Network and Security Basics, Secure Hash Functions, Stream Ciphers, and WiFi

CSE 548 Spring 2026
jedimaestro@asu.edu

“For the mind does not require filling like a bottle, but rather, like wood, it only requires kindling to create in it an impulse to think independently and an ardent desire for the truth.”

-Plutarch

“Information only has meaning in that it is subject to interpretation”

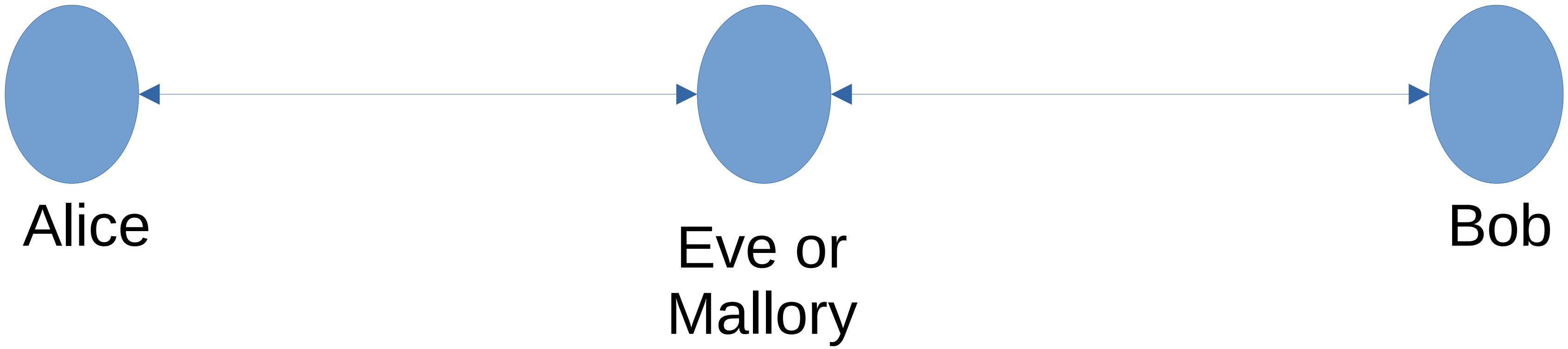
–Computer Viruses, Theory and Experiments by Fred Cohen, 1984

“The only laws on the Internet are assembly and RFCs”

–Phrack 65 article by julia@winstonsmith.info

“Information is inherently physical”

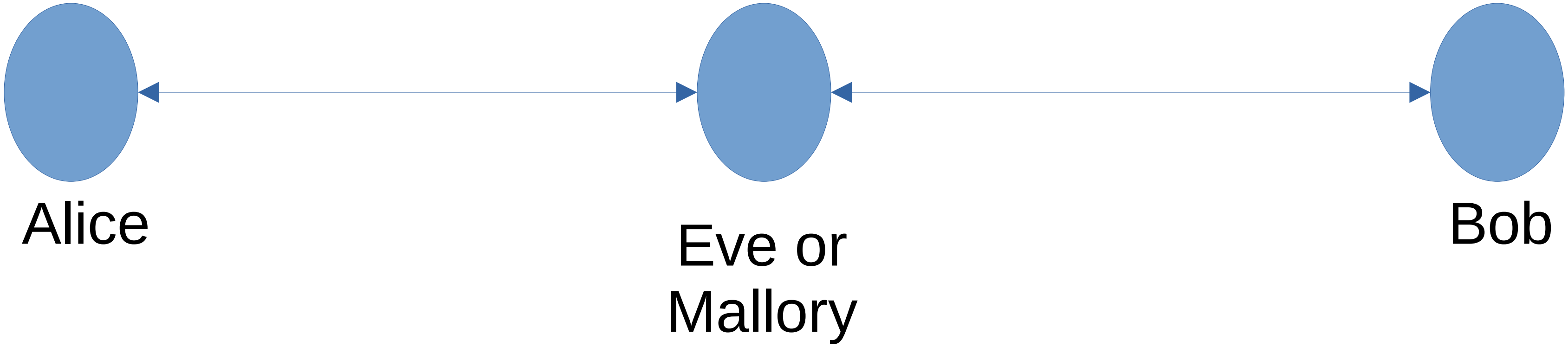
--(*Lots of people said this, but see Richard Feynman's Lectures on Computation*)



