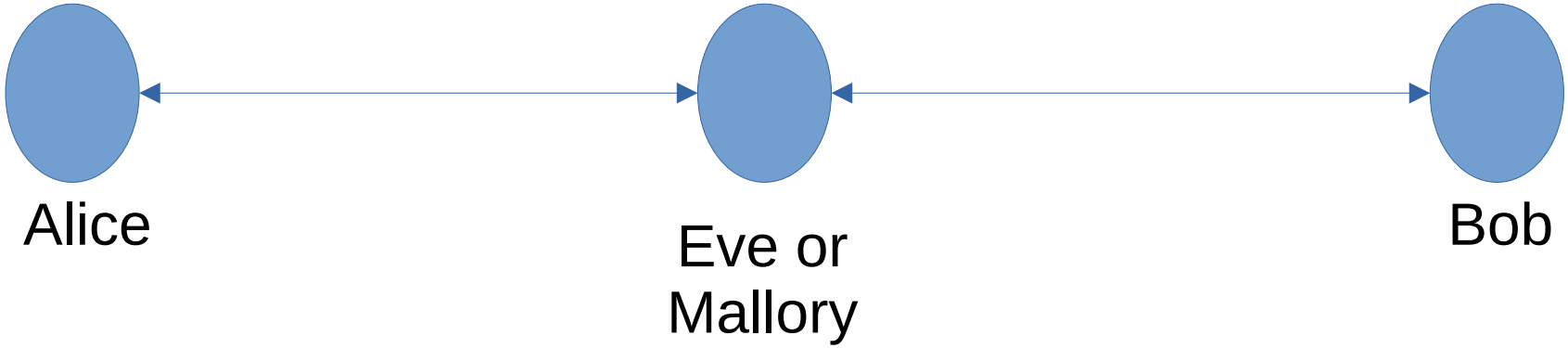
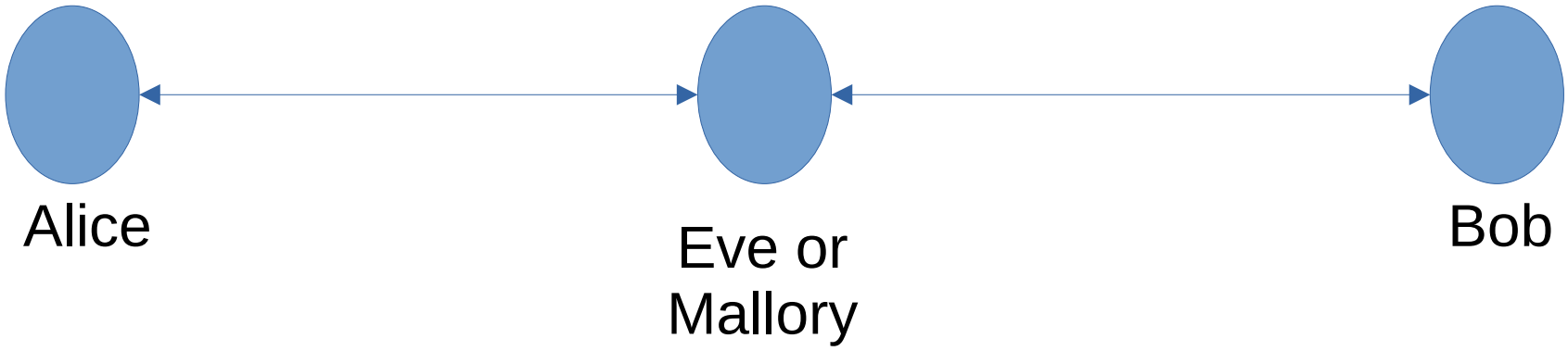
WiFi security and stream ciphers

CSE 468 Fall 2026

jedimaestro@asu.edu

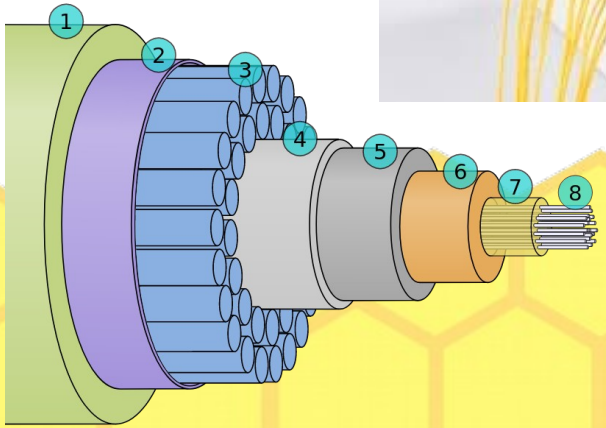

Alice
Eve or
Mallory
Bob



WiFi, electric path, or optical… Eve or Mallory get their own copy!

You want to connect two machines...

- Machines = desktops, laptops, mobile devices, routers, embedded devices, ...

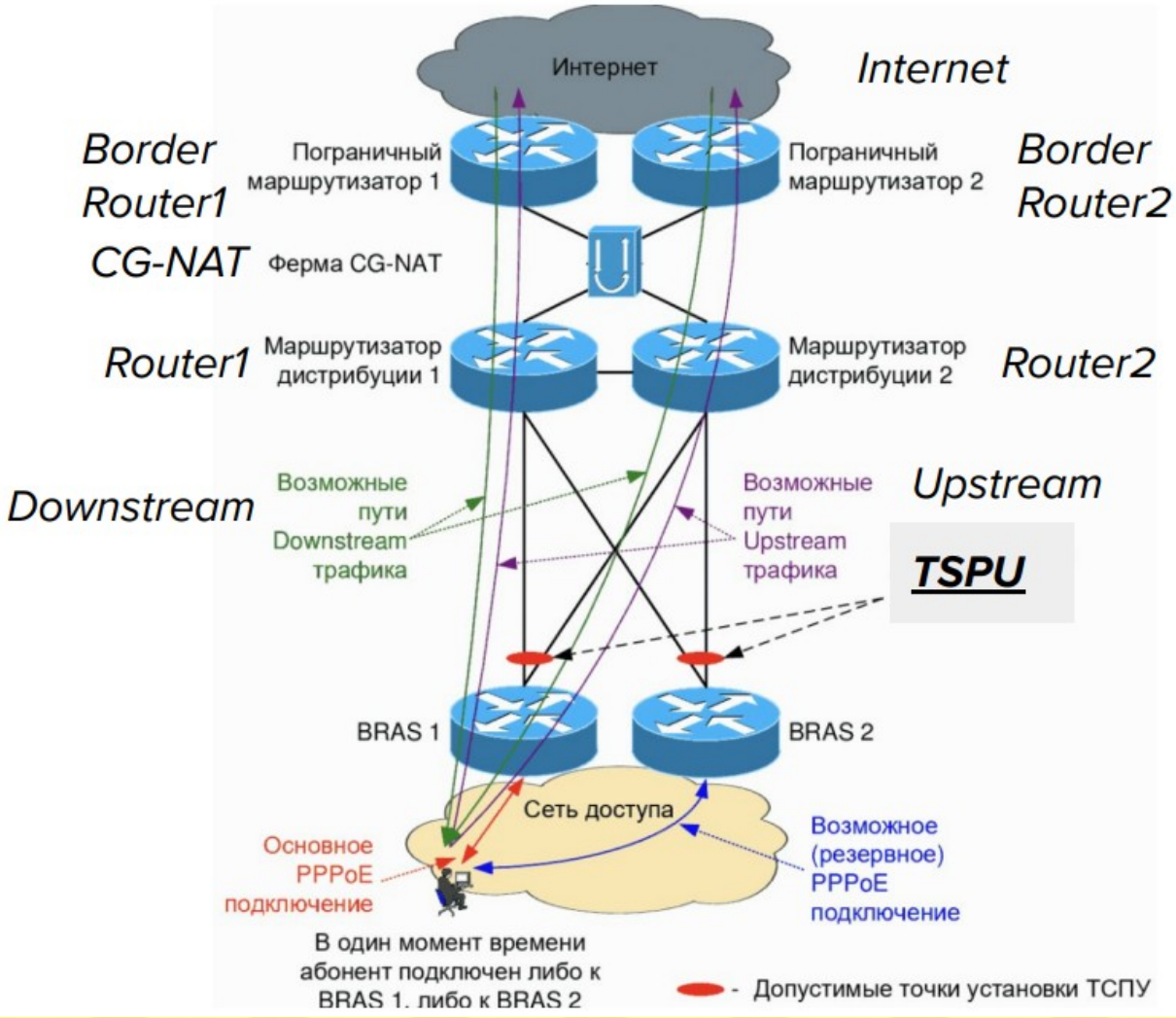


A “hop”

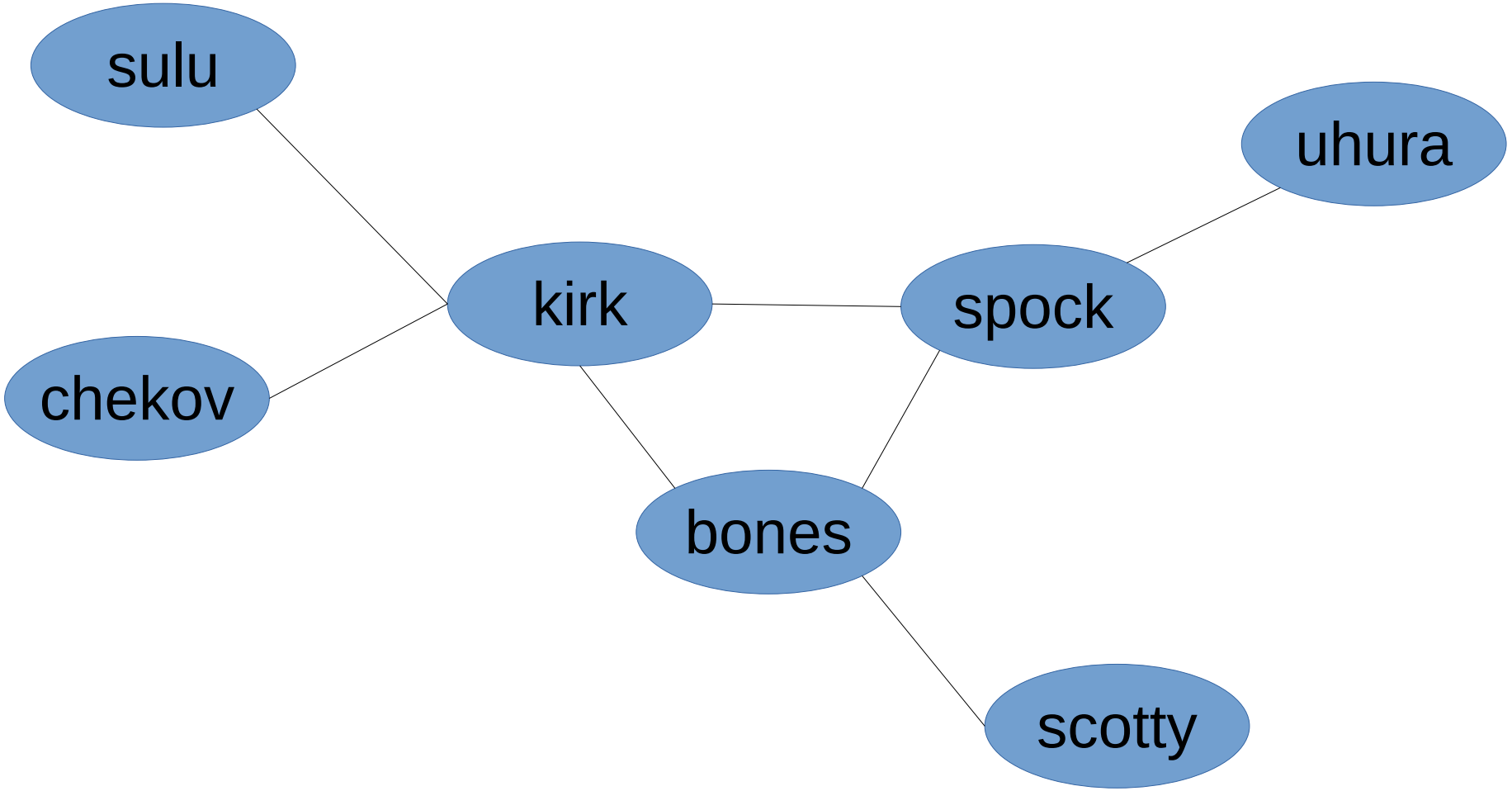
A “hop”

Ethernet, WiFi, optical cable...

There are electric paths between the edge users and the backbone



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

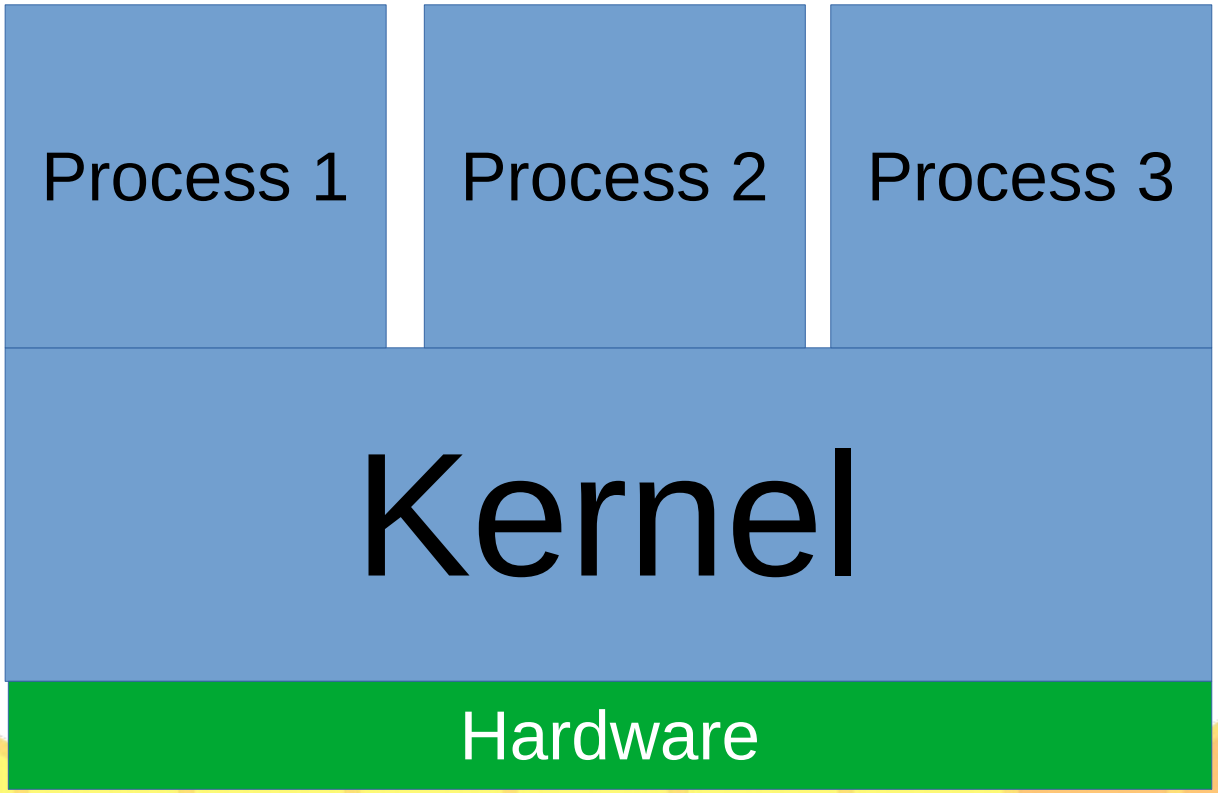
- IPv4 is 32-bits, broken into 4 bytes (review CIDR)
  - 192.168.7.8 is an IP on 192.168.7.0/24
  - 64.106.46.20
  - 8.8.8.8
- IPv6 is 128 bits
  - 2001:0db8:85a3:0000:0000:8a2e:0370:7334

A connection or flow

- 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”
- TCP has a three-way handshake

Process?

