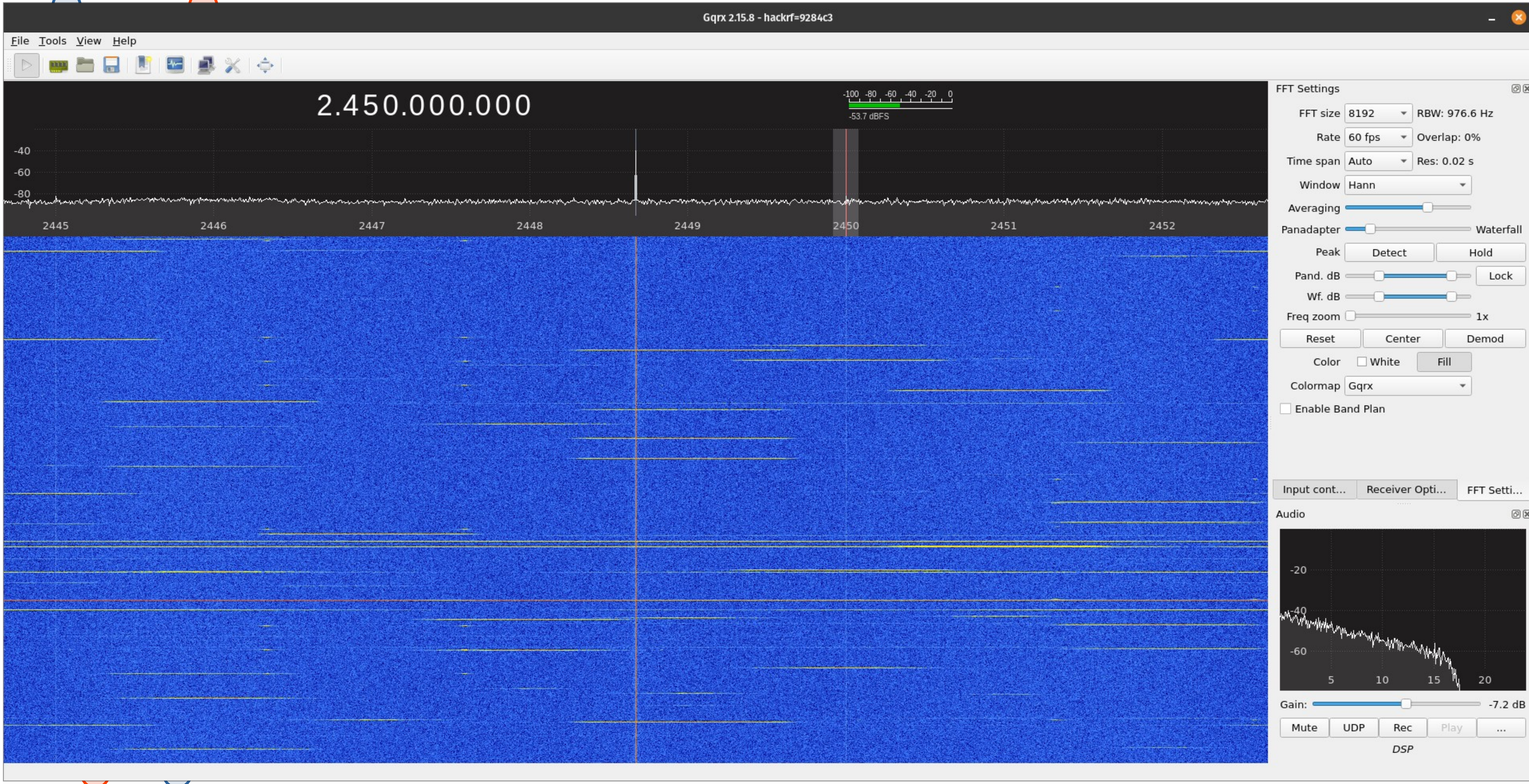
jedimaestro@asu.edu

To prepare for this lecture...

- https://www.youtube.com/watch?v=JiQz58Y67To

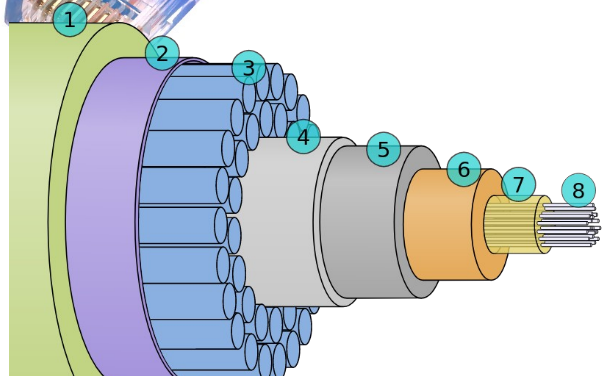
Someone... was beaming powerful wireless pulses into the theatre and they were strong enough to interfere with the projector's electric arc discharge lamp. Mentally decoding the missive, [Fleming's assistant Arthur] Blok realised it was spelling one facetious word, over and over: "Rats". A glance at the output of the nearby Morse printer confirmed this. The incoming Morse then got more personal, mocking Marconi: "There was a young fellow of Italy, who diddled the public quite prettily," it trilled. Further rude epithets - apposite lines from Shakespeare - followed.

https://www.theatlantic.com/technology/archive/2011/12/the-great-wireless-hack-of-1903/250665/


Gqrx 2.15.8 - hackrf=9284c3
File Tools View Help
2.450.000.000
-100 -80 -60 -40 -20 0
-53.7 dBFS
-40
-60
-80
2445
2446
2447
2448
2449
2450
2451
2452
FFT Settings
FFT size 8192
RBW: 976.6 Hz
Rate 60 fps
Overlap: 0%
Time span Auto
Res: 0.02 s
Window Hann
Averaging
Panadapter
Waterfall
Peak
Detect
Hold
Pand. dB
Lock
Wf. dB
Freq zoom
1x
Reset
Center
Demod
Color
White
Fill
Colormap Gqrx
Enable Band Plan
Input cont...
Receiver Opti...
FFT Setti...
Audio
-20
-40
-60
5
10
15
20
Gain:
-7.2 dB
Mute
UDP
Rec
Play
...
DSP

Internet in a nutshell...

You want to connect two machines (desktops, laptops, mobile devices, routers, embedded devices, ...)