Alice

Eve or
Mallory

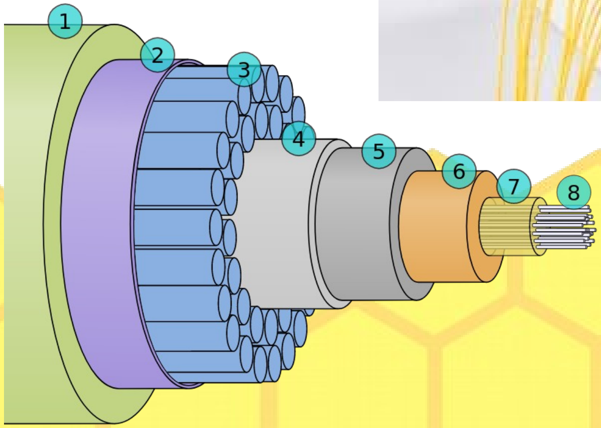
Bob



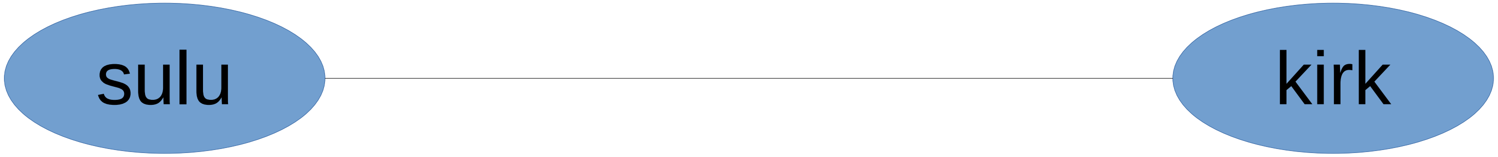
WiFi, electric path, or optical… Eve or Mallory get their own copy!

You want to connect two machines...

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

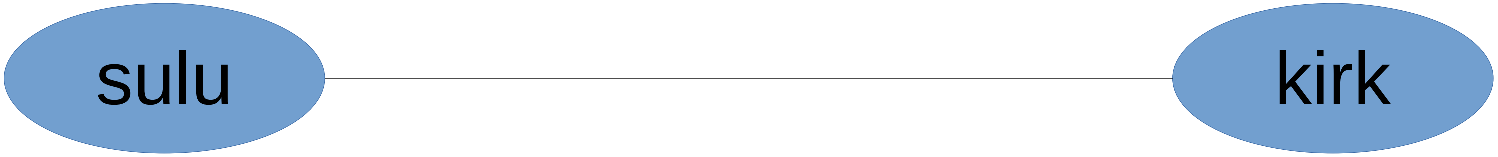


A “hop”

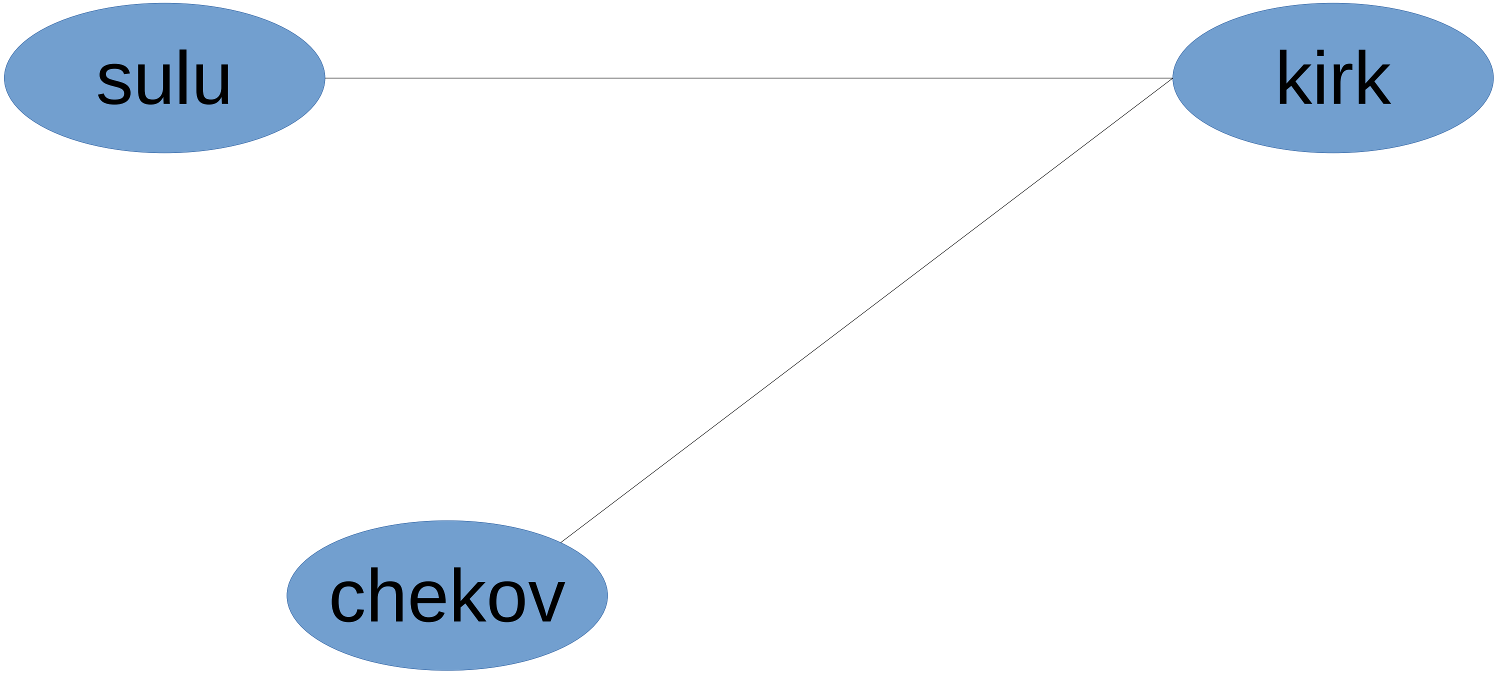


A “hop”