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



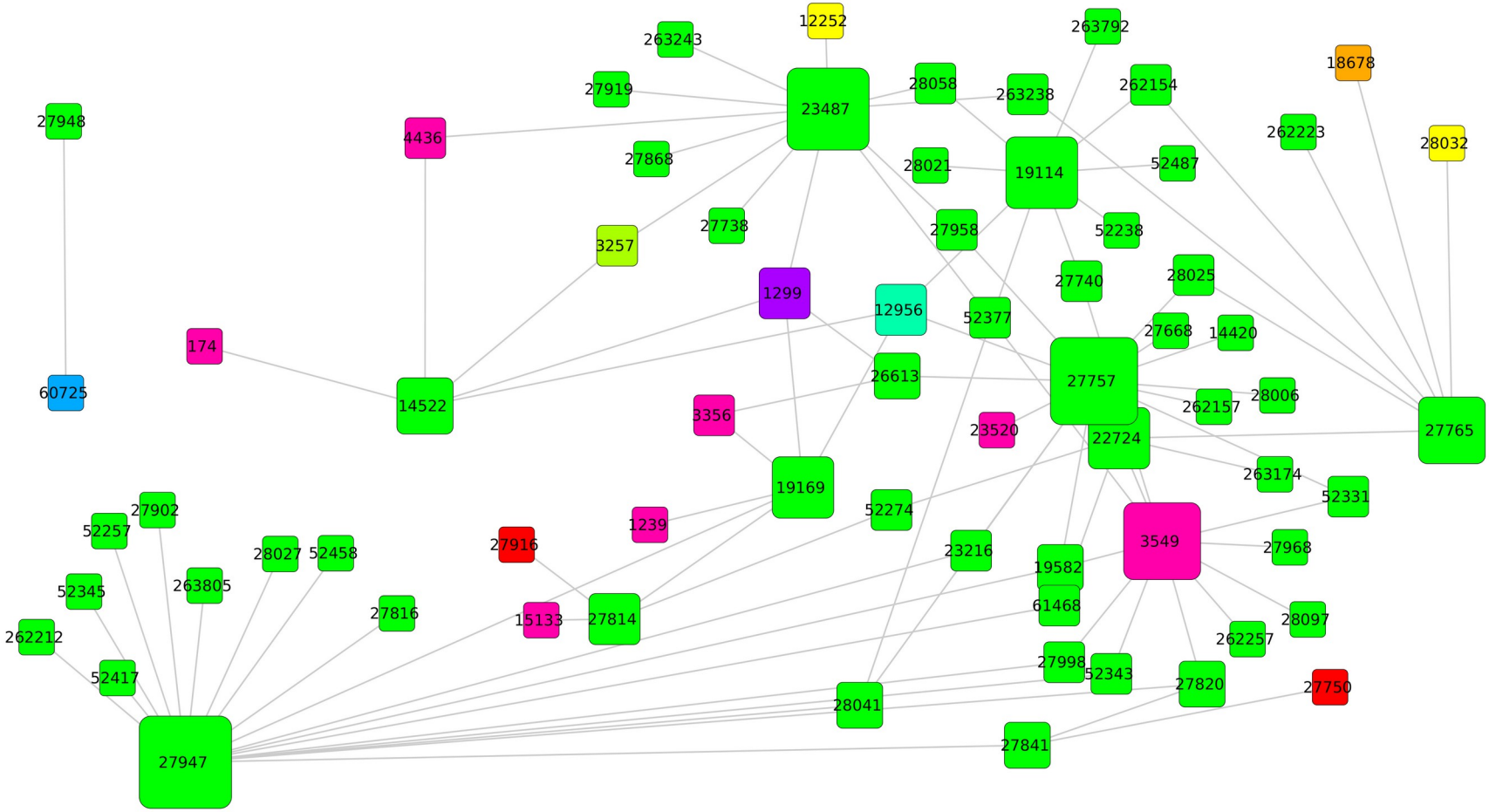
Interprocess communication (can be over a network or not)

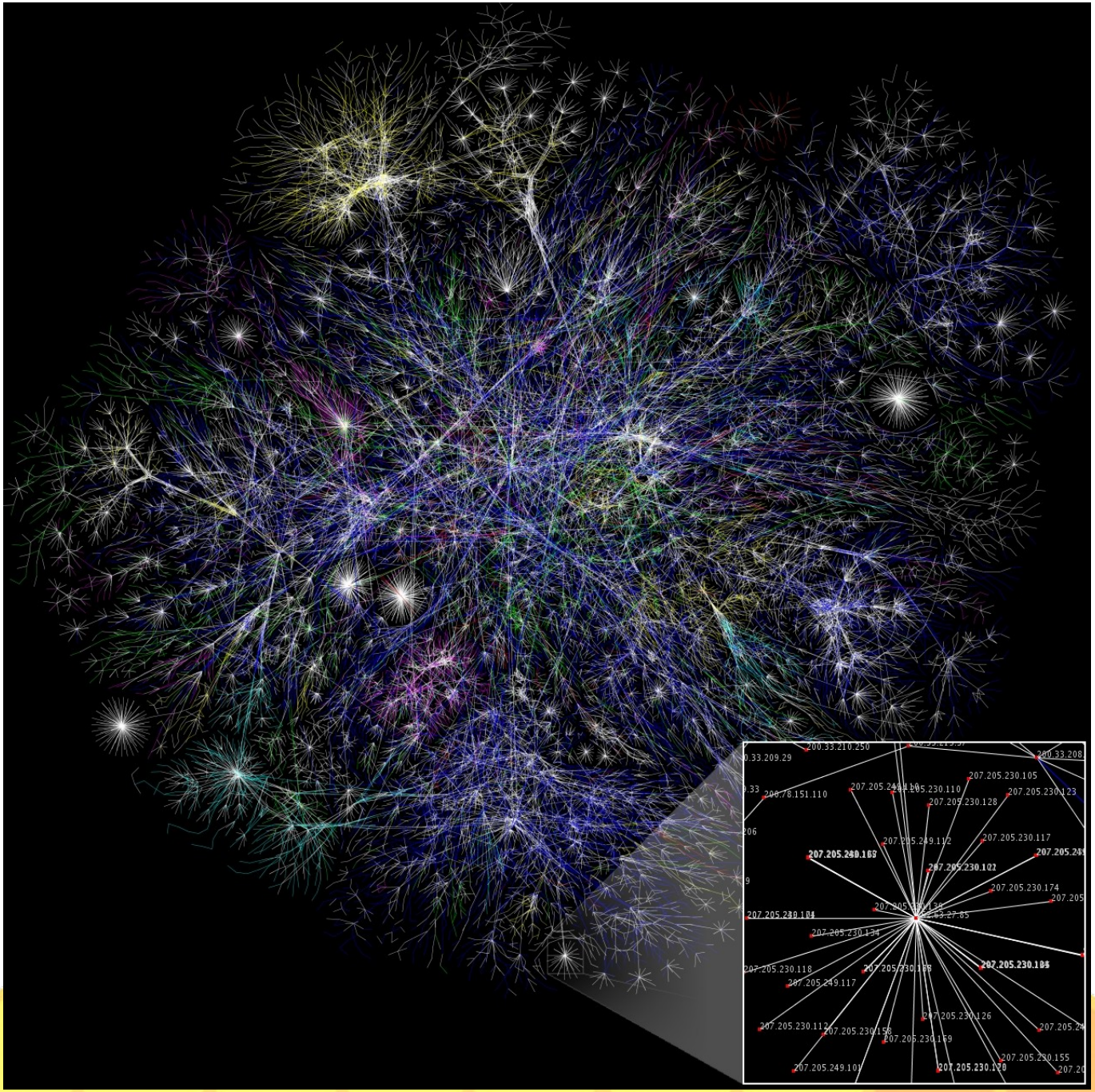
- Stream socket
  - Full duplex
  - Bytes always arrive in order
  - No delimiters
  - Example: TCP
- Datagram socket
  - Not connection-based
  - Datagrams can arrive out of order
  - Datagrams are delimiters
  - Example: UDP

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
207.205.230.110
207.205.230.123
207.78.151.110
207.205.230.128
207.205.249.112
207.205.230.117
207.205.230.174
207.205.230.134
207.205.230.118
207.205.249.117
207.205.230.126
207.205.230.155

OSI model

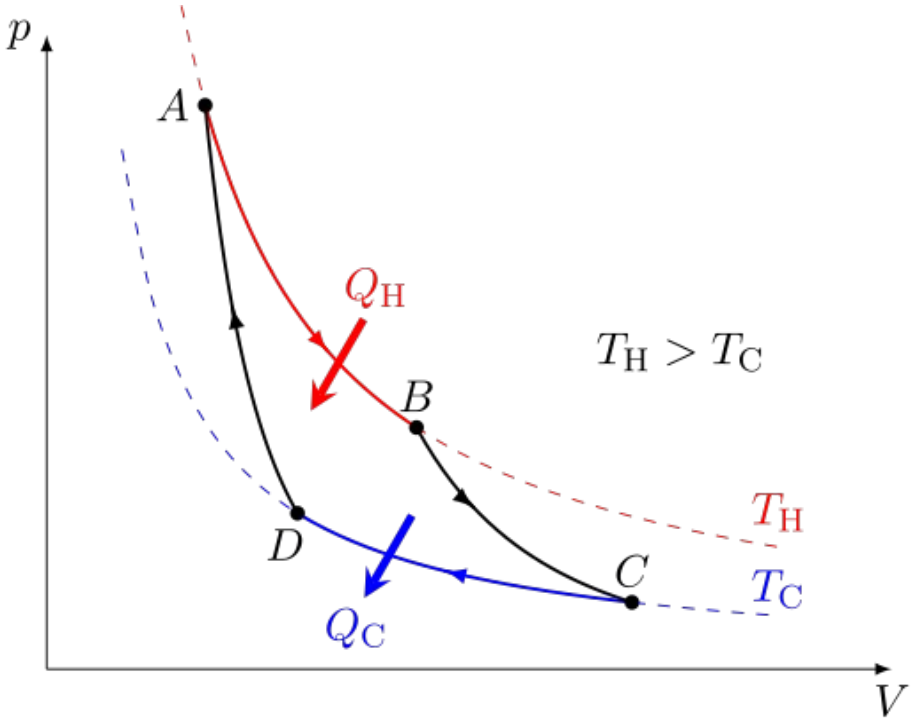
- 1. Physical
- 2. Link
- 3. Network
- 4. Transport
- 5. Session
- 6. Presentation
- 7. Application

OSI model

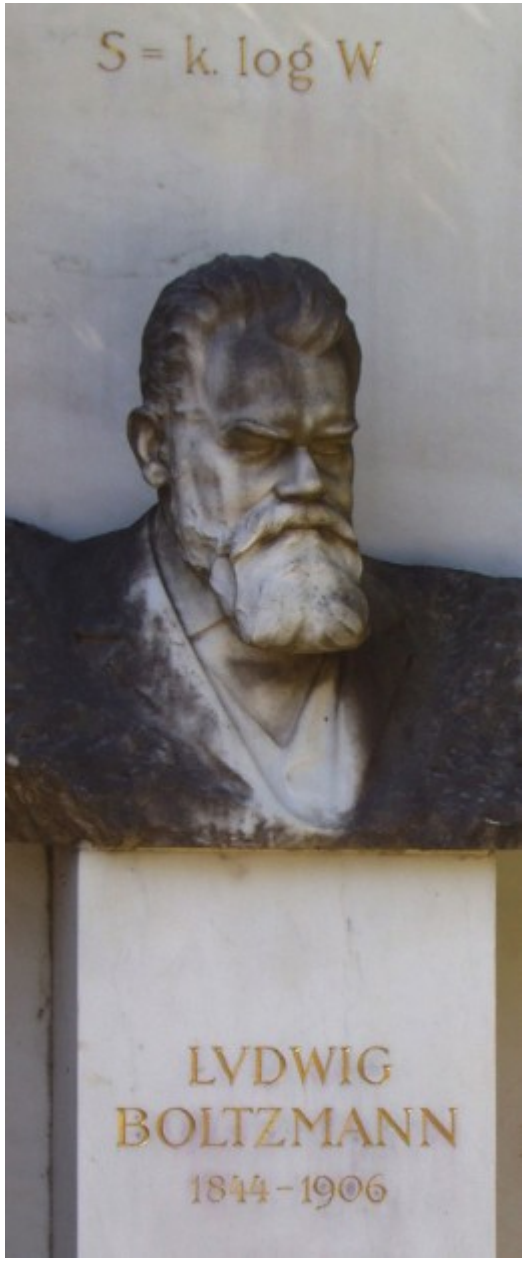
- 1. Physical
- 2. Link
- 3. Network
- 4. Transport
- 5. Session
- 6. Presentation
- 7. Application

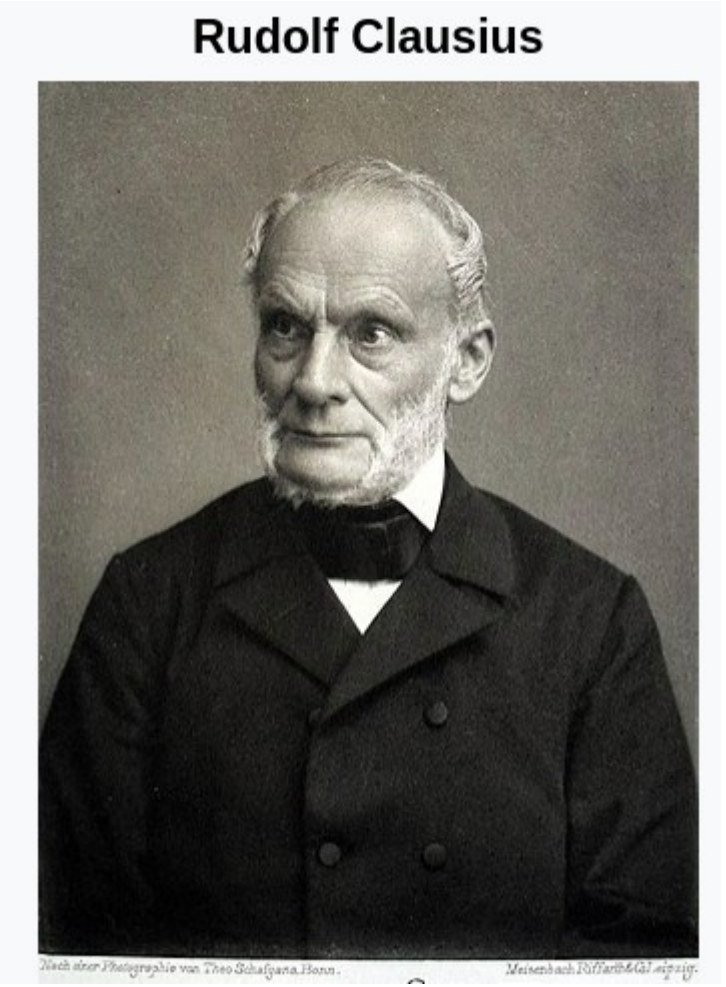
WiFi security (mostly)
lives in these two layers

What is information?



https://en.wikipedia.org/wiki/Nicolas_L%C3%A9onard_Sadi_Carnot
https://en.wikipedia.org/wiki/Carnot_heat_engine





https://en.wikipedia.org/wiki/Rudolf_Clausius

“entropy”

(from Greek ἐν en "in" and τροπή tropē "transformation")

Like energy, but you can’t use it.