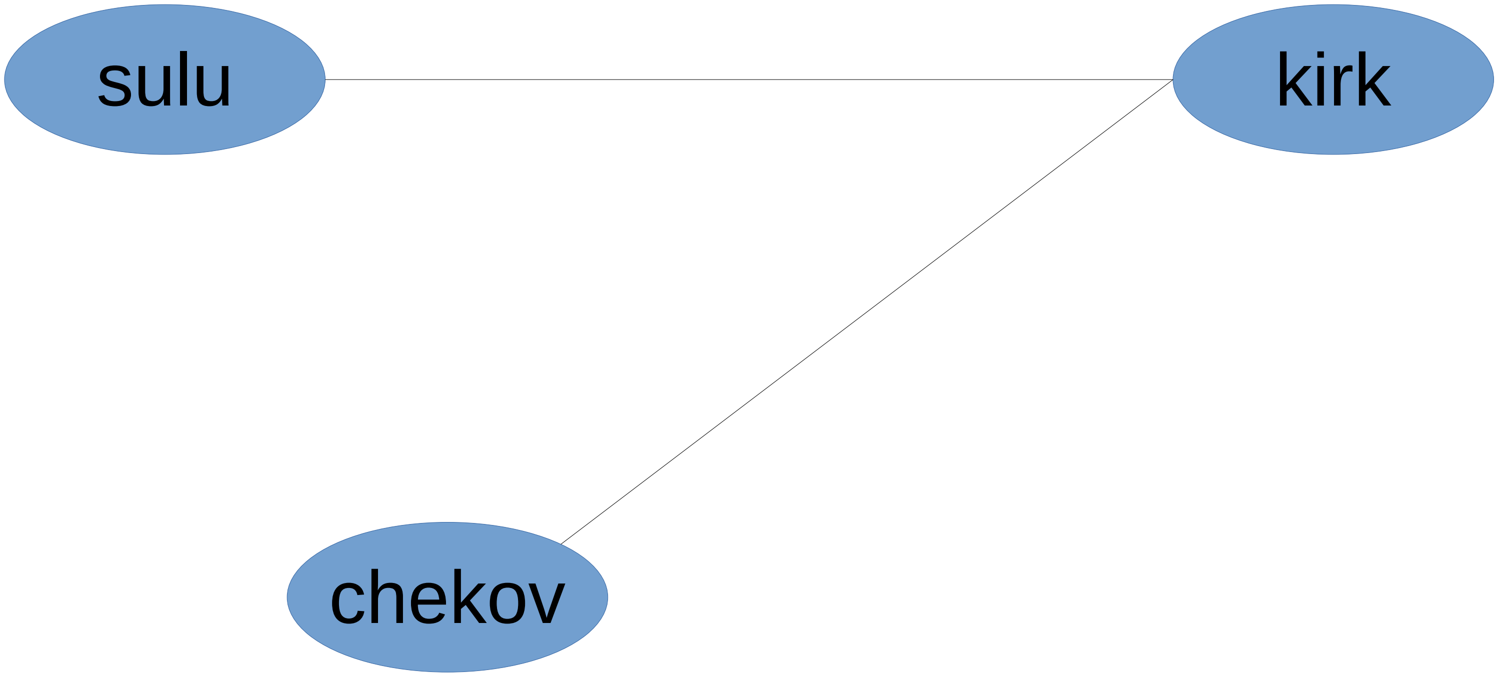


A “hop”

A “hop”

(even Ethernet is broadcast)

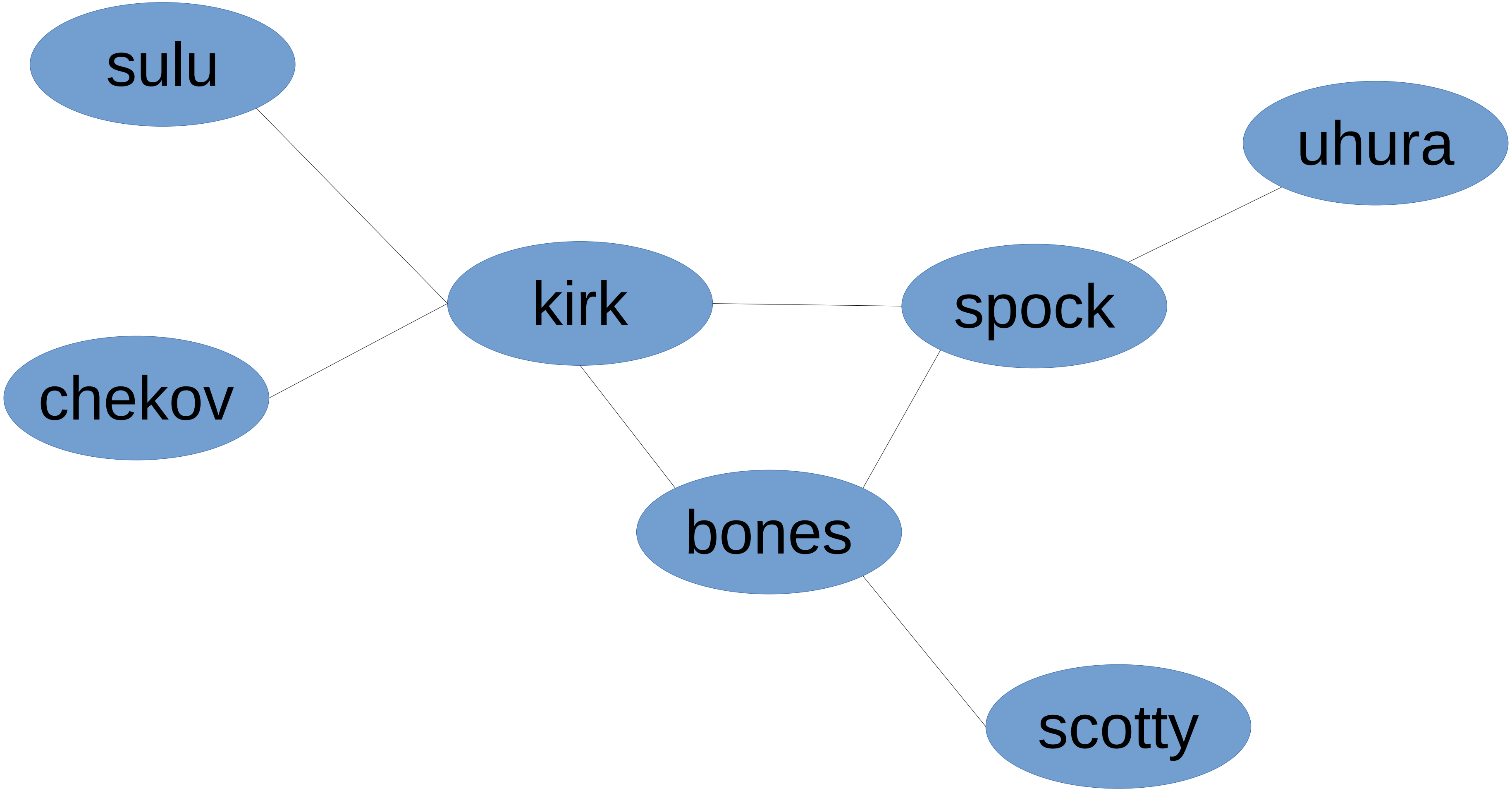
A “subnet”