Ethernet

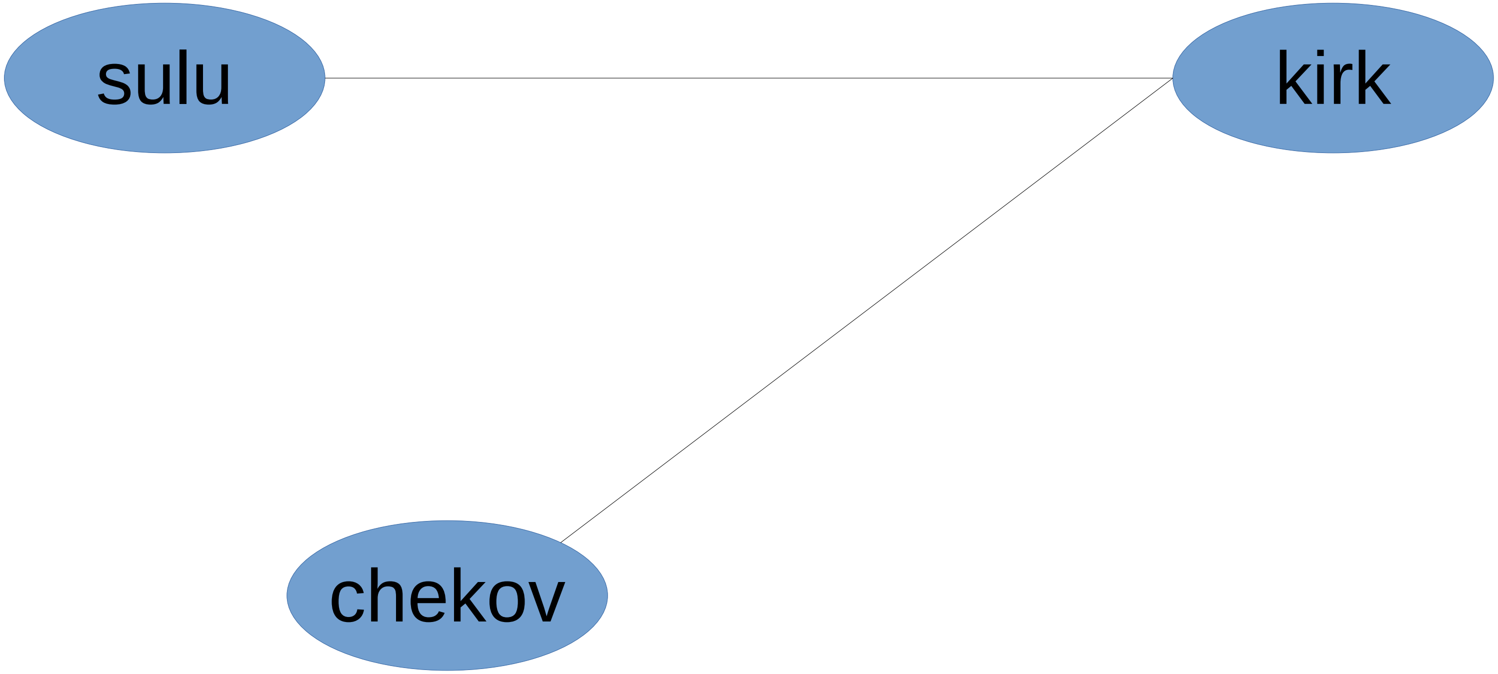


A “subnet”