Entropy

- Statistical foundation by Gibbs, Boltzmann, Maxwell, Planck, *etc.*
- Directly inspired the name of entropy in Shannon’s information theory

$$H = -\sum_i p_i \log_2 (p_i)$$

Requirements (Shannon, 1948)

1) I(p) ≥ 0 (information is non-negative, p≥1)
2) I(1) = 0 (events that always occur carry no information)
3) I(p1 p2) = I(p1) + I(p2) (information due to independent events is additive)

   Also, continuity, symmetry, and maximum when all possible events are equiprobable.

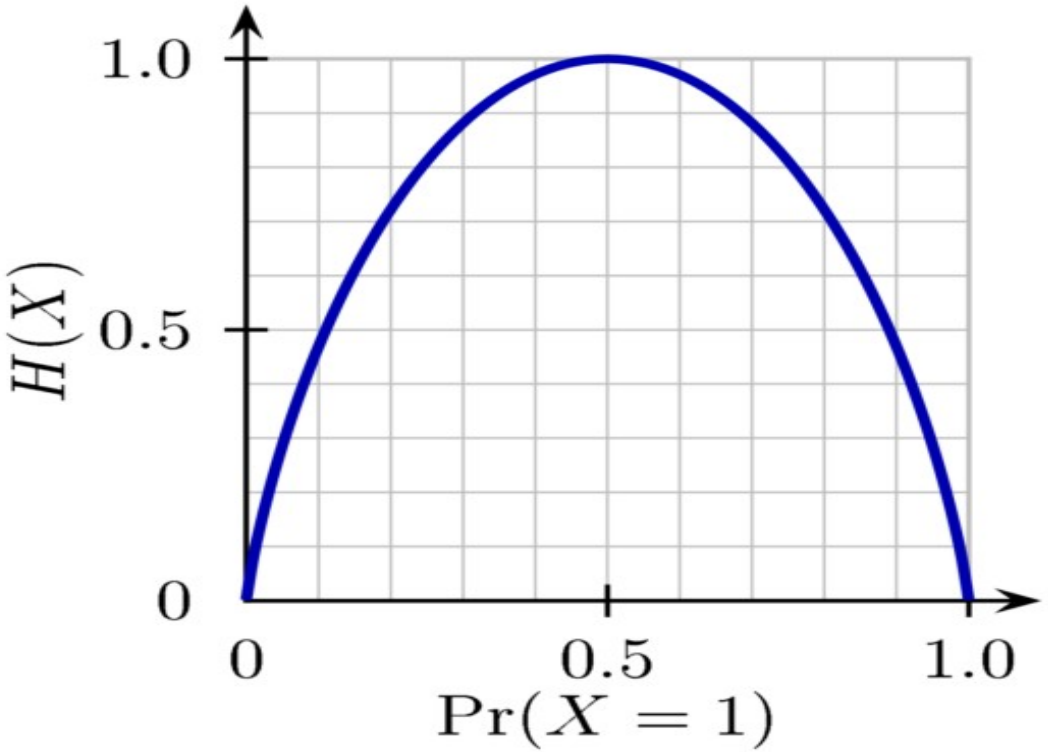
I(p) = log(1/p)

1) I(1/2) = 0.30102999566...
2) I(1) = 0
3) I(1/2) + I(1/3) = log(2) + log(3) = 0.77815125038...
Joint probability: I(1/6) = 0.77815125038...

Continuity: I(1/2.01) = 0.30319605742...
Symmetry: log (3) + log(2) = 0.77815125038...
Maximum: log 3 + log 3 + log 3 = 1.43136376416...
log 2 + log 4 + log 4 = 1.20411998266...

Information = Entropy = Surprise

$$H[p] = -\sum_{i=1}^{k} p_i \log p_i$$



Side note – Differential Entropy

https://en.wikipedia.org/wiki/Differential_entropy

$$h(X) = \mathbf{E}[-\log(f(X))] = -\int_{\mathcal{X}} f(x)\log f(x)\,dx$$

f(x) is a probability density function for the signal, the more the signal “jumps around” the higher the entropy, therefore modulating higher frequencies
means more entropy and therefore more bandwidth.

Not a pop quiz #1

- When a 3yo walks by with a stepstool…
  - 4 times out of 10 it's to get something they're not supposed to have
  - 2 times out of 10 it's to climb up to somewhere they're not supposed to be
  - 1 time out of 10 it's to wash their hands
  - 1 time out of 10 it's to get something they are allowed to have
  - 1 time out of 10 it's to use as a dollhouse
  - 1 time out of 10 it's to turn over and use as a storage bin
- What is the entropy of each instance of 3yo stepstool habits?

Answer

Input:

$$-0.4 \log_2(0.4) - 0.2 \log_2(0.2) - 4\,(0.1 \log_2(0.1))$$

Result:

$$2.32193\ldots$$

Not a pop quiz #2

- There are three possible states the Tempe weather could be in during any given hour on a summer day (very hot and bright out, very hot and it’s nighttime, monsoonal rains). What probability distribution over these events would give the maximum entropy in terms of what you might observe in a randomly chosen hour from the summer?

Answer

Input:

$$-\frac{1}{3}\log_2\left(\frac{1}{3}\right)-\frac{1}{3}\log_2\left(\frac{1}{3}\right)-\frac{1}{3}\log_2\left(\frac{1}{3}\right)$$

Exact result:

$$\frac{\log(3)}{\log(2)}$$

$\log(x)$ is the natural logarithm

Decimal approximation:

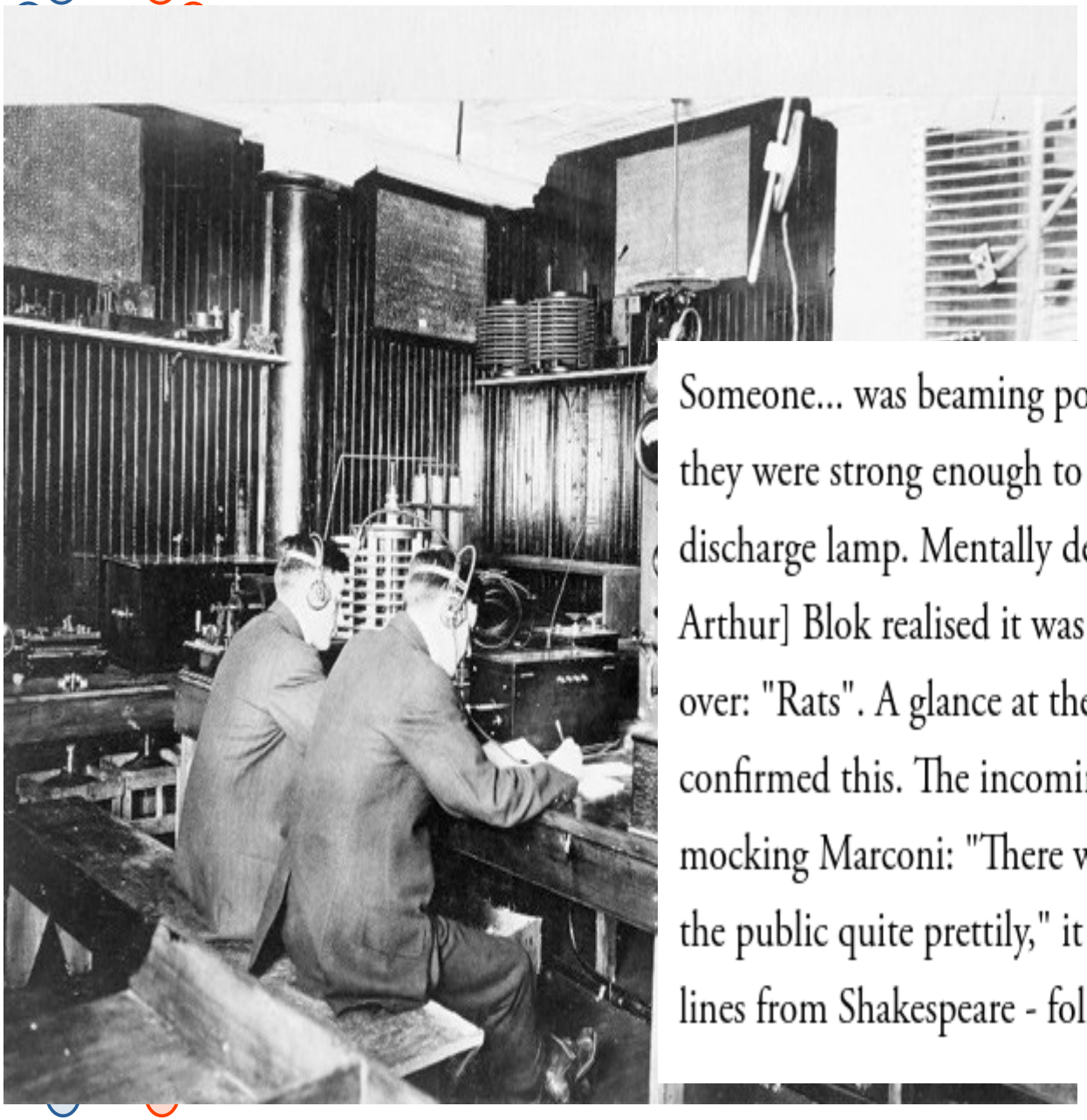
More digits

1.584962500721156181453738943947816508759814407692481060455...

Not a pop quiz #3

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.

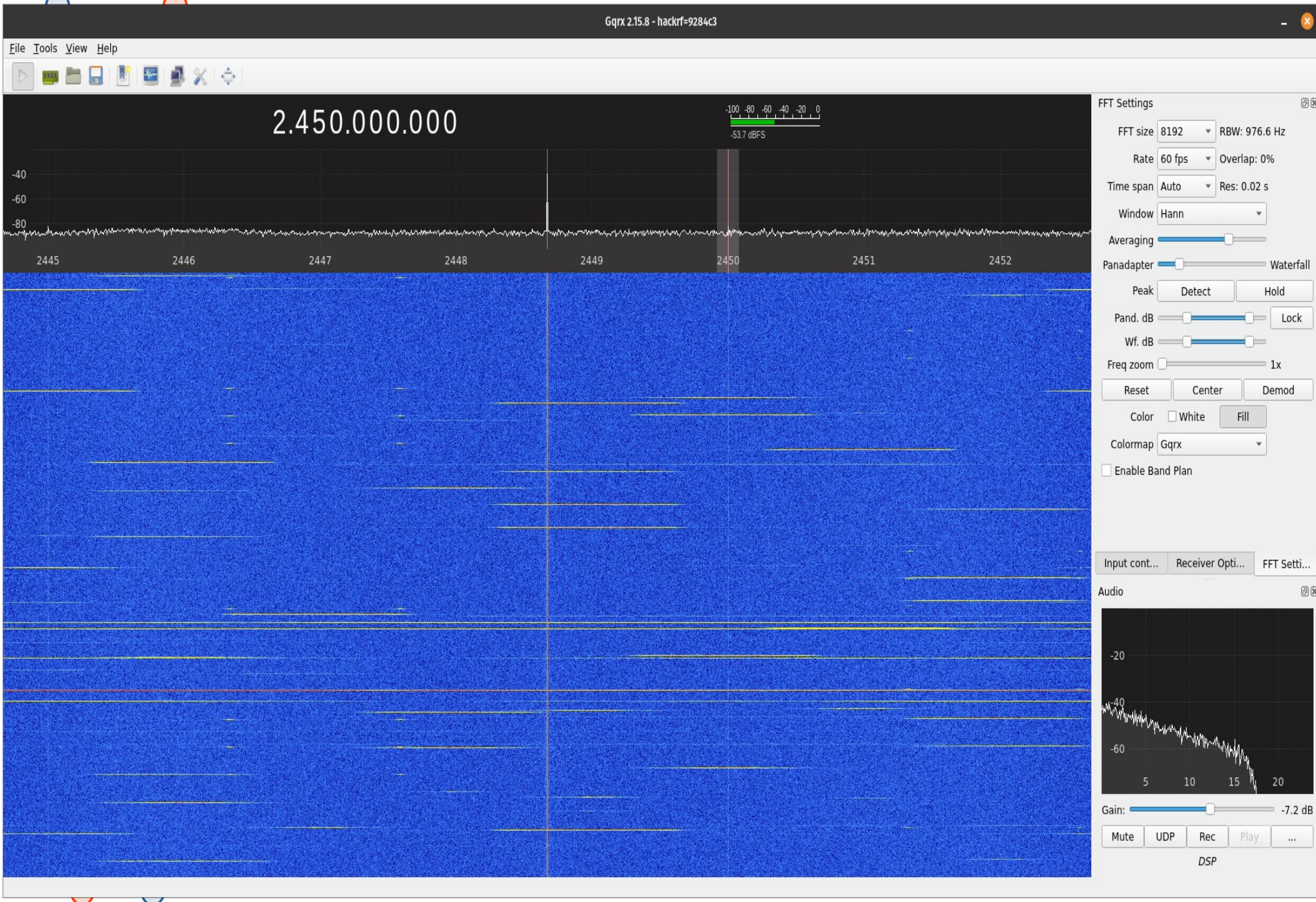
WiFi and stream ciphers...



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.

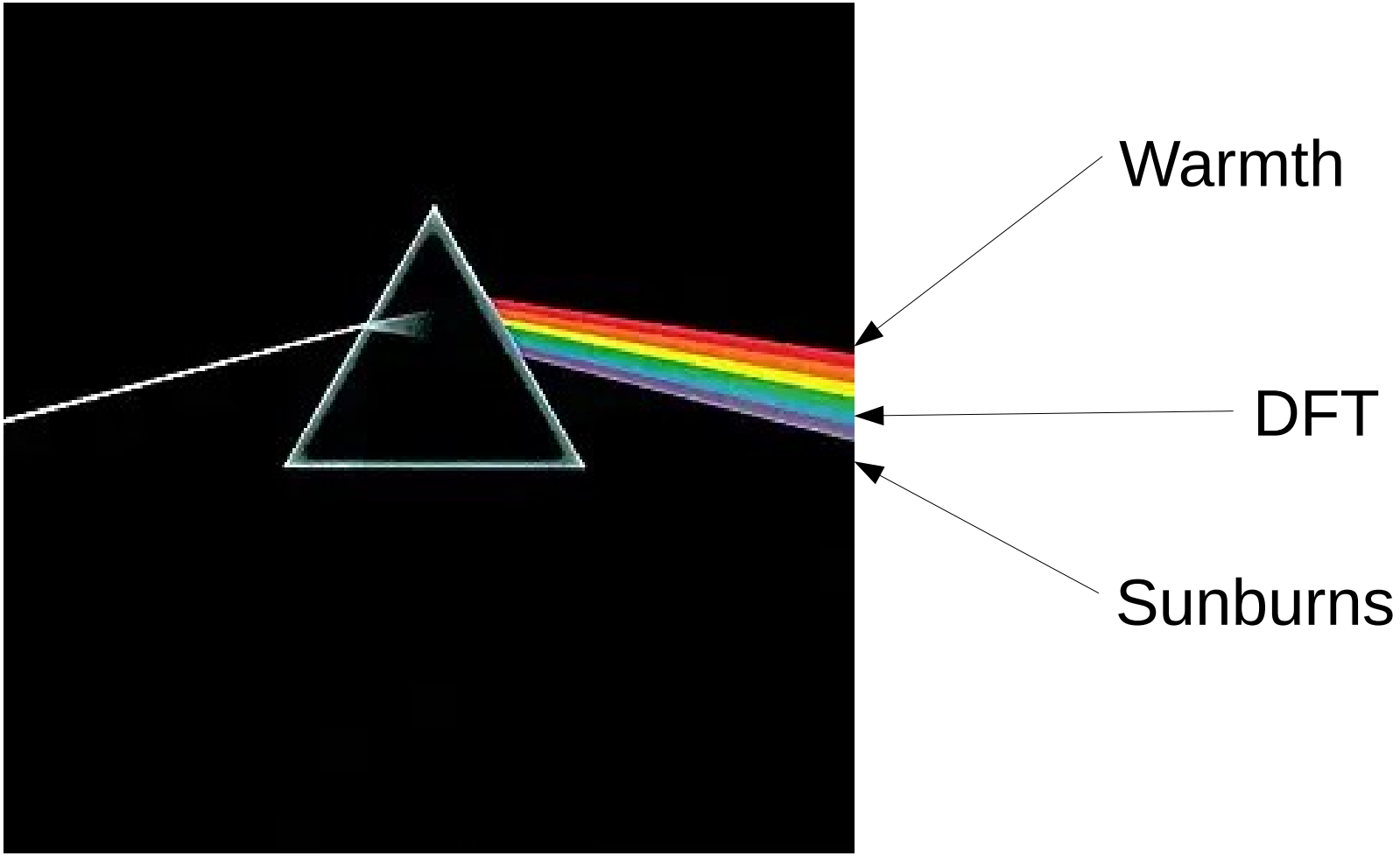
https://www.theatlantic.com/technology/archive/2011/12/the-great-wireless-hack-of-1903/250665/