A “subnet”

ARP = Address Resolution Protocol

A network with routers



More terminology

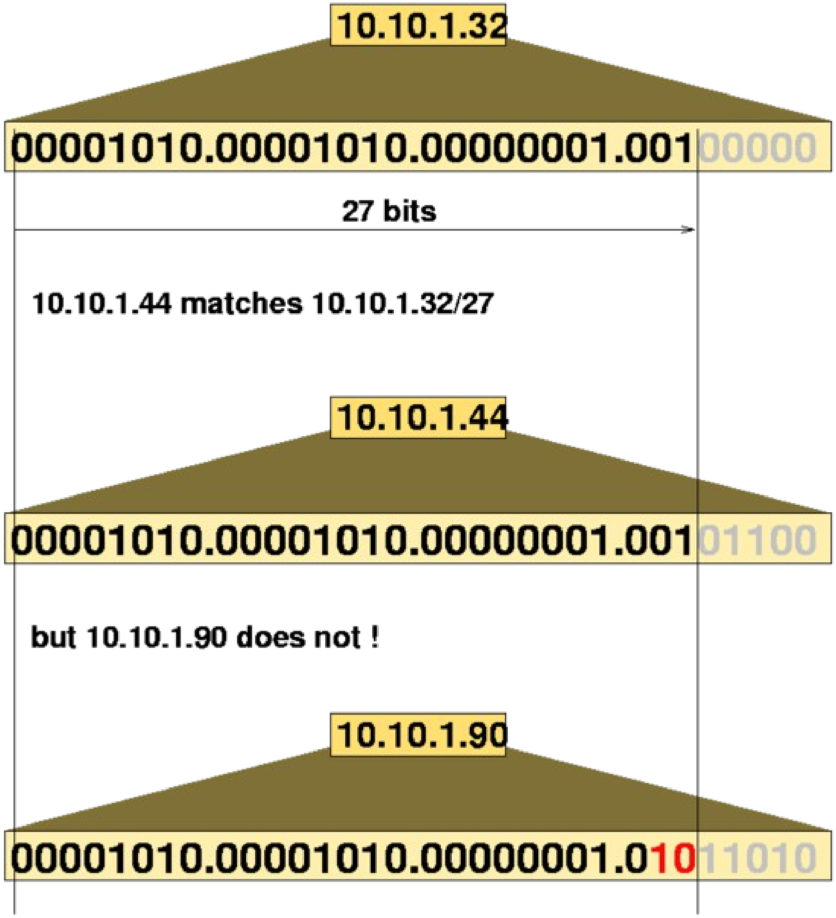
- IP = Internet protocol
- Forwarding, or “routing”
  - How packets get across the network
- Interface
  - WiFi, cellular, ...
- Path (or “route”), reverse path

IP address

- IPv4 is 32-bits, broken into 4 bytes
  - 192.168.7.8
  - 64.106.46.20
  - 8.8.8.8
- IPv6 is 128 bits
  - 2001:0db8:85a3:0000:0000:8a2e:0370:7334

CIDR

- Classless Inter-Domain Routing
- /27 has a net mask of 255.255.255.224

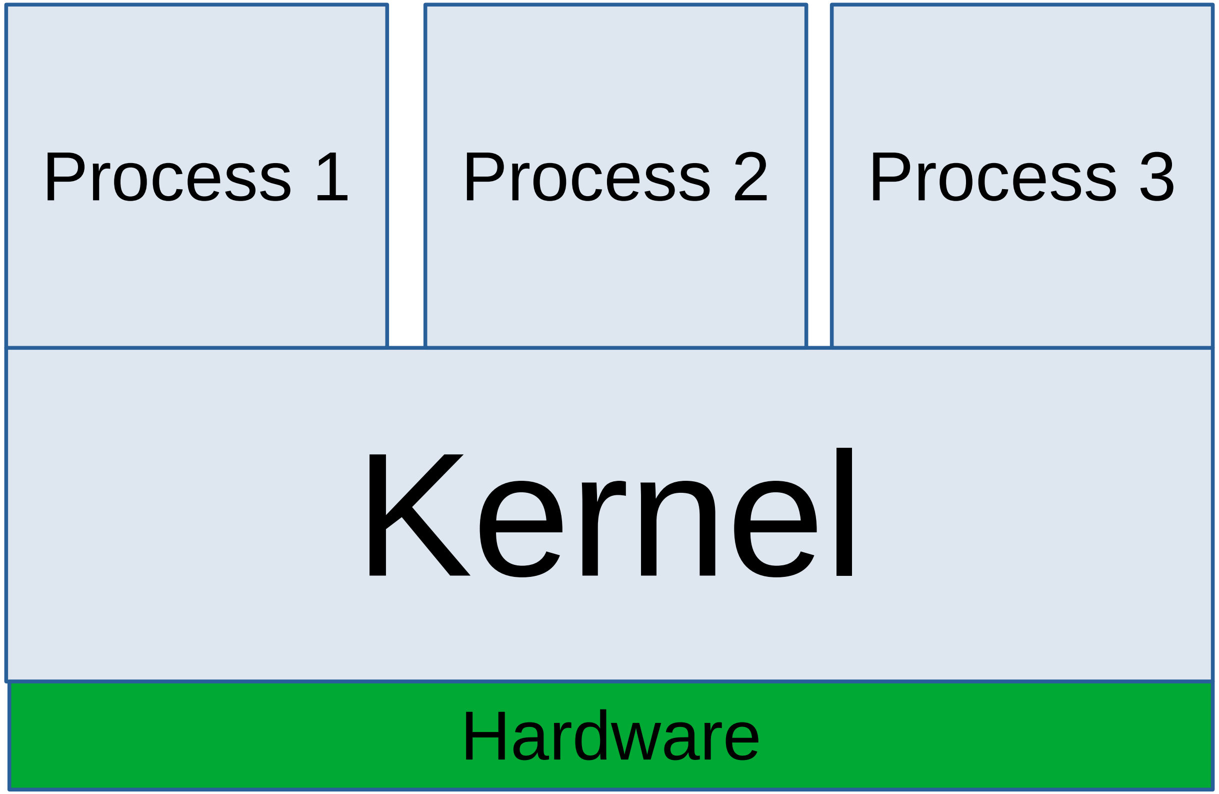


A connection

- For now, just know TCP, UDP, and ICMP
  - Stream sockets *vs.* datagrams
- TCP and UDP have “ports”
  - Port helps identify a process for incoming packets
  - Open port == “listening”
- Three-way handshake

Process?