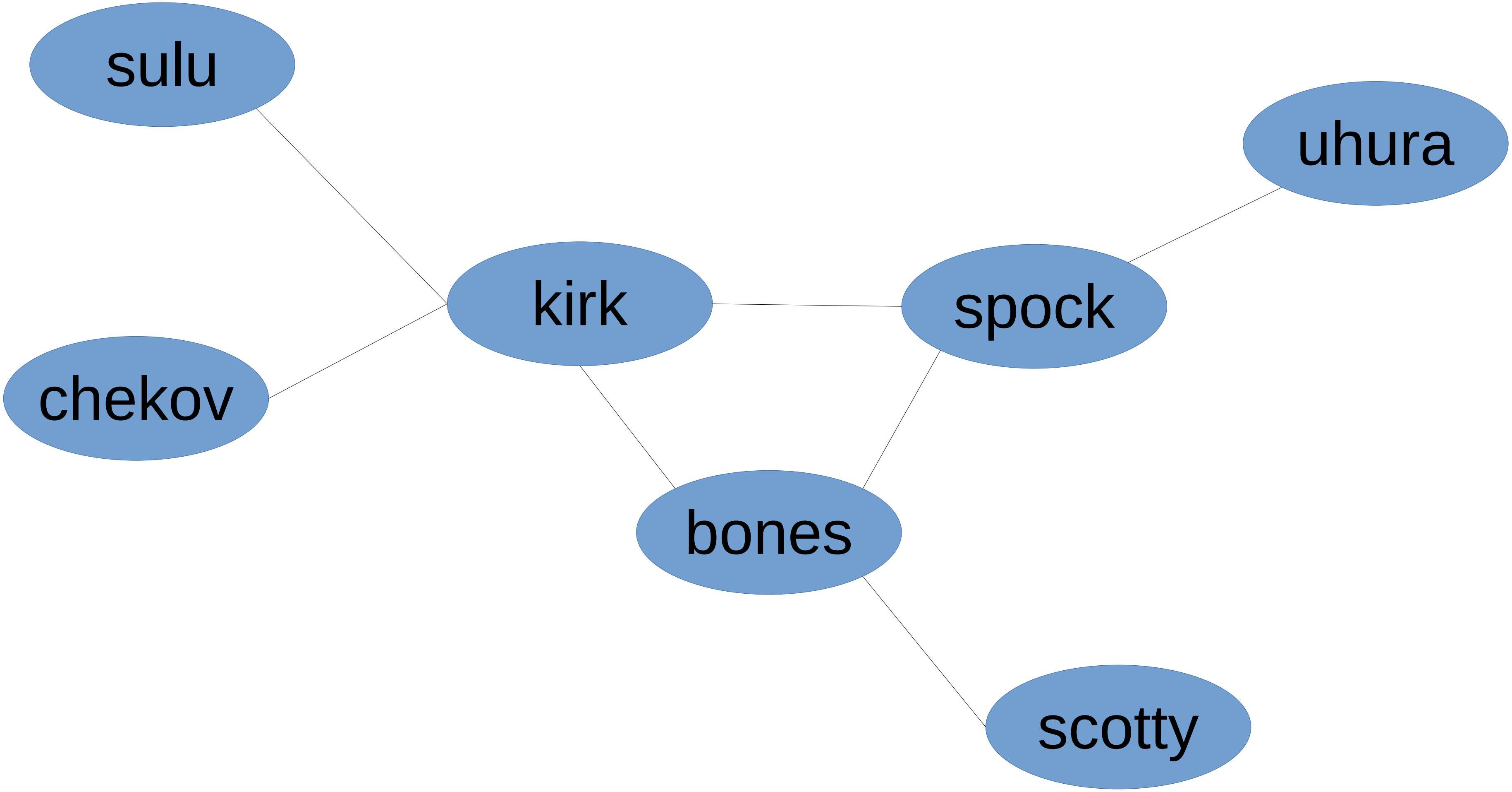


A “subnet”

ARP = Address Resolution Protocol



A network with routers



More terminology

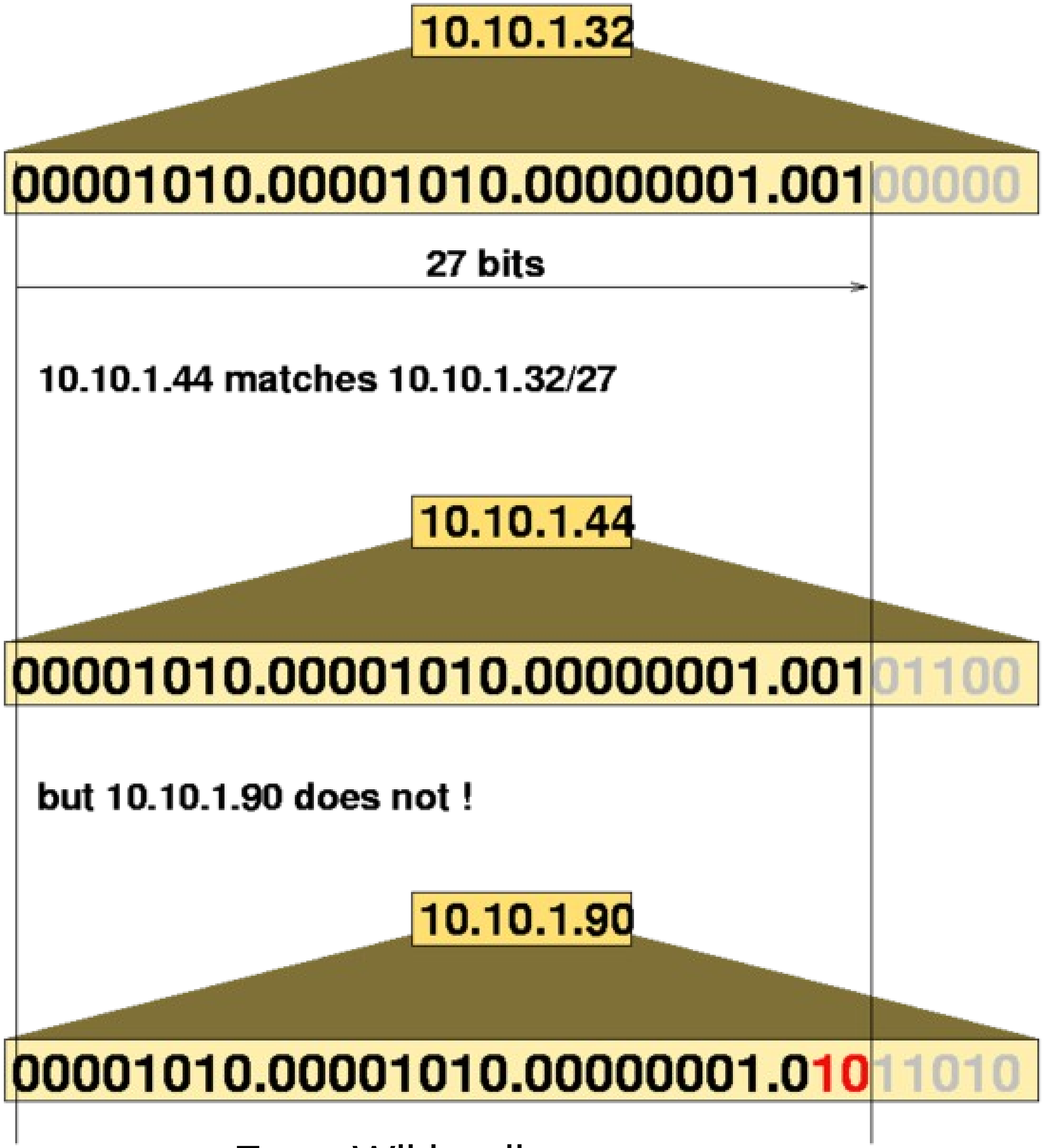
- IP = Internet protocol
- Forwarding, or “routing”
  - How packets get across the network
- Interface
  - WiFi, cellular, ...
- Path (or “route”), reverse path