CubicSDR v0.2.5 :: www.cubicsdr.com
File
Settings
Sample Rate
Audio Sample Rate
Recording
Rig Control
Display
FM
FMS
NBFM
AM
LSB
USB
DSB
I/Q
Modem Settings
99.900
FM
Frequency
Bandwidth
Center Frequency
99900000
200000
100000000
Search..
Active
99.9MHz FM
View Ranges
Bookmarks
Recents
99.90191MHz FM
Label
Freq 99.9MHz
BW 200KHz
Type FM
Bookmark..
Start Recording
Remove Active

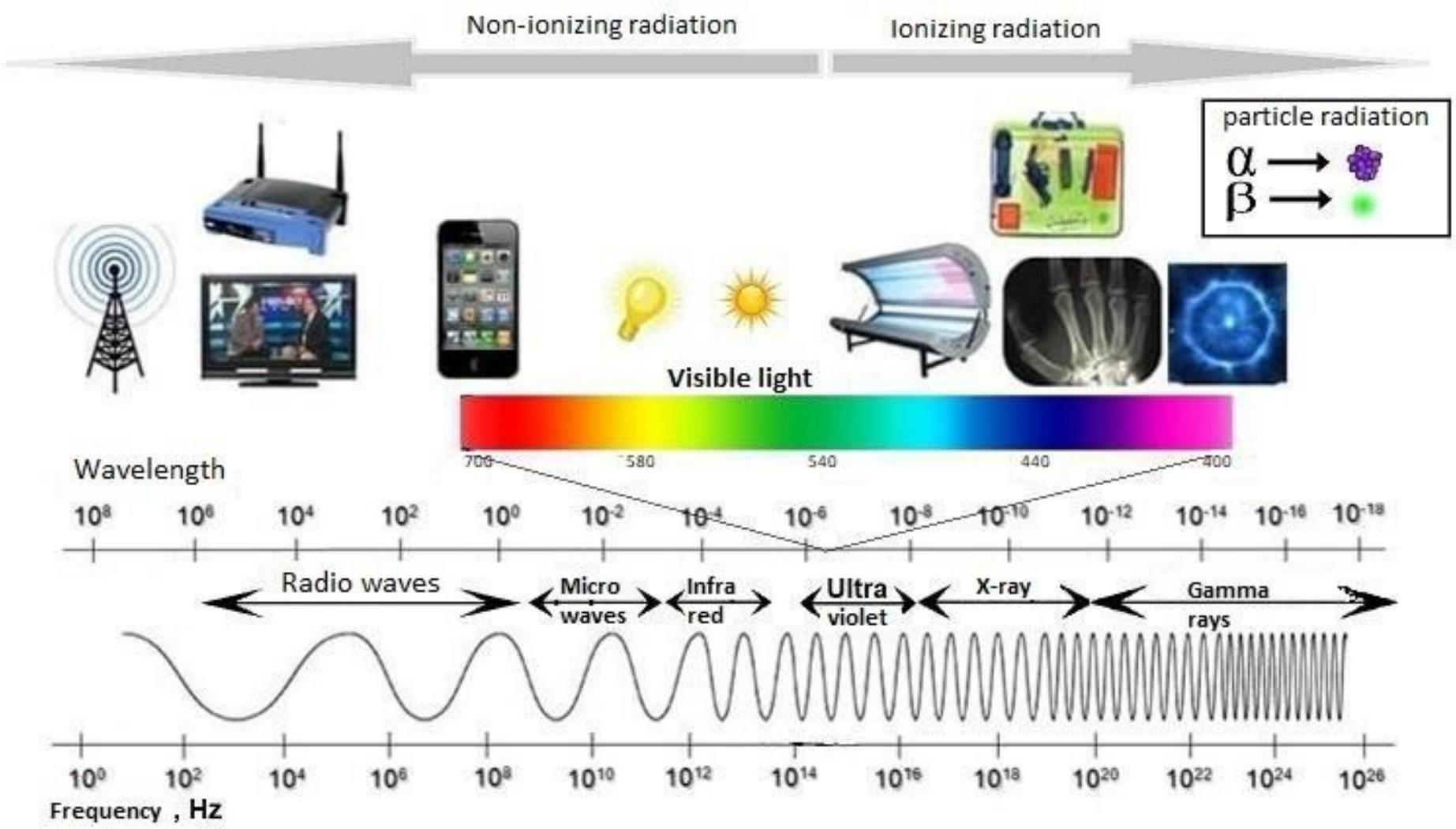

Gqrx 2.15.8 - hackrf=9284c3
File Tools View Help
2.450.000.000
-100 -80 -60 -40 -20 0
-53.7 dBFS
-40
-60
-80
2445
2446
2447
2448
2449
2450
2451
2452
FFT Settings
FFT size 8192
RBW: 976.6 Hz
Rate 60 fps
Overlap: 0%
Time span Auto
Res: 0.02 s
Window Hann
Averaging
Panadapter
Waterfall
Peak Detect Hold
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

Warmth

Sunburns

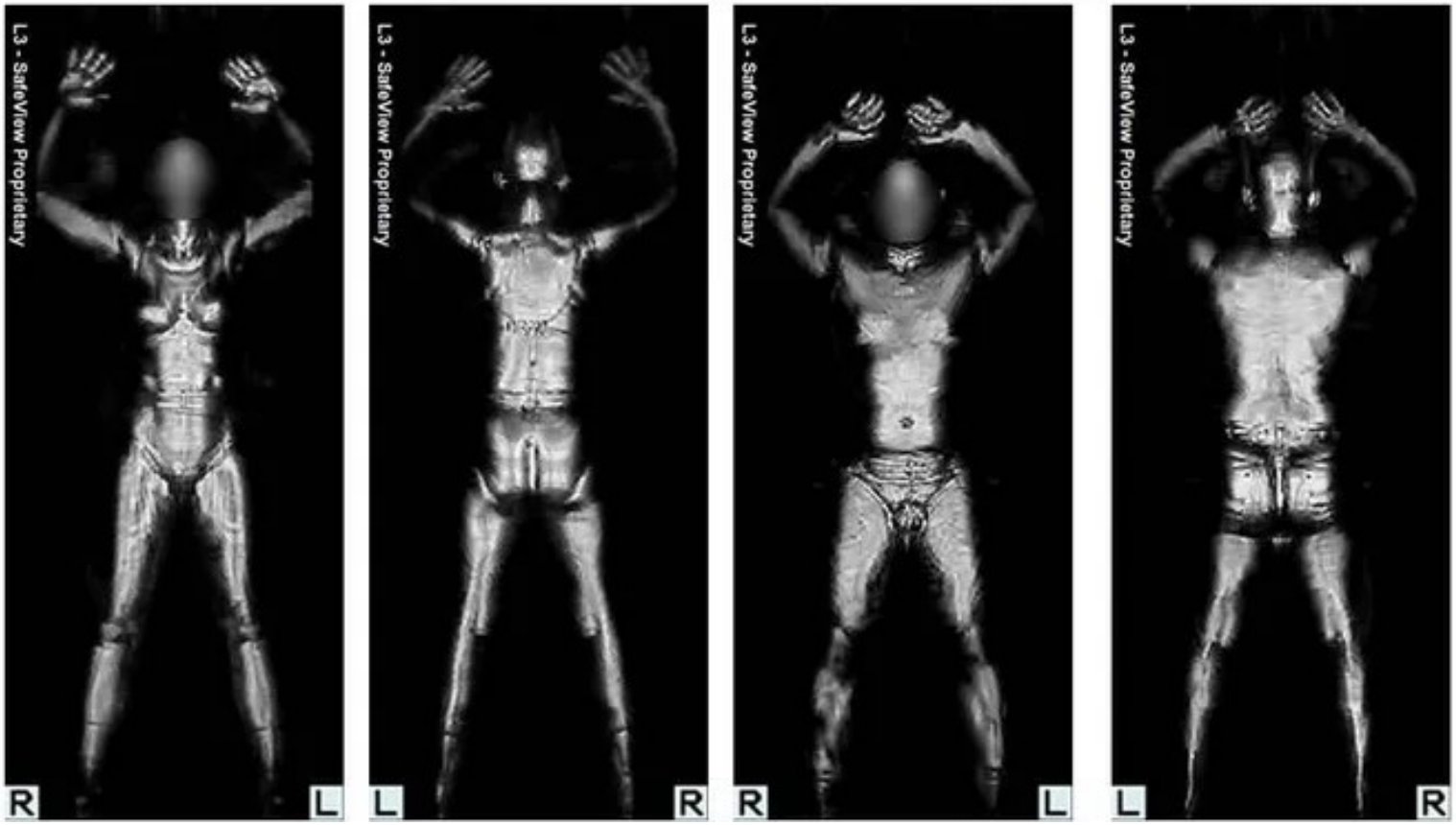

Warmth
DFT
Sunburns

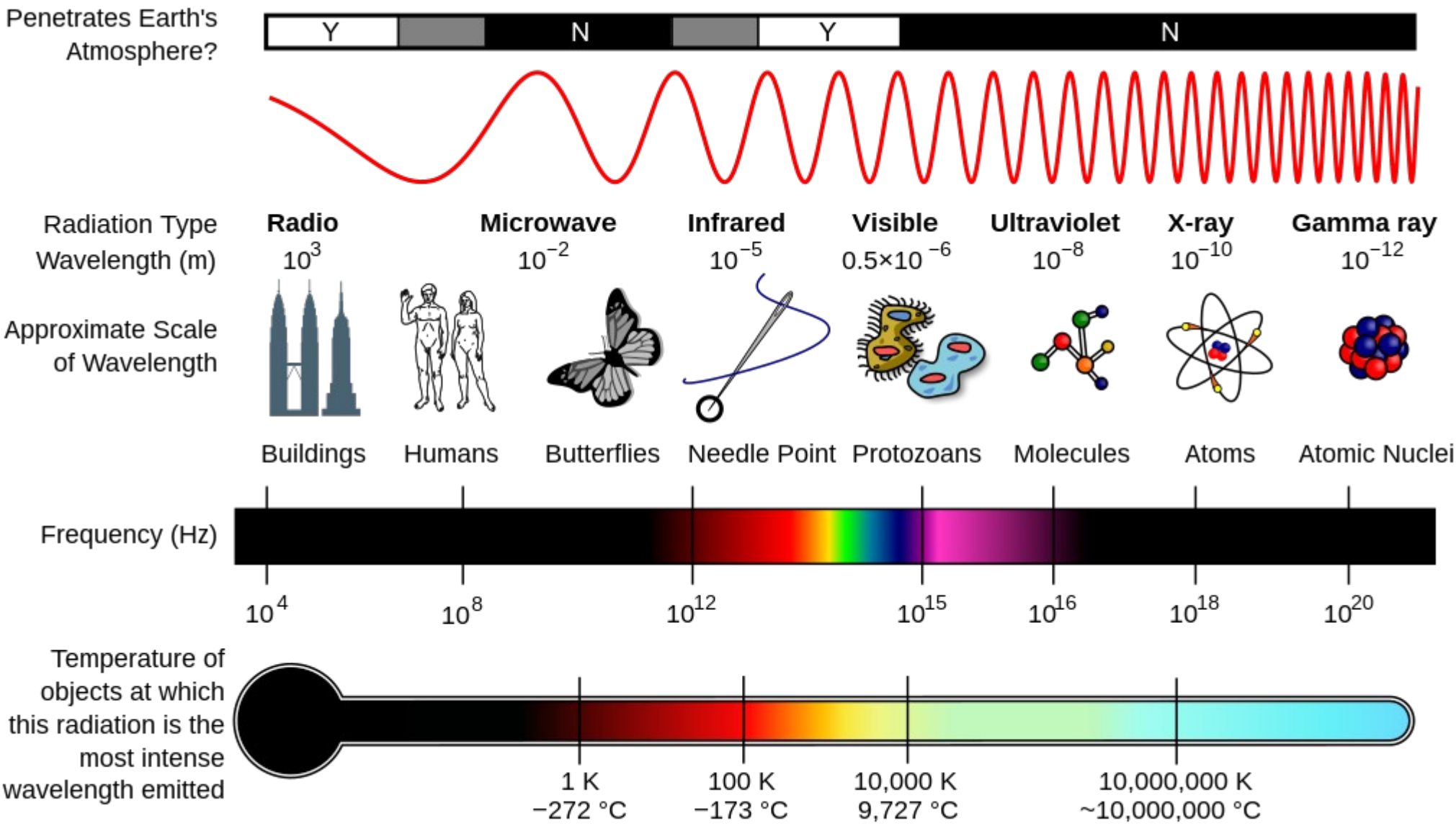
The electromagnetic spectrum



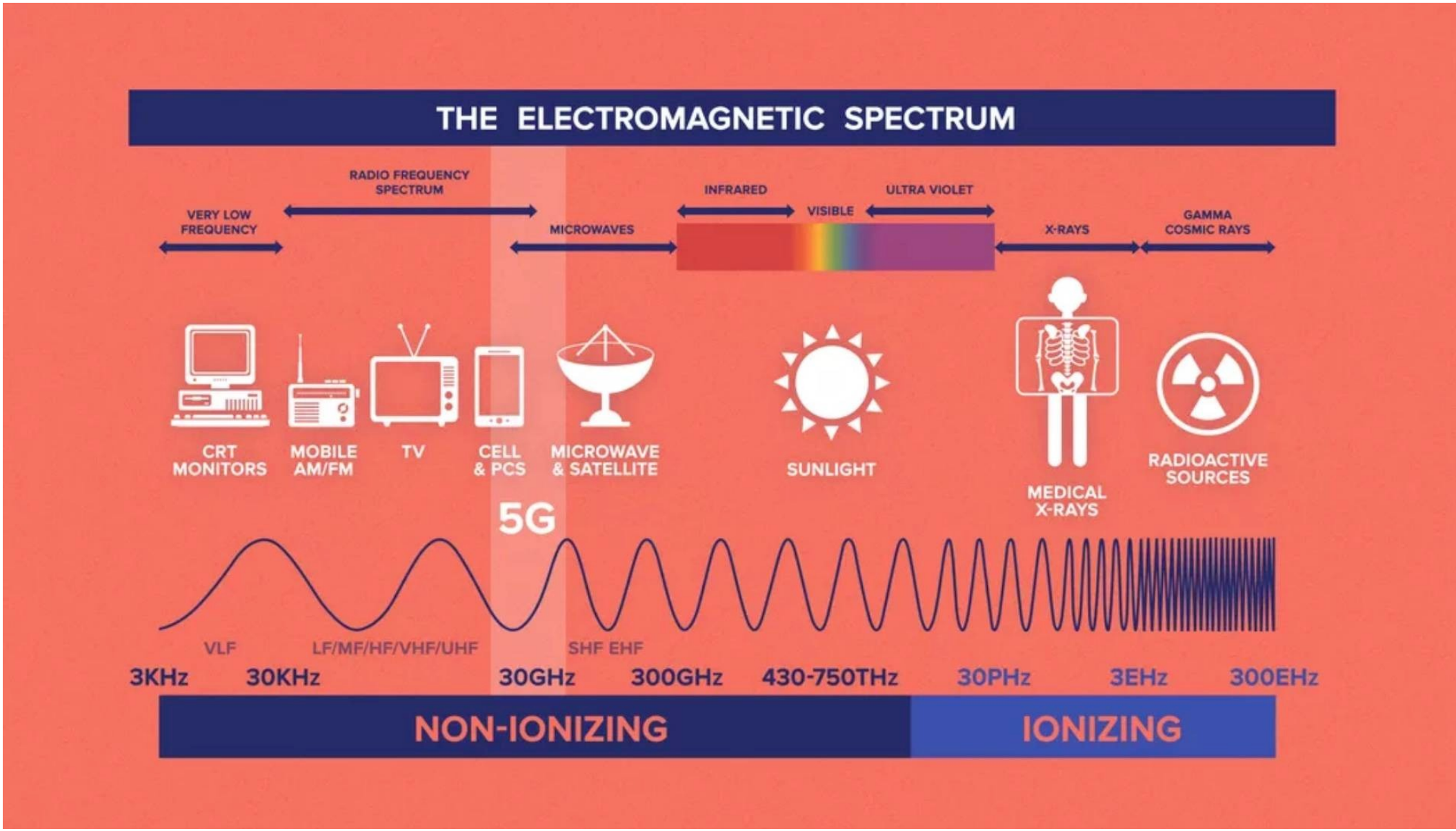
https://www.uib.no/en/hms-portalen/75292/electromagnetic-spectrum

https://www.usatoday.com/story/travel/roadwarriorvoices/2015/08/17/tsa-has-spent-160-million-on-body-scanners-and-theyre-still-terrible/83288622/





https://commons.wikimedia.org/wiki/File:EM_Spectrum_Properties_edit.svg



https://www.islandssounder.com/news/part-i-the-hype-about-5g/

Doctors at the X-Ray be like: "This is completely safe, don't worry"