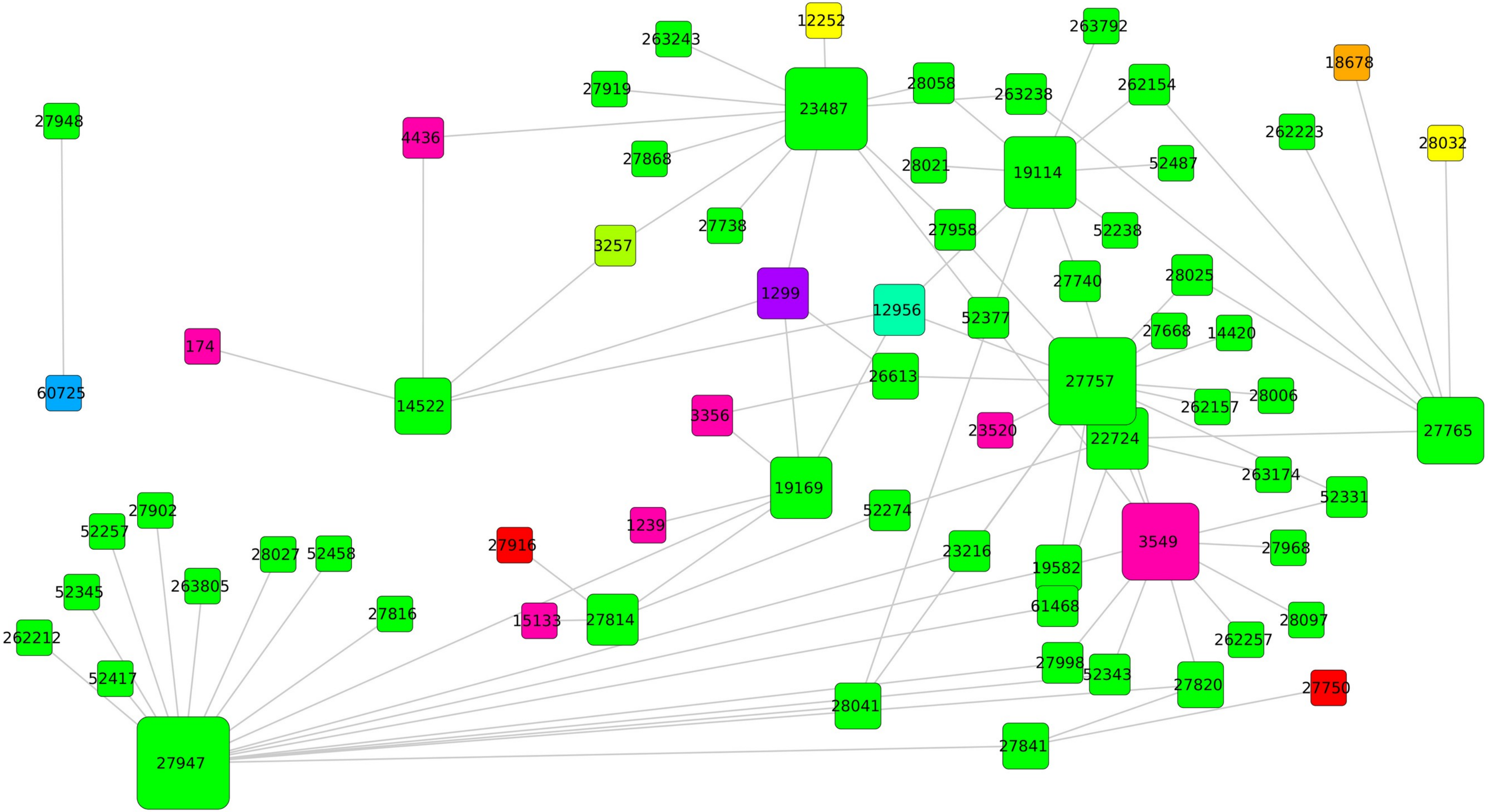
Separated by virtual memory, access system resources *via* system calls.