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



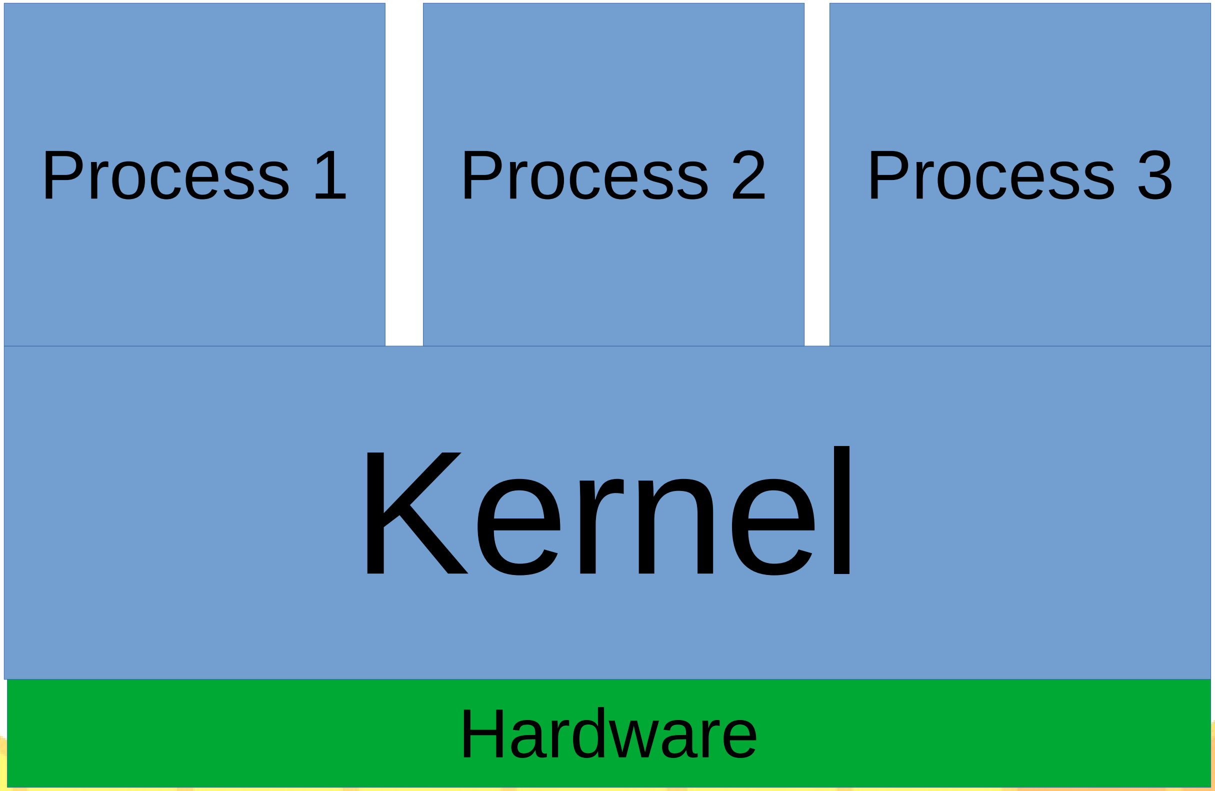
From Wikipedia

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)