Also doctors at the X-Ray:

Microwaves

- EHF (Sir Jagadish Chandra Bose – Bengali scientist) 30 to 300GHz
  - Point-to-point, satellite, IEEE 802.11ay (20 Gbps), security screening at the airport, 5G
- SHF – 3 to 30 GHz
  - Point-to-point, radar, satellite phones, microwave ovens, 5G
- UHF – 300 MHz to 3 GHz
  - TV, cell phones, satellites, GPS, WiFi, Bluetooth, walkie talkies, garage door openers, industrial controllers

https://www.reddit.com/r/nostalgia/comments/ut3emp/80s_tv_knobs_bonus_points_for_describing_the_feel/

Radio waves

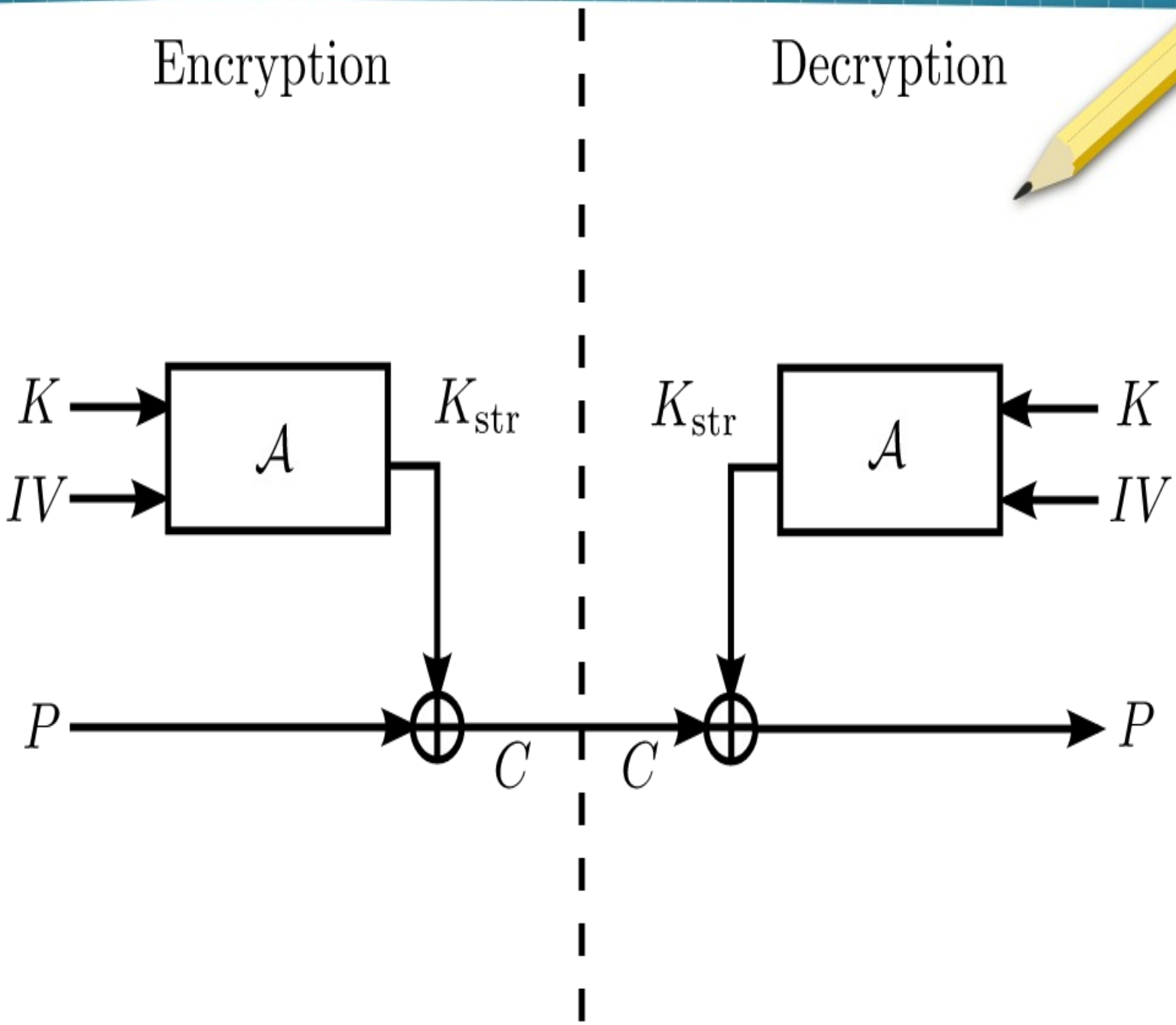
- VHF – 30MHz to 300MHz
  - Line of sight, but refracted up to 100 miles or so
  - FM radio, TV, amateur radio
- HF – 3MHz to 30MHz
  - Reflected off the ionosphere
  - Military, amateur radio, maritime, CB radio
- MF – 300KHz to 3 MHz
  - AM radio, maritime

As you go lower than 300 KHz...

- Weather, beacons, time, radio in other parts of the world, RFID, submarine communications

WiFi security…

- Why stream ciphers?
- WEP
  - IVs reused because of birthday principle
- WPA2
  - IVs reused because of key re-installation (KRACK attacks)
- WPA3
  - Dragonblood side channels
- FragAttacks on WPA2 and WPA3



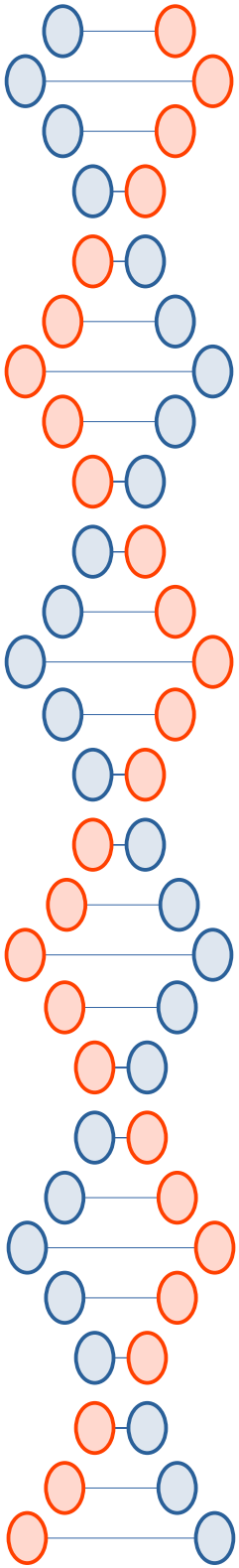
https://commons.wikimedia.org/wiki/File:Stream_cipher.svg

Good things about stream ciphers

- Can pre-compute key material, encryption/decryption is just XOR
- Can send small bursts without wasting space on padding
- More modular implementation in hardware
  - IV and key are only inputs
- Some stream ciphers that are not based on block ciphers are very fast
  - *E.g.*, RC4

Playing with fire?

- You should NEVER reuse key material
  - Harder than it sounds
    - Handshake protocols, *etc.* might have replay attacks
    - APIs, education
    - Downgrade attacks
- You should NEVER assume that successful decryption is the same as authentication
  - Even worse to assume this than it is for block ciphers



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

A theme we will see in asymmetric cryptography…

Crypto protocols and network protocols sometimes don't always play nicely together.

(Messages can be lost, modified, replayed, dropped, *etc.*)

WiFi security

Basically three use cases

-Open

-Personal (e.g., a passphrase)

-Enterprise

https://securityuncorked.com/2022/07/wifi-security-the-3-types-of-wifi-networks/

WiFi security in a nutshell

WEP is very bad

- Can be broken in seconds/minutes

WPA was only a stop gap

- RC4 hardware

WPA2 is maybe okay for now if you do it right?

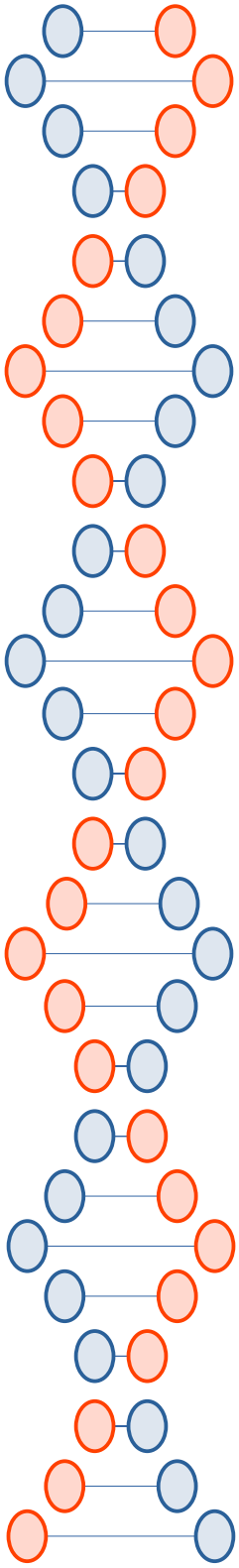
- Notion of personal *vs.* enterprise introduced here
- KRACK attacks, FragAttacks

WPA3 is better, maybe?

- Dragonblood attacks, FragAttacks
- Open no longer means just “unencrypted”

WEP

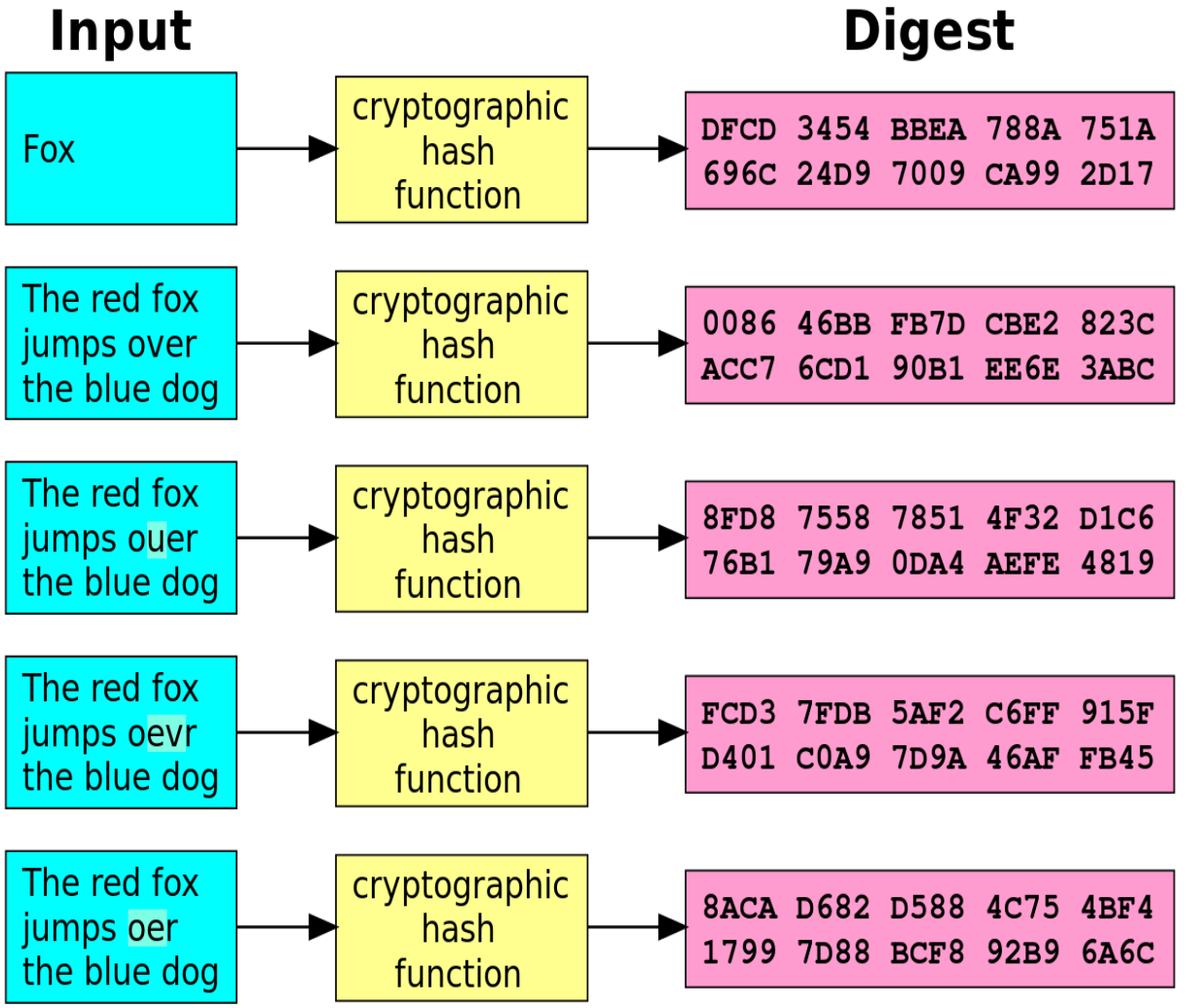
- IV is only 24 bits
- No real authentication
  - CRC is not a cryptographic hash function