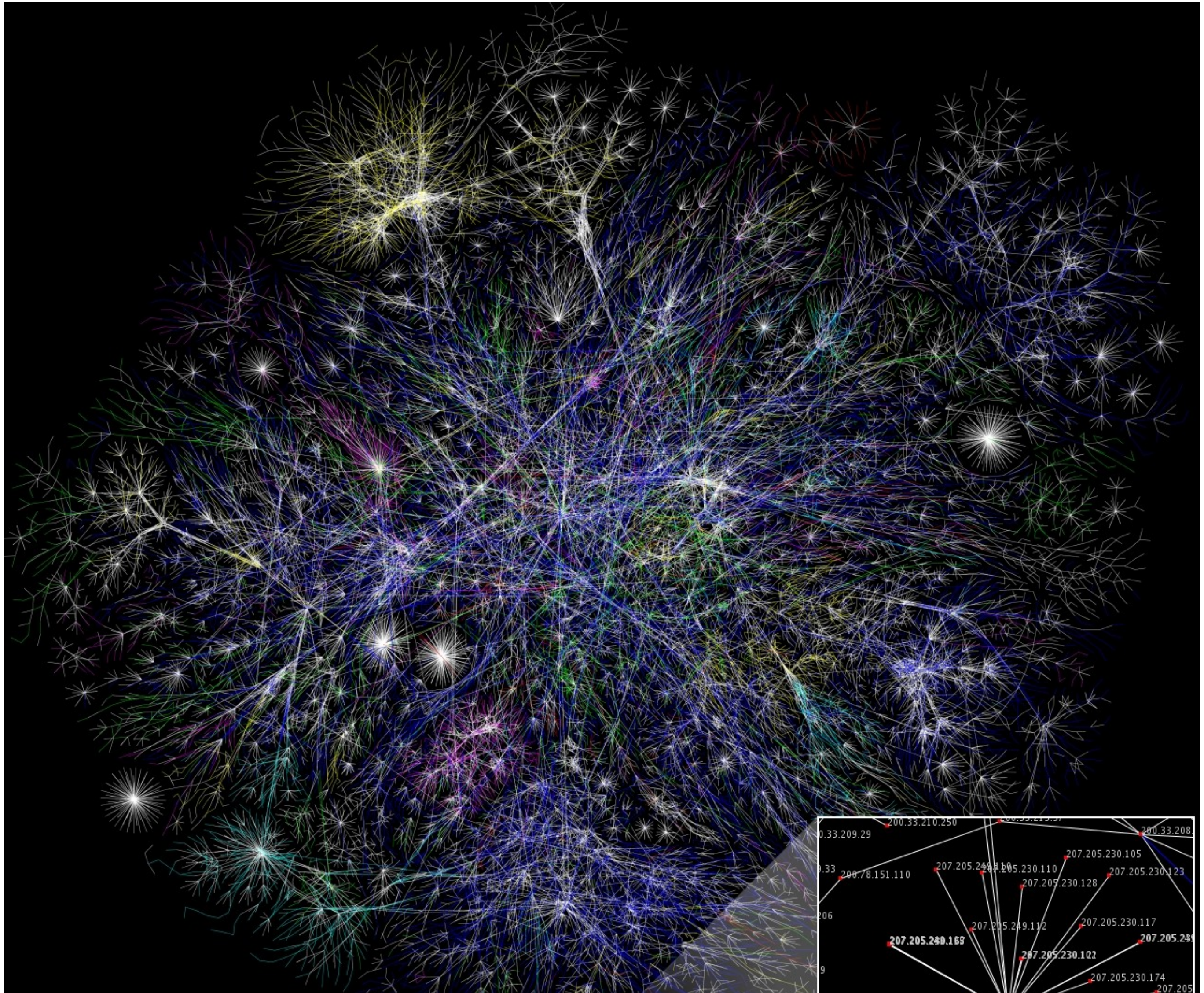


Almost there…

- DNS for resolving hostnames to IPs
  - breakpointingbad.com becomes 149.28.240.117
- BGP to scale to the size of the Internet
  - Path vector protocol
- HTTP as another example of an application layer protocol

Internet in Ecuador...




200.33.210.250
207.205.230.105
208.78.151.110
207.205.230.123
207.205.230.128
207.205.249.112
207.205.230.117
207.205.230.174

OSI model

- 1. Physical
- 2. Link
- 3. Network
- 4. Transport
- 5. Session
- 6. Presentation
- 7. Application

Why do we need crypto?

- Potential adversaries at every hop
  - Confidentiality of messages
    - (Crypto doesn’t hide the message’s existence, that’s steganography)
  - Integrity of messages
    - If a bit gets changed in transit, we’d like to know
  - Authenticity
    - Who actually sent the message?

Other properties we might like (preview)...

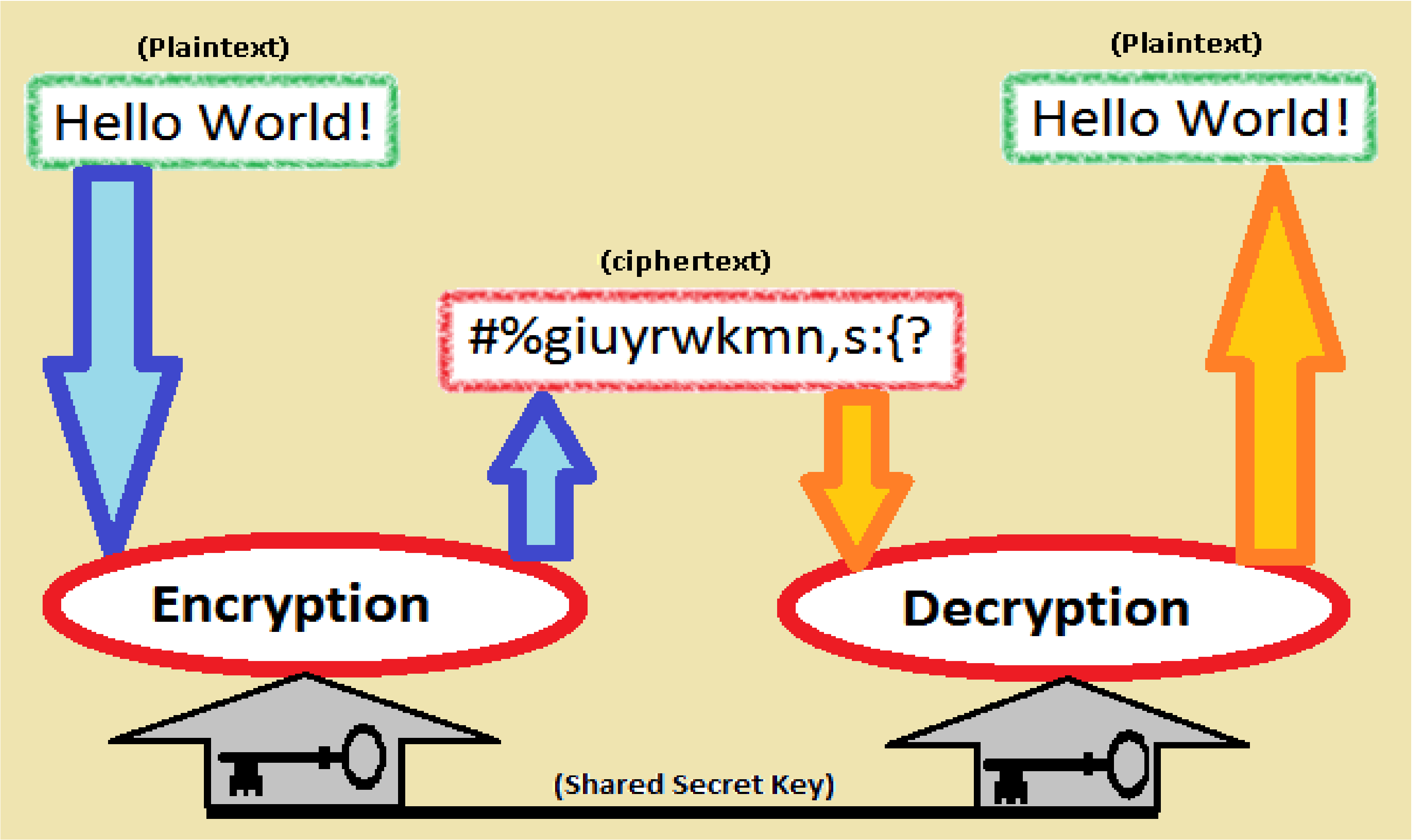
- Key exchange
- Non-repudiation
- Forward secrecy
- Off-the-record
  - Malleability, plausible deniability
- Future secrecy

Overview

- Symmetric encryption
  - Assumes two parties wishing to communicate already have a shared secret
- Asymmetric encryption
  - Makes different assumptions (*e.g.*, that everybody knows the public key or that the eavesdropper is passive)
  - Quantum computers break current algorithms that are used in practice
- Secure hash functions and message authentication

Symmetric Crypto

- Confidentiality
- Integrity
- ~~Availability~~
- Authentication
- ~~Non-repudiation~~
- ~~A way to distribute the shared secret keys~~



Source: Wikipedia

Terminology

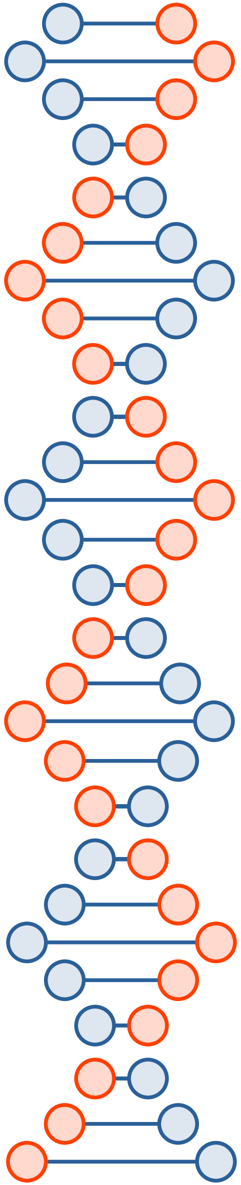
- Plaintext – before encryption, easy to read
- Ciphertext – after encryption, hopefully indecipherable without the key
- Key – the shared secret, typically just bits that were generated with a high entropy process

Review on your own...