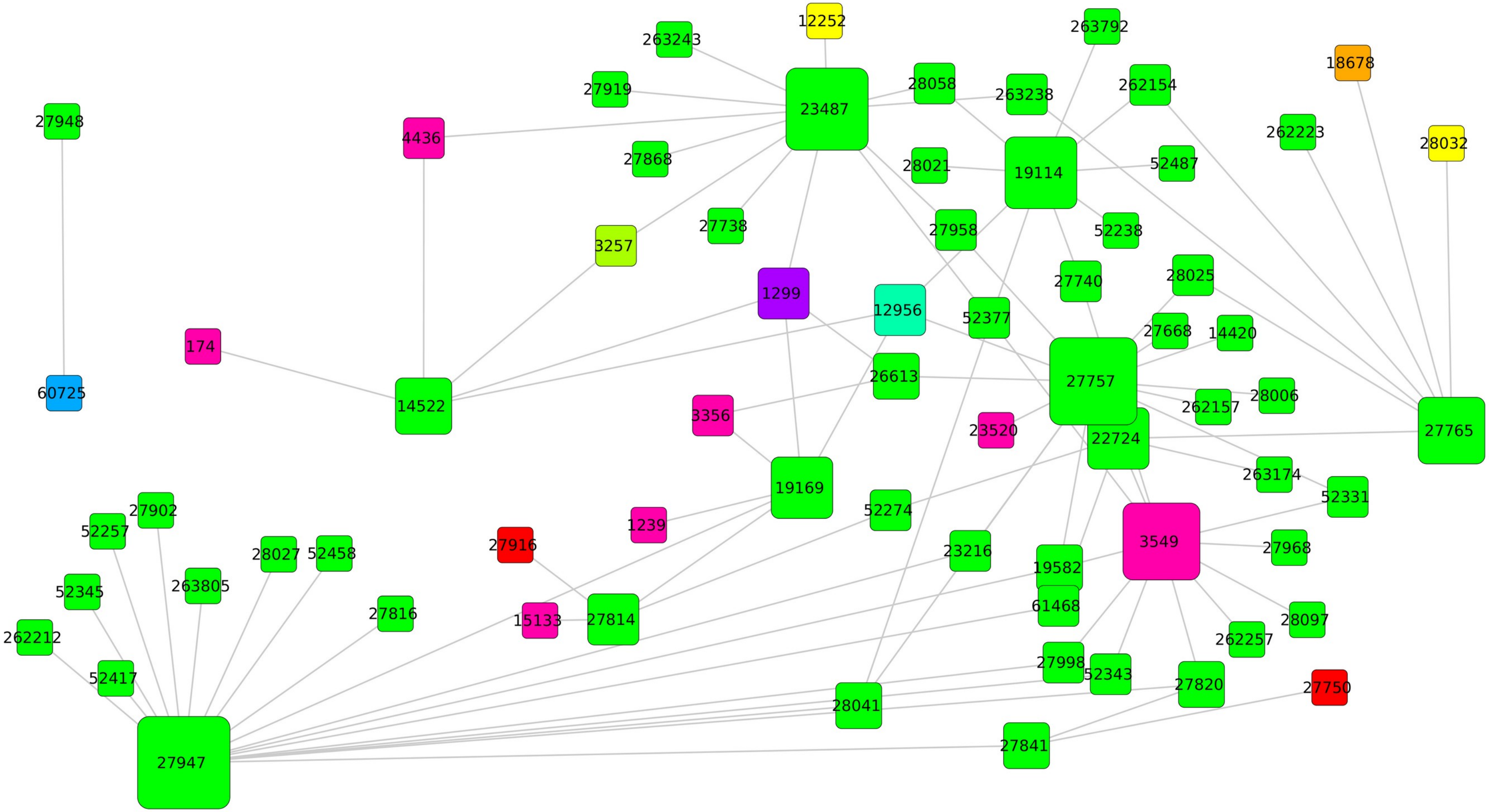
- Stream socket
  - Full duplex
  - Bytes always arrive in order
  - No delimiters
  - Example: TCP

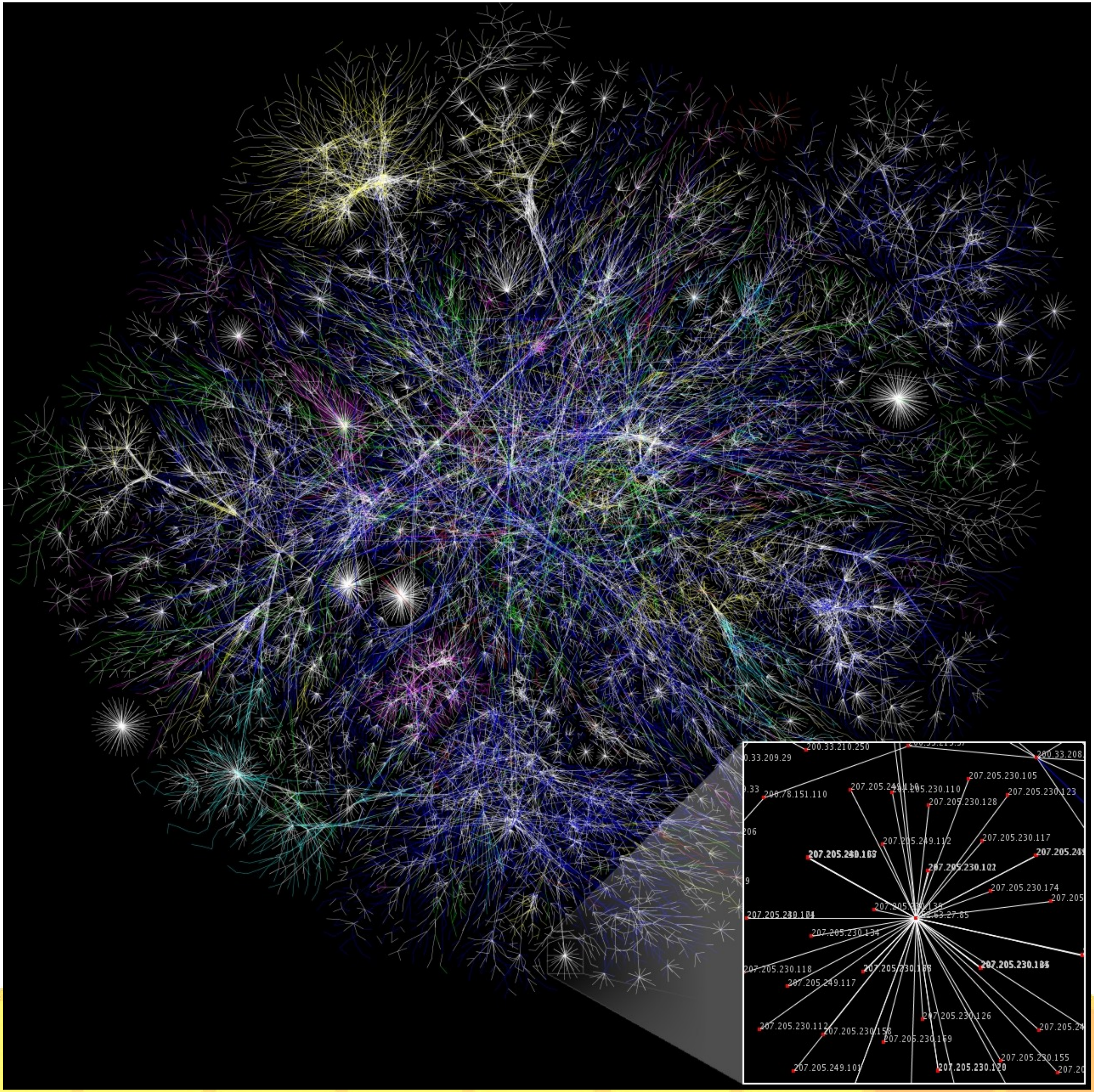
- Datagram socket
  - Not connection-based
  - Datagrams can arrive out of order
  - Datagrams are delimiters
  - Example: UDP