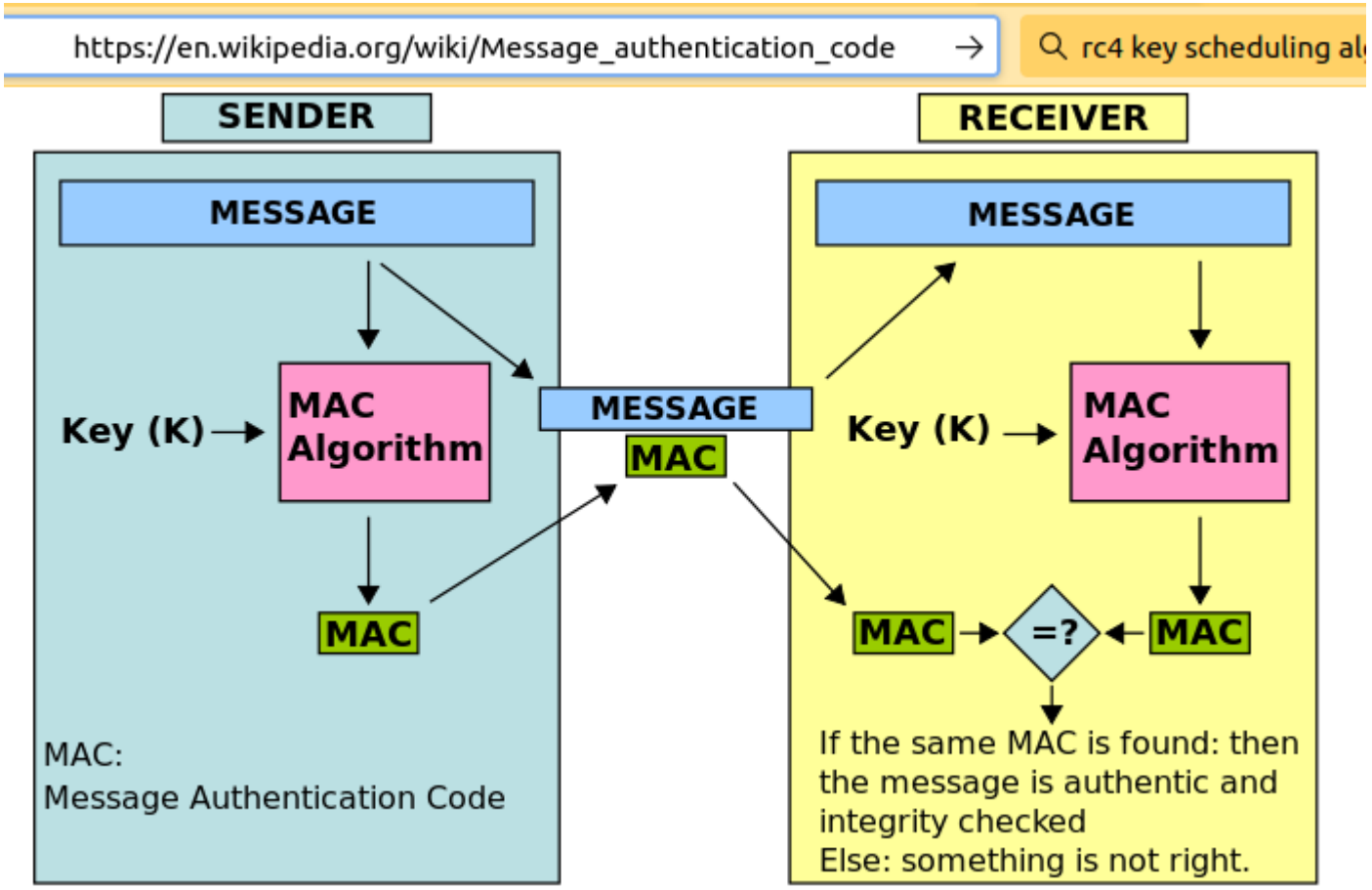


Why hash functions?

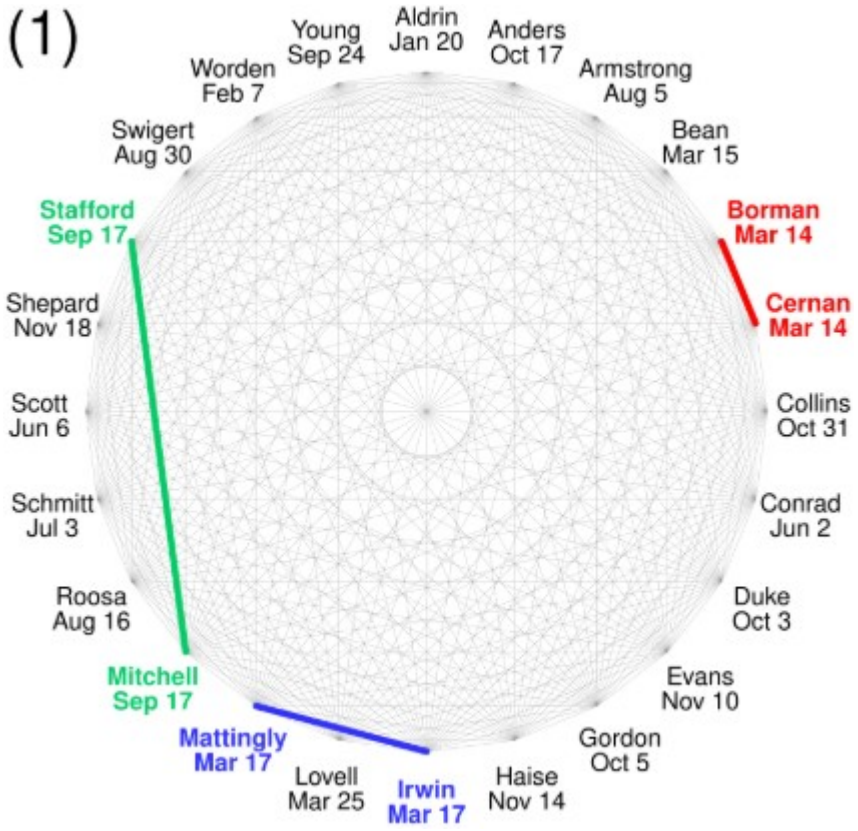
- Speed
  - Symmetric crypto is generally faster than asymmetric
  - Hashes are generally faster than either
- Error detection (*e.g.*, checksum)
- Security and privacy
  - Secure hash functions should avoid collisions in adversarial settings.

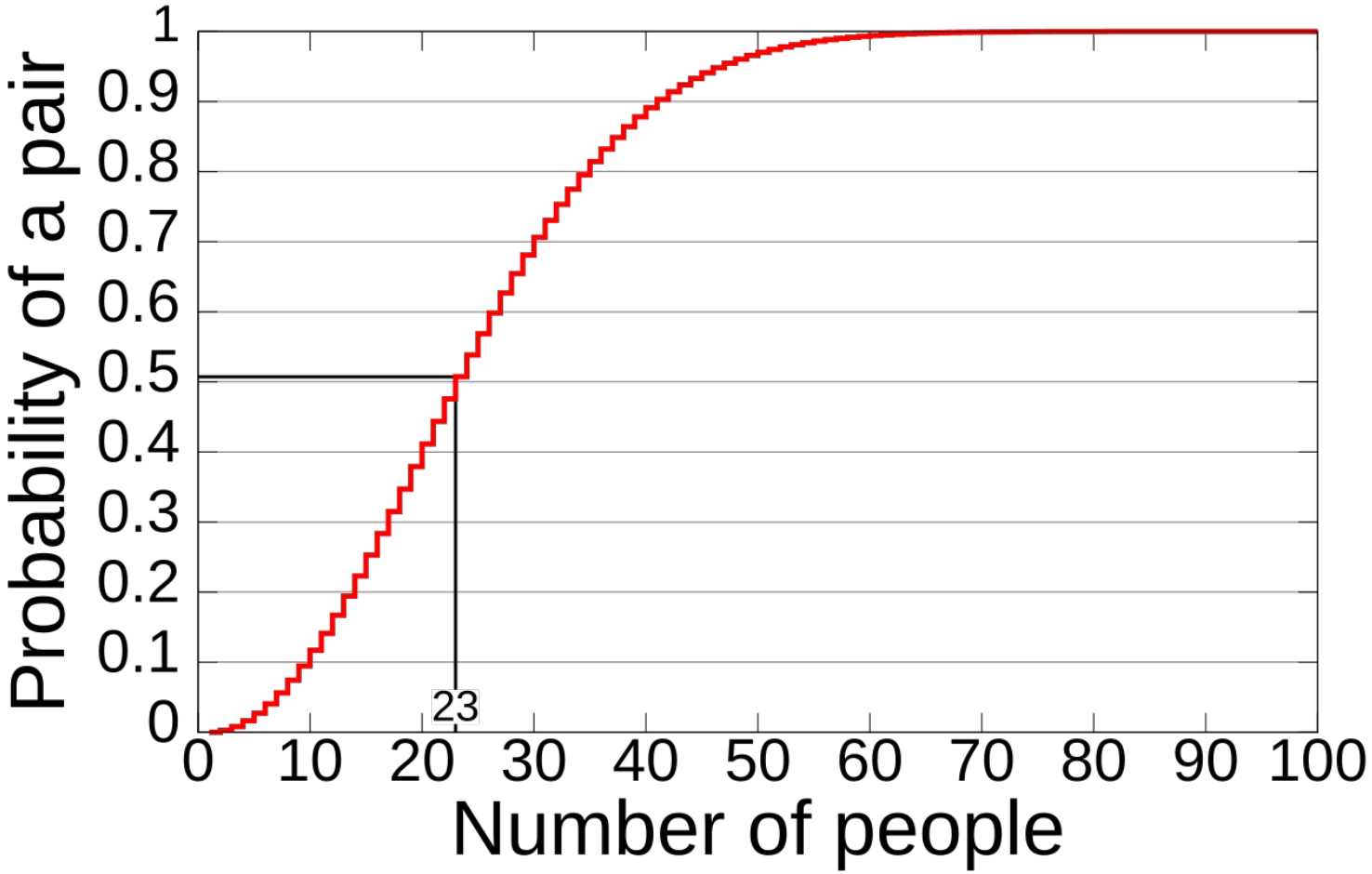
Cryptographic hash function example...




https://en.wikipedia.org/wiki/Message_authentication_code
rc4 key scheduling al
SENDER
RECEIVER
MESSAGE
MESSAGE
Key (K)
MAC Algorithm
MESSAGE
MAC
Key (K)
MAC Algorithm
MAC
MAC
=?
MAC
MAC:
Message Authentication Code
If the same MAC is found: then the message is authentic and integrity checked
Else: something is not right.

https://en.wikipedia.org/wiki/Birthday_attack




Probability of a pair
1
0.9
0.8
0.7
0.6
0.5
0.4
0.3
0.2
0.1
0
0
10
20
30
40
50
60
70
80
90
100
23
Number of people

This process can be generalized to a group of n people, where $p(n)$ is the probability of at least two of the n people sharing a birthday. It is easier to first calculate the probability $\bar{p}(n)$ that all n birthdays are *different*. According to the pigeonhole principle, $\bar{p}(n)$ is zero when $n > 365$. When $n \leq 365$:

$$\bar{p}(n) = 1 \times \left(1 - \frac{1}{365}\right) \times \left(1 - \frac{2}{365}\right) \times \cdots \times \left(1 - \frac{n-1}{365}\right)$$

The Taylor series expansion of the exponential function (the constant $e \approx 2.718\,281\,828$)

$$e^x = 1 + x + \frac{x^2}{2!} + \cdots$$

provides a first-order approximation for e^x for $|x| \ll 1$:

$$e^x \approx 1 + x.$$

To apply this approximation to the first expression derived for $\bar{p}(n)$, set $x = -\frac{a}{365}$. Thus,

$$e^{-a/365} \approx 1 - \frac{a}{365}.$$

Then, replace a with non-negative integers for each term in the formula of $\bar{p}(n)$ until $a = n - 1$, for example, when $a = 1$,

$$e^{-1/365} \approx 1 - \frac{1}{365}.$$

The first expression derived for $\bar{p}(n)$ can be approximated as

$$\begin{aligned}\bar{p}(n) &\approx 1 \cdot e^{-1/365} \cdot e^{-2/365} \cdots e^{-(n-1)/365} \\ &= e^{-\left(1+2+\cdots+(n-1)\right)/365} \\ &= e^{-\frac{n(n-1)/2}{365}} = e^{-\frac{n(n-1)}{730}}.\end{aligned}$$

$$p(n, d) \approx 1 - e^{-\frac{n(n-1)}{2d}}$$

Therefore,

$$p(n) = 1 - \bar{p}(n) \approx 1 - e^{-\frac{n(n-1)}{730}}.$$

An even coarser approximation is given by

$$p(n) \approx 1 - e^{-\frac{n^2}{730}},$$

A good rule of thumb which can be used for mental calculation is the relation

$$p(n, d) \approx \frac{n^2}{2d}$$

which can also be written as

$$n \approx \sqrt{2d \times p(n)}$$

which works well for probabilities less than or equal to $\frac{1}{2}$. In these equations, d is the number of days in a year.

For instance, to estimate the number of people required for a $\frac{1}{2}$ chance of a shared birthday, we get

$$n \approx \sqrt{2 \times 365 \times \tfrac{1}{2}} = \sqrt{365} \approx 19$$

Which is not too far from the correct answer of 23.

WEP encryption

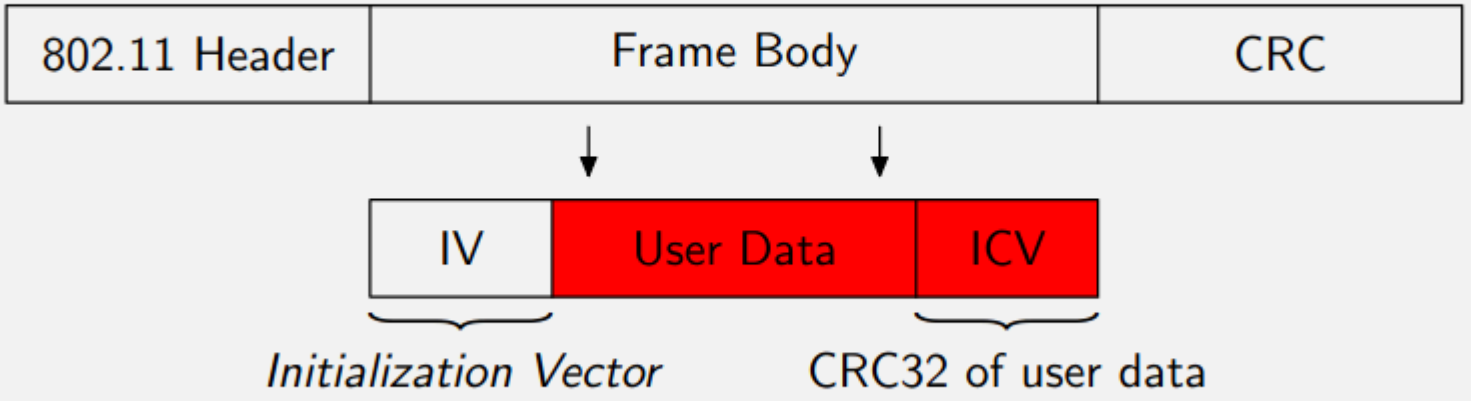
“Wired Equivalent Privacy”

-Have to be physically in a building to plug in, have to know the passphrase to join WiFi (or do you?)