- Caesar Cipher
- Vigenere Cipher and related attacks

Modern symmetric crypto

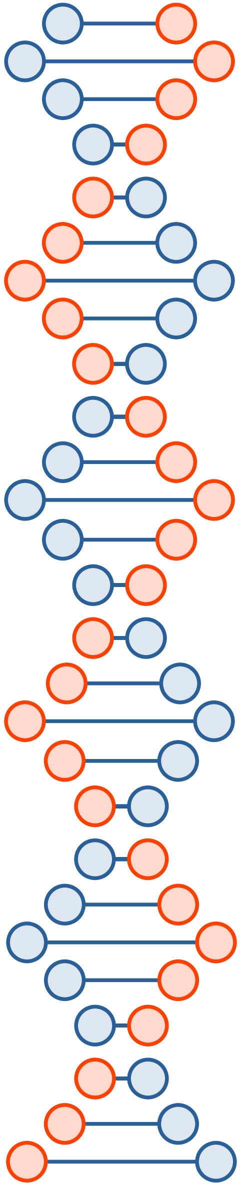
- Mostly:
  - Substitution
  - Permutation
  - XOR



Substitution

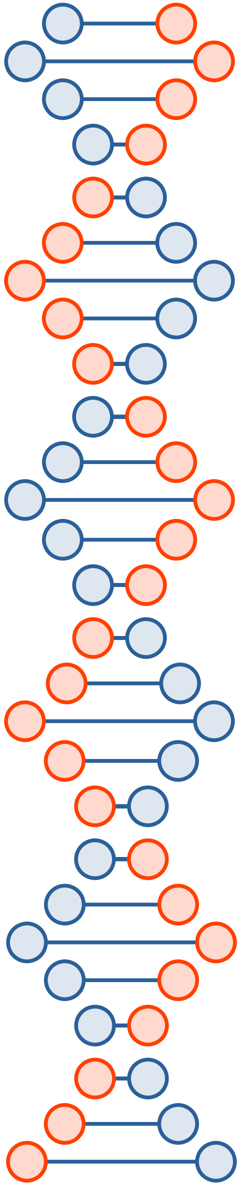
HELLO WORLD

TNWWX DXPWE



Permutation

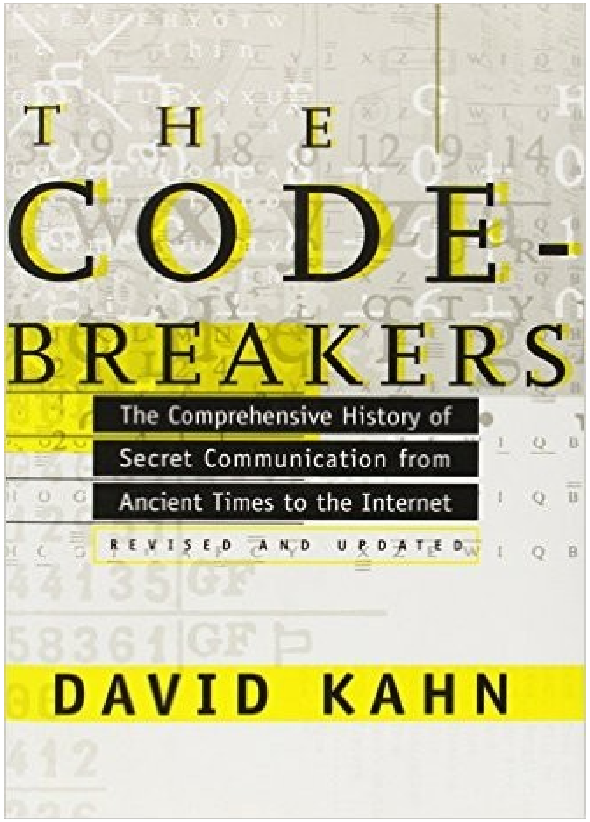
ABCD	ABDC	ACBD	ACDB	ADBC	ADCB
BACD	BADC	BCAD	BCDA	BDAC	BDCA
CABD	CADB	CBAD	CBDA	CDAB	CDBA
DABC	DACB	DBAC	DBCA	DCAB	DCBA



Bitwise XOR

$$
\begin{aligned}
& 00101010_b \\
\oplus\, & 10000110_b \\
=\, & 10101100_b
\end{aligned}
$$

2000+ years of history...