Almost there…

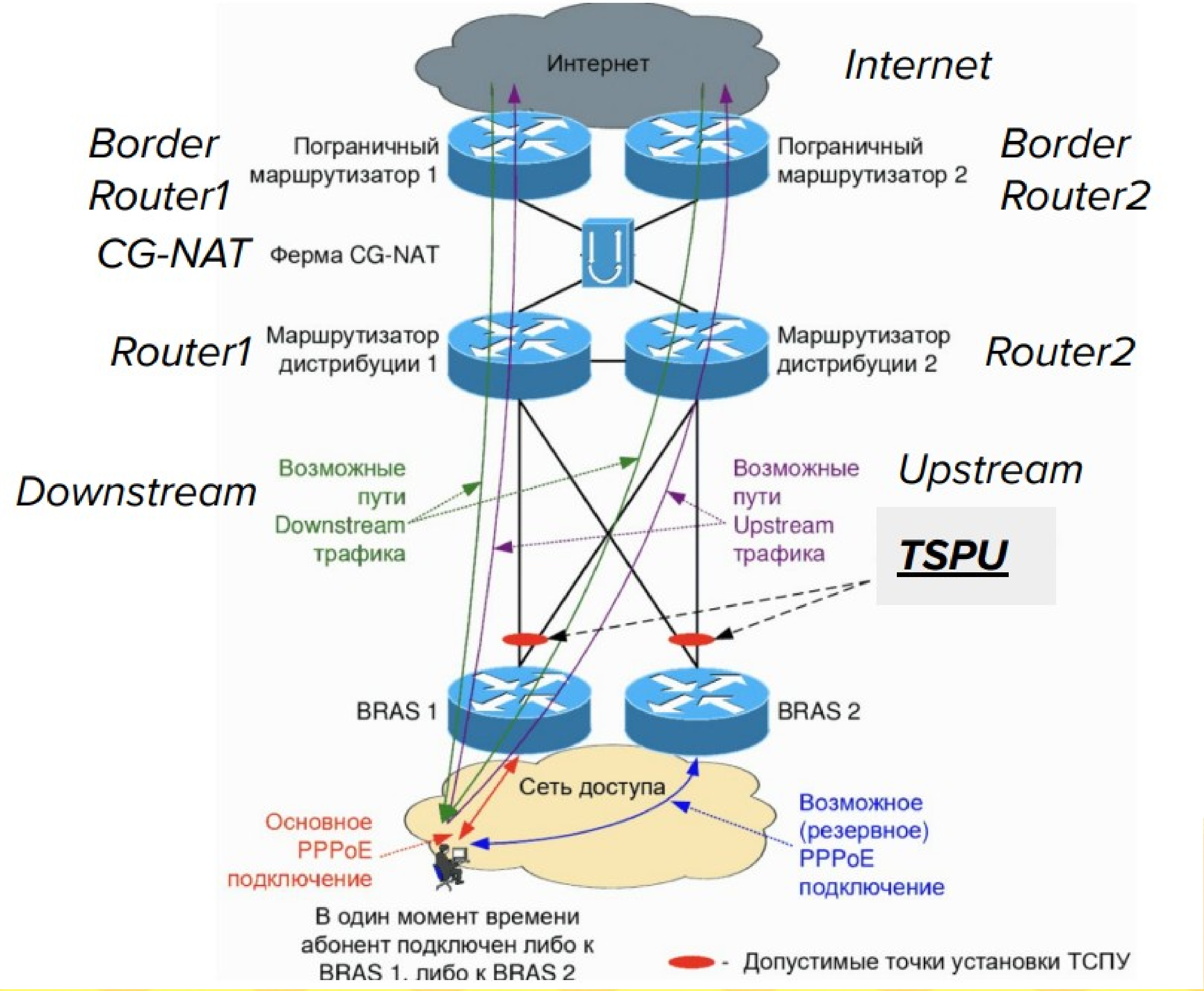
- DNS for resolving hostnames to IPs
  - breakpointingbad.com becomes 149.28.240.117
- BGP to scale to the size of the Internet
  - Path vector protocol
- HTTP as another example of an application layer protocol

Internet in Ecuador...