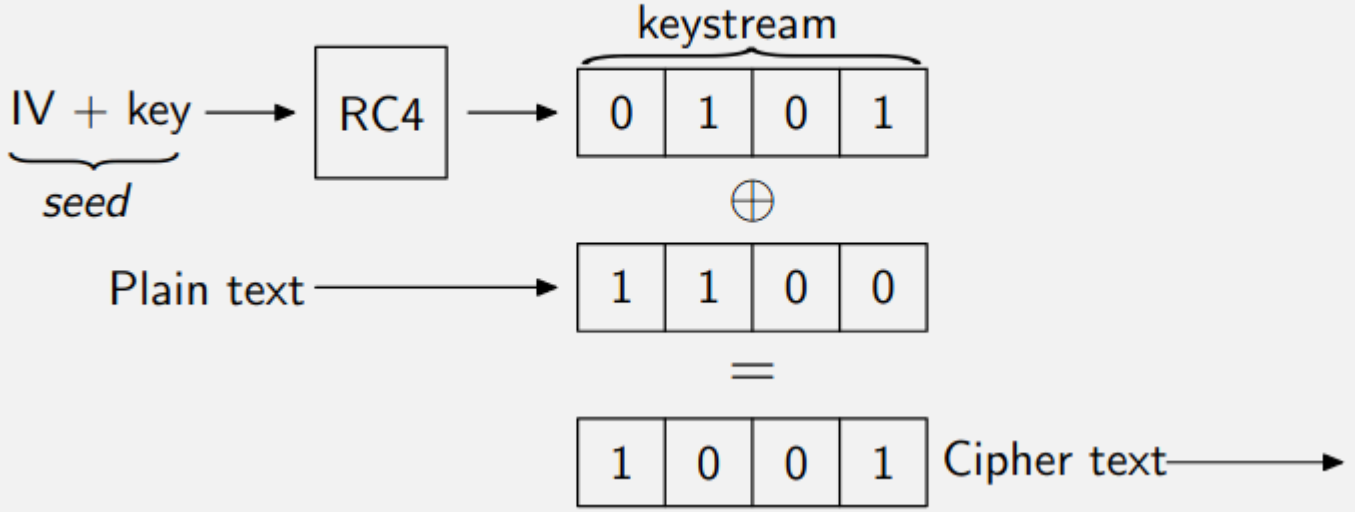
RC4, 40-bit key, 24-bit IV

Following are from: https://jedcrandall.github.io/courses/cse468fall2022/wep/198fbe890b692e5296fcf7ad1b015e653ec9.pdf

Data frame format



Encryption



If cipher-text & plain-text pair is known, their XOR is a keystream.
Known plain-text (LLC/SNAP headers) in IP packets:

802.11 header	0xAA	0xAA	0x03	0x00	0x00	0x00	0x08	0x00

$\oplus$

802.11 header	Cipher-text

$=$

8 bytes of keystream

Can recover 8 bytes of keystream by eavesdropping a packet.

- Can encrypt (and transmit) 8 bytes of arbitrary data.

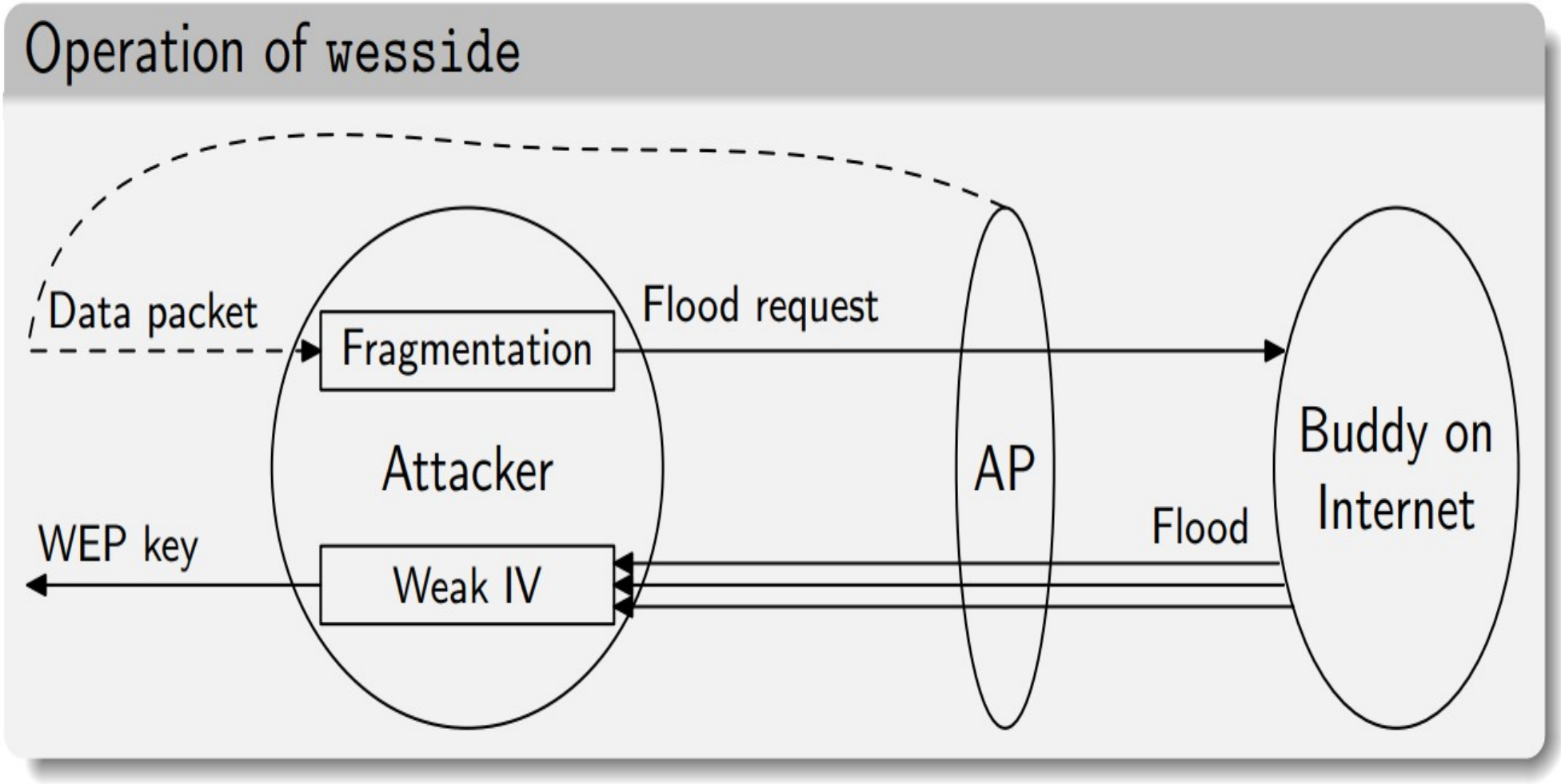
rc4-3.py

Possible to create statistical biases in the Key Scheduling Algorithm (KSA)

More info:

https://www.youtube.com/watch?v=2o3Hs-JDWLs

Crack WEP key in minutes…



WPA2

- IV is 48 bits (128-bit key with AES in a special counter mode called CCMP)
- SHA1 HMAC for authentication (called a MIC)
  - 160 bits

KRACK attacks...

https://www.youtube.com/watch?v=fZ1R9RliM1w



https://papers.mathyvanhoef.com/ccs2017.pdf

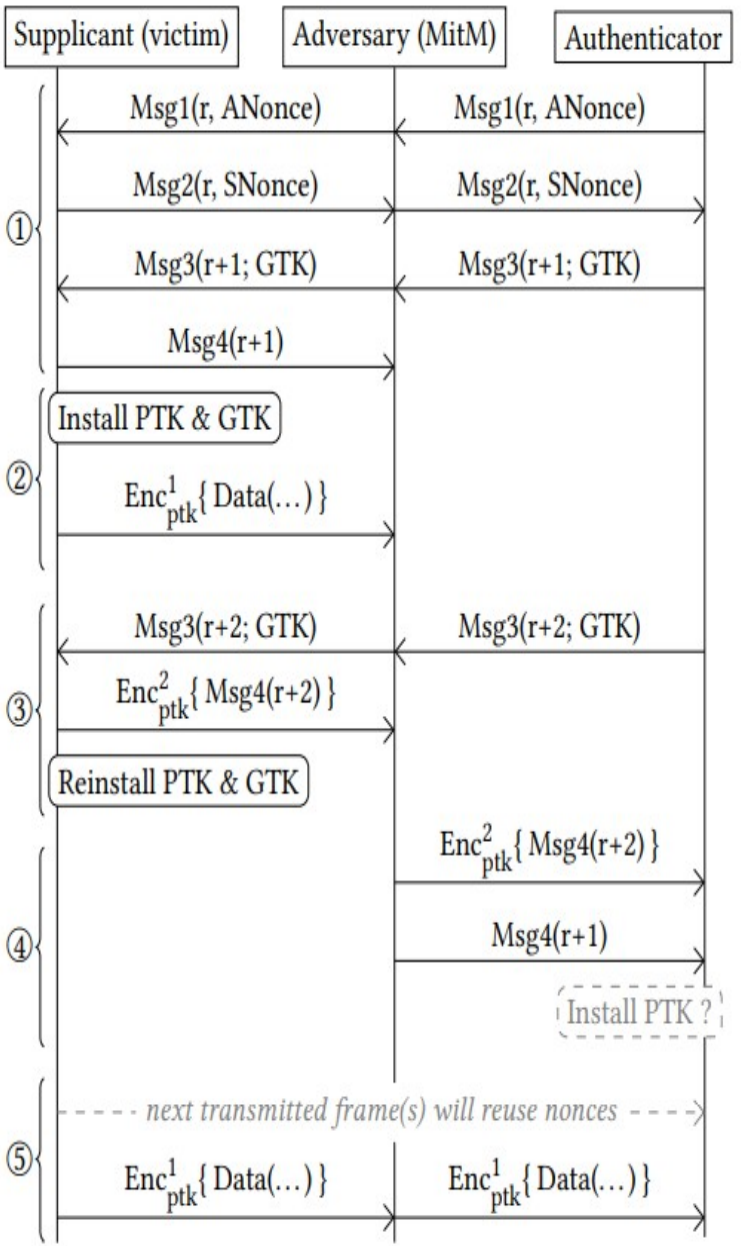
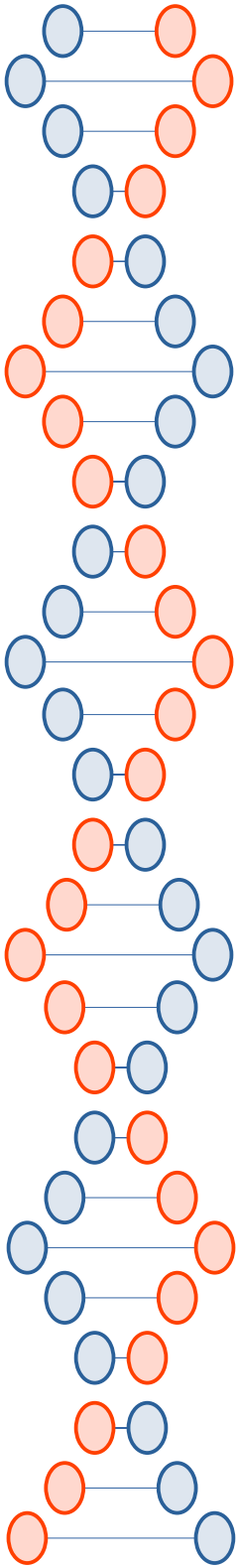


Figure 4: Key reinstallation attack against the 4-way handshake, when the supplicant (victim) still accepts plaintext retransmissions of message 3 if a PTK is installed.

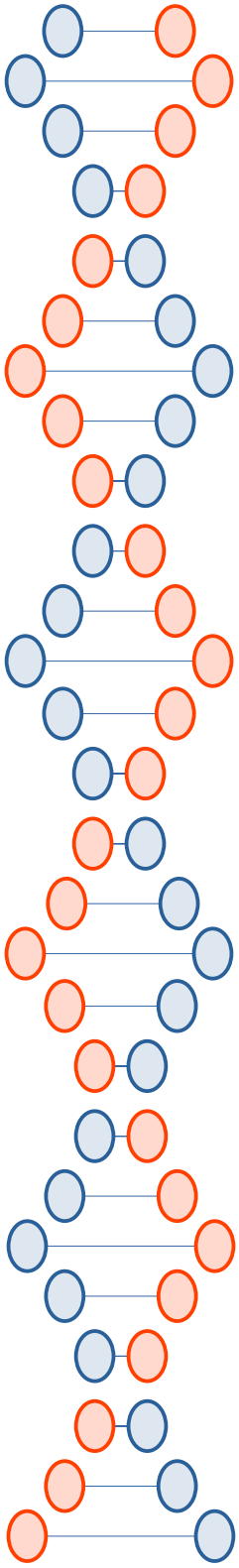
KRACK attacks



Dragonblood attacks on WPA3

- Downgrade attacks (enterprise)
- Side channel (personal)
- Slides plagiarized from…

  https://papers.mathyvanhoef.com/wac2019-slides.pdf



Convert password to MODP element

```
for (counter = 1; counter < 256; counter++)
    value = hash(pw, counter, addr1, addr2)
    if value >= p: continue
    P = value^((p-1)/q)
    return P
```