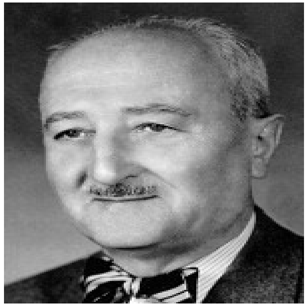


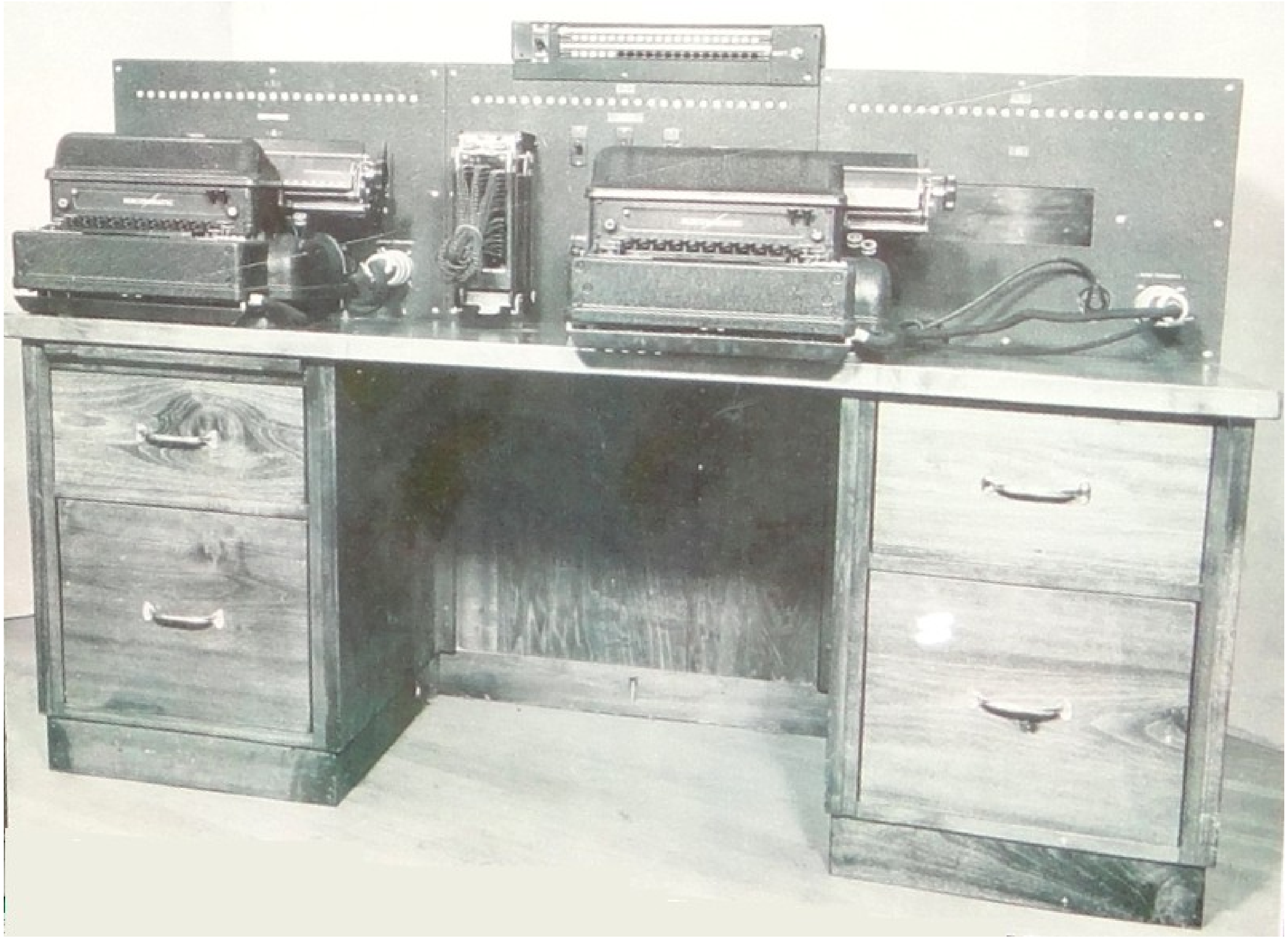
Symmetric encryption over time

- Handwritten notes, *etc.* for centuries
  - Typically the algorithm was secret
- 1883 … Kerckhoff’s rules
  - Now we know the key should be the only secret
- 1975 … DES
  - Efficient in hardware, not in software
- 2001 … AES
  - Efficient in software, and lots of different kinds of hardware

William and Elizabeth Friedman

- Met while analyzing Shakespeare ciphers at Riverbank Laboratories ("William Friedman wrote Shakespeare's plays")
- Elizabeth solved ciphers of alcohol and drug smugglers, then German ambassadors in South America (three enigma machines)
- William led a team that solved PURPLE, conceived CryptoAG scheme





https://en.wikipedia.org/wiki/Type_B_Cipher_Machine#/media/File:Purple_cipher_machine_analog_bw_photo_NCM.jpg

https://en.wikipedia.org/wiki/Enigma_machine#/media/File:Enigma_(crittografia)_-_Museo_scienza_e_tecnologia_Milano.jpg

Zodiac cipher

Image from wikia

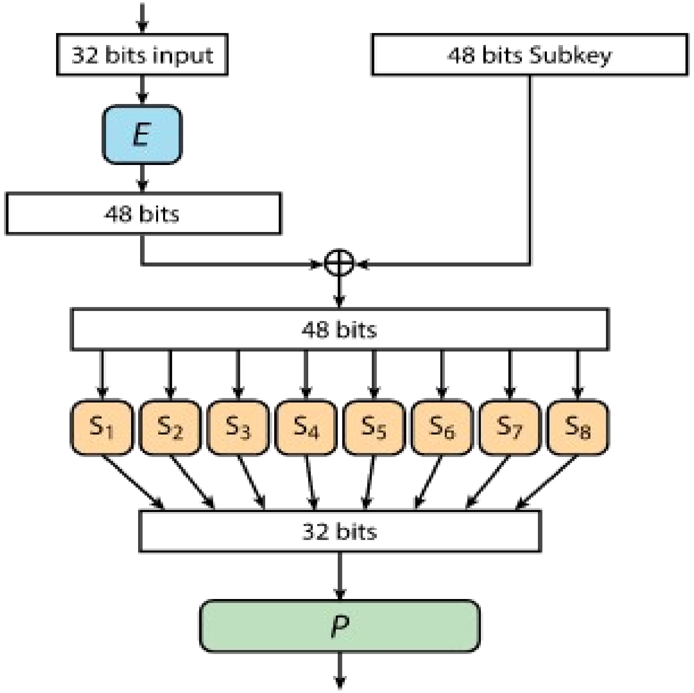
Bitwise XOR as a cipher itself

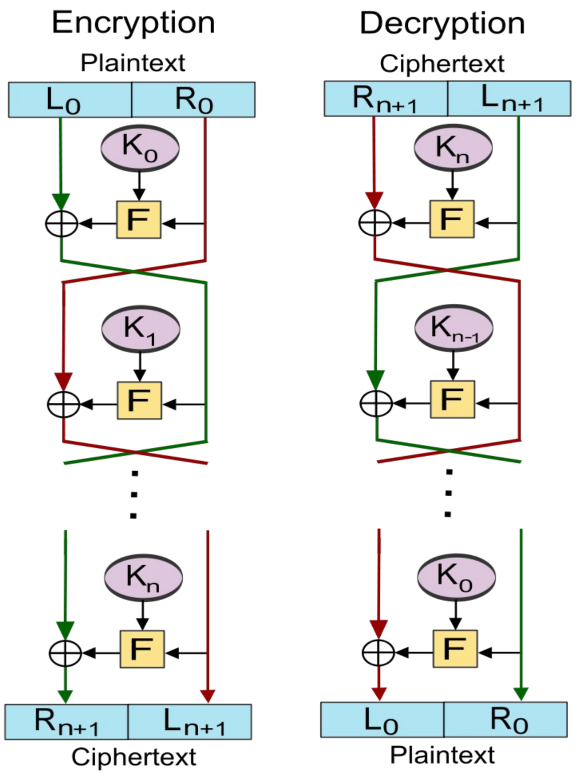
- Typically used by malware, 8 or 32 bits
  - WEP attack uses these properties
- (B xor K) xor K = B
- (A xor K) xor (B xor K) = A xor B
- (0 xor K) = K
- (K xor K) = 0
- Frequency analysis or brute force

One-time pad

- *E.g.*, an XOR cipher or Caesar cipher where the key has good randomness and is as long as the plaintext
  - And never gets reused
- Most codes made by the NSA through the 1980s were one-time pads
  - What if it’s not practical to share enough key material beforehand, *e.g.*, on the Internet?