16

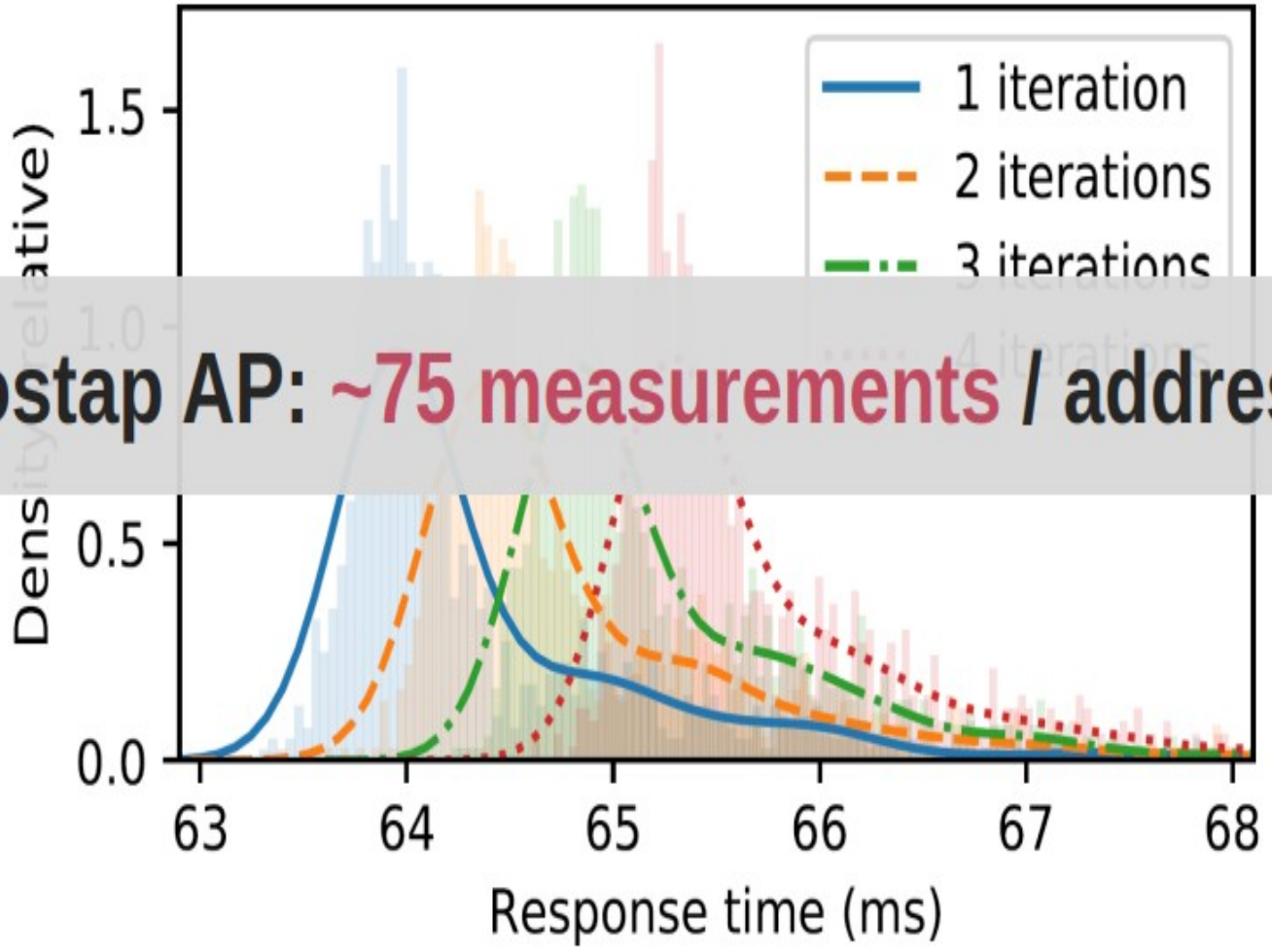
Leaked information: #iterations needed

Leaked information: #iterations needed

Forms a signature of the password

Need ~17 addresses to determine password in RockYou (~10^7) dump

Raspberry Pi 1 B+: differences are measurable



Hostap AP: ~75 measurements / address

29

FragAttacks

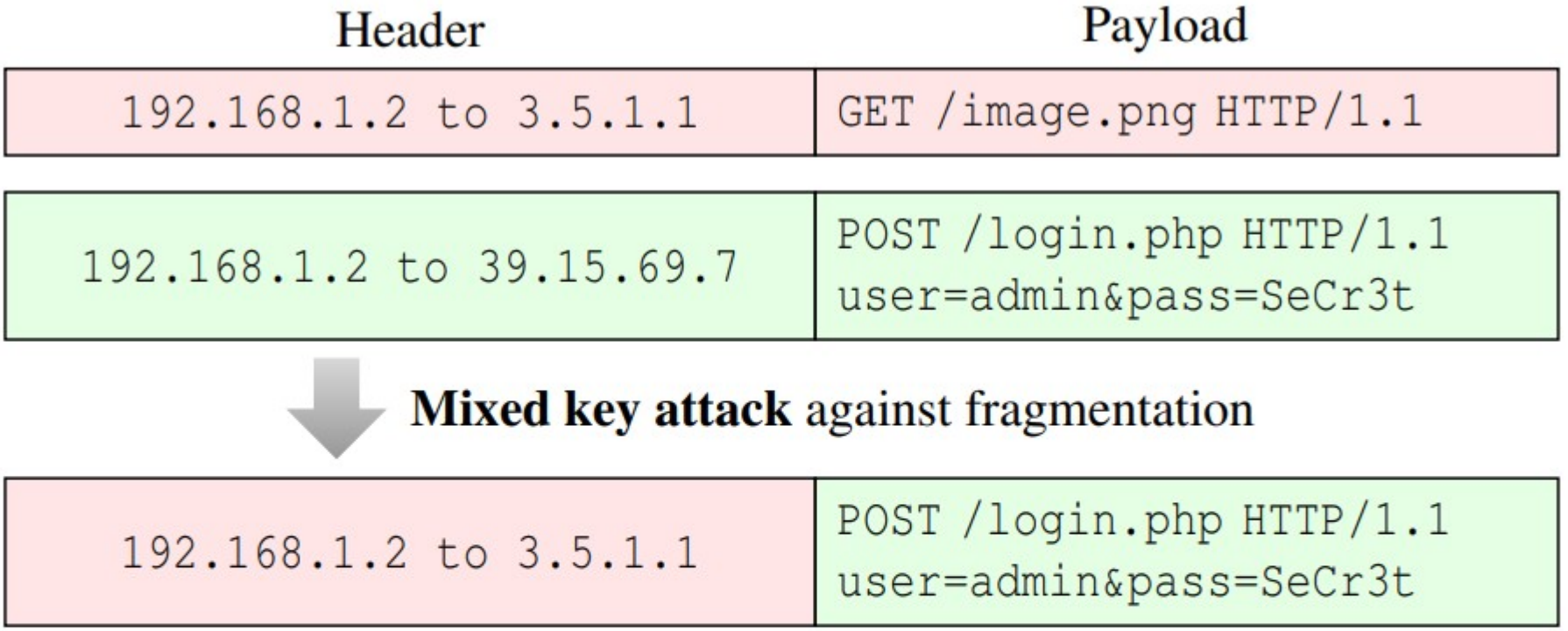


Figure 5: Mixing fragments of two packets to exfiltrate user data to an attacker-controlled server. The red packet is sent to the attacker's server, and the green packet contains user data.

https://eprint.iacr.org/2021/763.pdf

BACKUP SLIDES...

Many other stream cipher fails...

ShadowSocks

- Let’s the user choose between non-AEAD and AEAD ciphers, with many options for each
  - AEAD = Authenticated Encryption with Associated Data
  - Most implementations don’t support AEAD
    - No authentication of messages

Following is from…
https://www.idcoffer.com/wp-content/uploads/2020/02/Redirect-attack-on-Shadowsocks-stream-ciphers.pdf

Ciphers of shadowsocks:

Shadowsocks support the two kinds of ciphers:

Steam ciphers (none-AEAD cipher):

Rc4-md5, salsa20,chacha20,chacha-ietf, aes-ctf, bf-cfb, camellia-cfb, aes-cfb

AEAD ciphers:

aes-gcm,chacha-ietf-poly1305,xchacha20-ietf-poly1305

What is ShadowSocks?

The Shadowsocks local component (ss-local) acts like a traditional SOCKS5 server and provides proxy service to clients. It encrypts and forwards data streams and packets from the client to the Shadowsocks remote component (ss-remote), which decrypts and forwards to the target. Replies from target are similarly encrypted and relayed by ss-remote back to ss-local, which decrypts and eventually returns to the original client.

client <---> ss-local <--[encrypted]--> ss-remote <---> target

[target address][payload]

Addresses used in Shadowsocks follow the SOCKS5 address format:

[1-byte type][variable-length host][2-byte port]

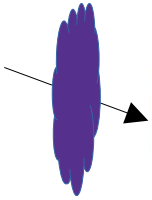
The following address types are defned:

0x01: host is a 4-byte IPv4 address.

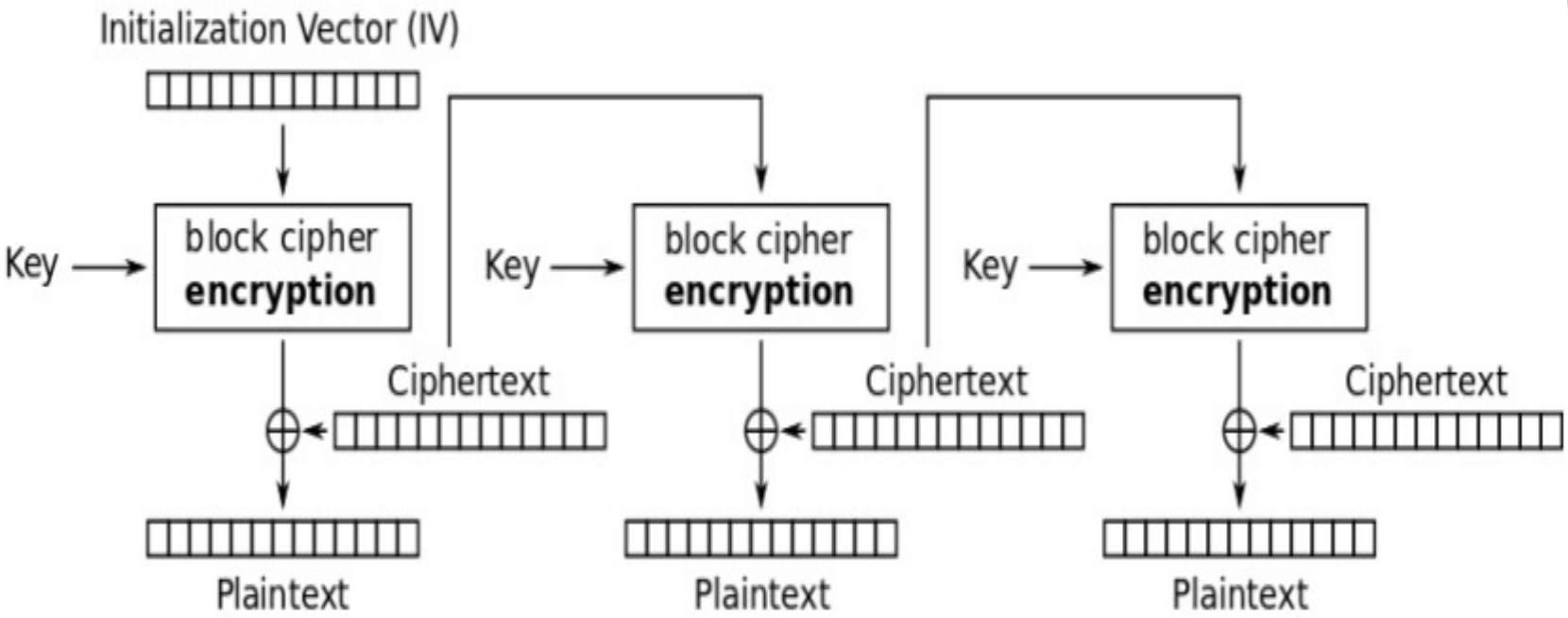
0x03: host is a variable length string, starting with a 1-byte length, followed by up to 255-byte domain name.

0x04: host is a 16-byte IPv6 address

The port number is a 2-byte big-endian unsigned integer.



[IV][encrypted payload]



Cipher Feedback (CFB) mode decryption

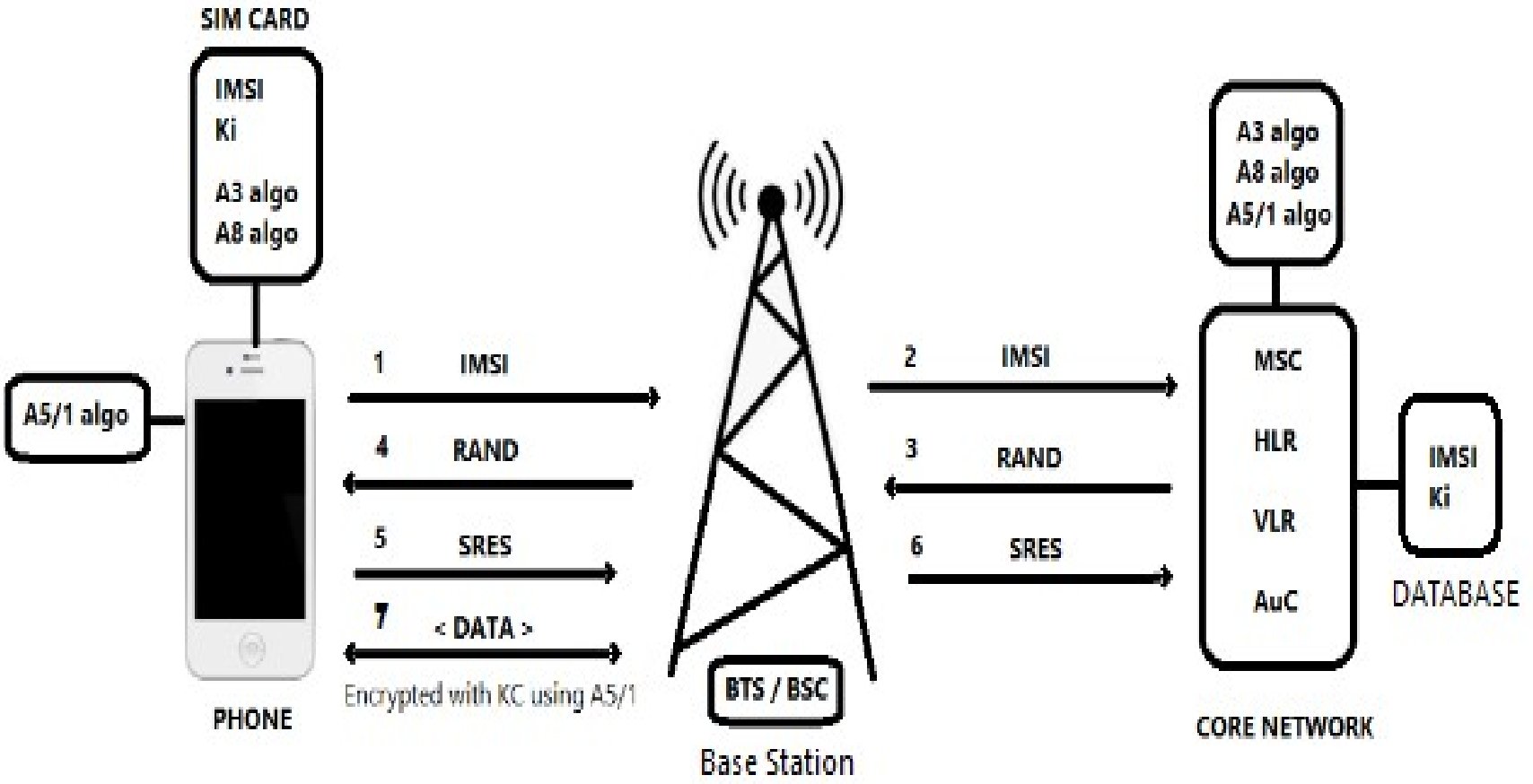
IVs are chosen randomly, transmitted in plaintext.

```
GET /html/en/reference/matrices/_sources/sage/mat
Host: doc.sagemath.org
Connection: keep-alive
Cache-Control: max-age=0
Upgrade-Insecure-Requests: 1
User-Agent: Mozilla/5.0 (Windows NT 10.0; WOW64)
Accept: text/html,application/xhtml+xml,applicati
Accept-Encoding: gzip, deflate
Accept-Language: zh-CN,zh;q=0.9,en;q=0.8
Cookie: __cfduid=ddc36b5813d7782ce467edb33058f732
__utma=138969649.1329315963.1545386824.154539484e
sphinxsidebar=visible; _gid=GA1.2.1229955866.1548
If-None-Match: W/"5c45d22a-127"
If-Modified-Since: Mon, 21 Jan 2019 14:07:38 GMT

HTTP/1.1 304 Not Modified
Date: Sat, 26 Jan 2019 09:59:47 GMT
Connection: keep-alive
Via: 1.1 varnish
Cache-Control: max-age=600
ETag: W/"5c45d22a-127"
Expires: Sat, 26 Jan 2019 10:09:47 GMT
Age: 0
```

```
root@DESKTOP-3UNO8NU:/mnt/g/code/shadowsocks/decrypt# nc -l -p 4626 >1.txt
^Z[10]   Killed                    nc -l -p 4626 > 1.txt

[11]+  Stopped                 nc -l -p 4626 > 1.txt
root@DESKTOP-3UNO8NU:/mnt/g/code/shadowsocks/decrypt# cat 1.txt
1 304 Not□i.□a□Q Sat, 26 Jan 2019 07:15:21 GMT
Connection: close
Via: 1.1 varnish
Cache-Control: max-age=600
ETag: W/"5c45d22a-127"
Expires: Sat, 26 Jan 2019 06:59:41 GMT
Age: 0
X-Served-By: cache-pao17445-PAO
X-Cache: MISS
X-Cache-Hits: 0
X-Timer: S1548486922.795009,VS0,VE25
Vary: Accept-Encoding
X-Fastly-Request-ID: 7f80e83d2fe5428bb3e38bb4e7d472af1b22eb4b
Server: cloudflare
CF-RAY: 49f1301d27589408-SJC
```

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

https://en.wikipedia.org/wiki/Type_B_Cipher_Machine#/media/File:Photograph_of_RED_cryptographic_device_-_National_Cryptologic_Museum_-_DSC07863.JPG



https://www.blackhillsinfosec.com/gsm-traffic-and-encryption-a5-1-stream-cipher/

Content Scramble System (CSS)

High-bandwidth Digital Content Protection

https://commons.wikimedia.org/wiki/File:Apple_TV,_1st_generation_-_mainboard_-_Silicon_Image_SiI1930CTU-3215.jpg