1977 - DES (16 rounds, 64-bit blocks, 56-bit key)





DES S-boxes

- 6 bits becomes 4 bits
- Somewhat arbitrary
  - IBM proposed some, NSA replaced with others

שורה	מס׳ עמודה															
	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15
	S_1															
0	14	4	13	1	2	15	11	8	3	10	6	12	5	9	0	7
1	0	15	7	3	14	2	13	1	10	6	12	11	9	5	3	8
2	4	1	14	8	13	6	2	11	15	12	9	7	13	10	5	0
3	15	12	8	2	4	9	1	7	5	11	3	14	10	0	6	13
	S_2															
0	15	1	8	14	6	11	3	4	9	7	2	13	12	0	5	10
1	3	13	4	7	15	2	8	14	12	0	1	10	6	9	11	5
2	0	14	7	11	10	4	13	1	5	8	12	6	9	3	2	15
3	13	8	10	1	3	15	4	2	11	6	7	12	0	5	14	9
	S_3															
0	10	0	9	14	6	3	15	5	1	13	12	7	11	4	2	8
1	13	7	0	9	3	4	6	10	2	8	5	14	12	11	15	1
2	13	6	4	9	8	15	3	0	11	1	2	12	5	10	14	7
3	1	10	13	0	6	9	8	7	4	15	14	3	11	5	2	12
	S_4															
0	7	13	14	3	0	6	9	10	1	2	8	5	11	12	4	15
1	13	8	11	5	6	15	0	3	4	7	2	12	1	10	14	9
2	10	6	9	0	12	11	7	13	15	1	3	14	5	2	8	4
3	3	15	0	6	10	1	13	8	9	4	5	11	12	7	2	14
	S_5															
0	2	12	4	1	7	10	11	6	8	5	3	15	13	0	14	9
1	14	11	2	12	4	7	13	1	5	0	15	10	3	9	8	6
2	4	2	1	11	10	13	7	8	15	9	12	5	6	3	0	14
3	11	8	12	7	1	14	2	13	6	15	0	9	10	4	5	3
	S_6															
0	12	1	10	15	9	2	6	8	0	13	3	4	14	7	5	11
1	10	15	4	2	7	12	9	5	6	1	13	14	0	11	3	8
2	9	14	15	5	2	8	12	3	7	0	4	10	1	13	11	6
3	4	3	2	12	9	5	15	10	11	14	1	7	6	0	8	13
	S_7															
0	4	11	2	14	15	0	8	13	3	12	9	7	5	10	6	1
1	13	0	11	7	4	9	1	10	14	3	5	12	2	15	8	6
2	1	4	11	13	12	3	7	14	10	15	6	8	0	5	9	2
3	6	11	13	8	1	4	10	7	9	5	0	15	14	2	3	12
	S_8															
0	13	2	8	4	6	15	11	1	10	9	3	14	5	0	12	7
1	1	15	13	8	10	3	7	4	12	5	6	11	0	14	9	2
2	7	11	4	1	9	12	14	2	0	6	10	13	15	3	5	8
3	2	1	14	7	4	10	8	13	15	12	9	0	3	5	6	11

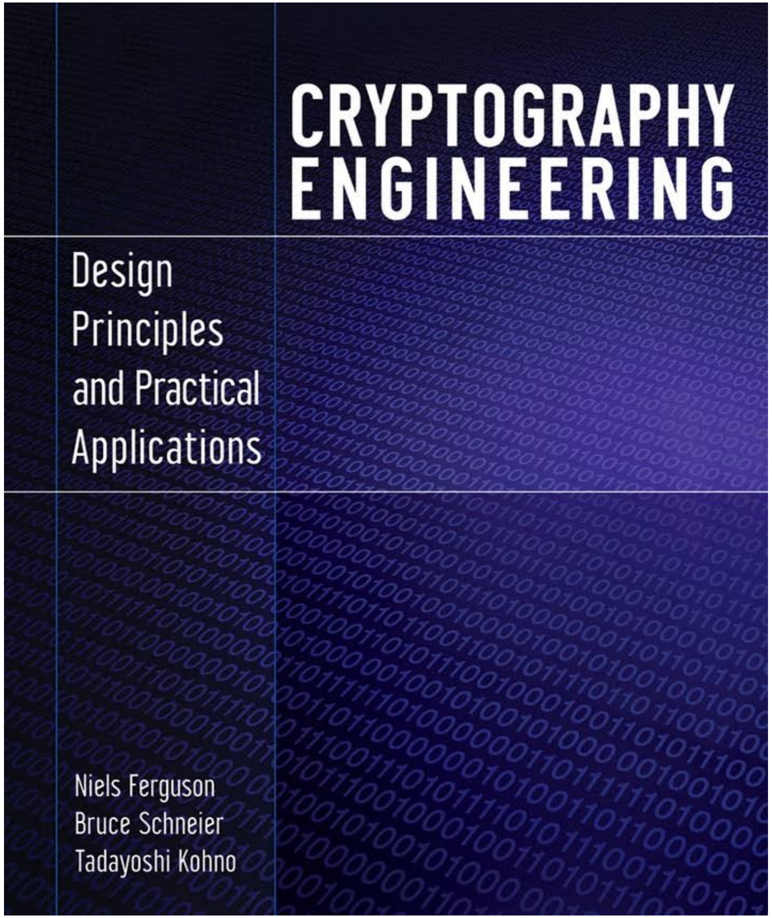
Importance of substitution

- XOR and permutation are linear functions
  - Solve for the key given plaintext and ciphertext?
- Bit differences in inputs are not changed at all by permuting bits
- XOR also preserves differences in bits

Different approaches (preview)

- DES simply tried to thwart these two specific types of attack (linear and differential) by carefully choosing the S boxes and letting them destroy information about the input (okay because of Feistel structure)
- AES is going to do something a lot more clever, that is invertible (no need for the Feistel structure, so fewer rounds) but still thwarts linear and differential cryptanalysis.

Cryptography Engineering by Ferguson *et al.*



Preparation for next lecture...

You have 12 coins, one is counterfeit. The counterfeit is either slightly heavier or slightly lighter, otherwise it's impossible to tell. You have a balance. Using the balance the fewest number of times, find the counterfeit coin.

Acknowledgments

- Many of the above images are from Wikipedia