200.33.210.250
0.33.209.29
200.33.208.
207.205.230.105
0.33
200.78.151.110
207.205.249.110
207.205.230.110
207.205.230.123
207.205.230.128
206
207.205.249.112
207.205.230.117
207.205.240.163
207.205.230.102
207.205.24
207.205.230.174
9
207.205
207.205.230.139
12.63.27.85
207.205.230.104
207.205.230.134
207.205.230.118
207.205.230.163
207.205.230.134
207.205.249.117
207.205.230.126
207.205.230.112
207.205.230.158
207.205.230.169
207.205.24
207.205.230.155
207.205.249.101
207.205.230.120
207.20

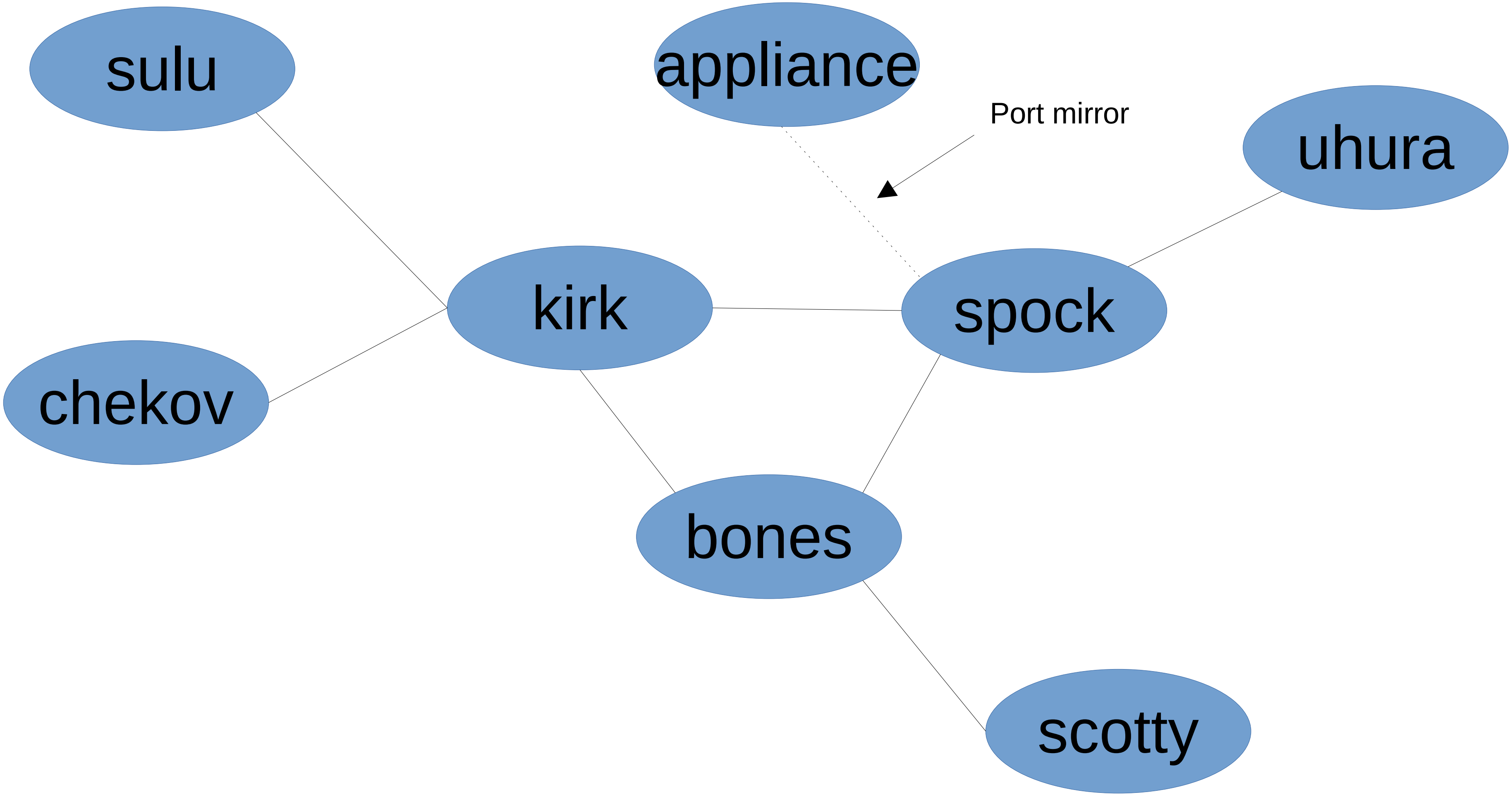
There are electric paths between the edge users and the backbone


Интернет
Internet
Border Router1
Пограничный маршрутизатор 1
Пограничный маршрутизатор 2
Border Router2
CG-NAT
Ферма CG-NAT
Router1
Маршрутизатор дистрибуции 1
Маршрутизатор дистрибуции 2
Router2
Downstream
Возможные пути Downstream трафика
Возможные пути Upstream трафика
Upstream
TSPU
BRAS 1
BRAS 2
Сеть доступа
Основное PPPoE подключение
Возможное (резервное) PPPoE подключение
В один момент времени абонент подключен либо к BRAS 1, либо к BRAS 2
- Допустимые точки установки ТСПУ

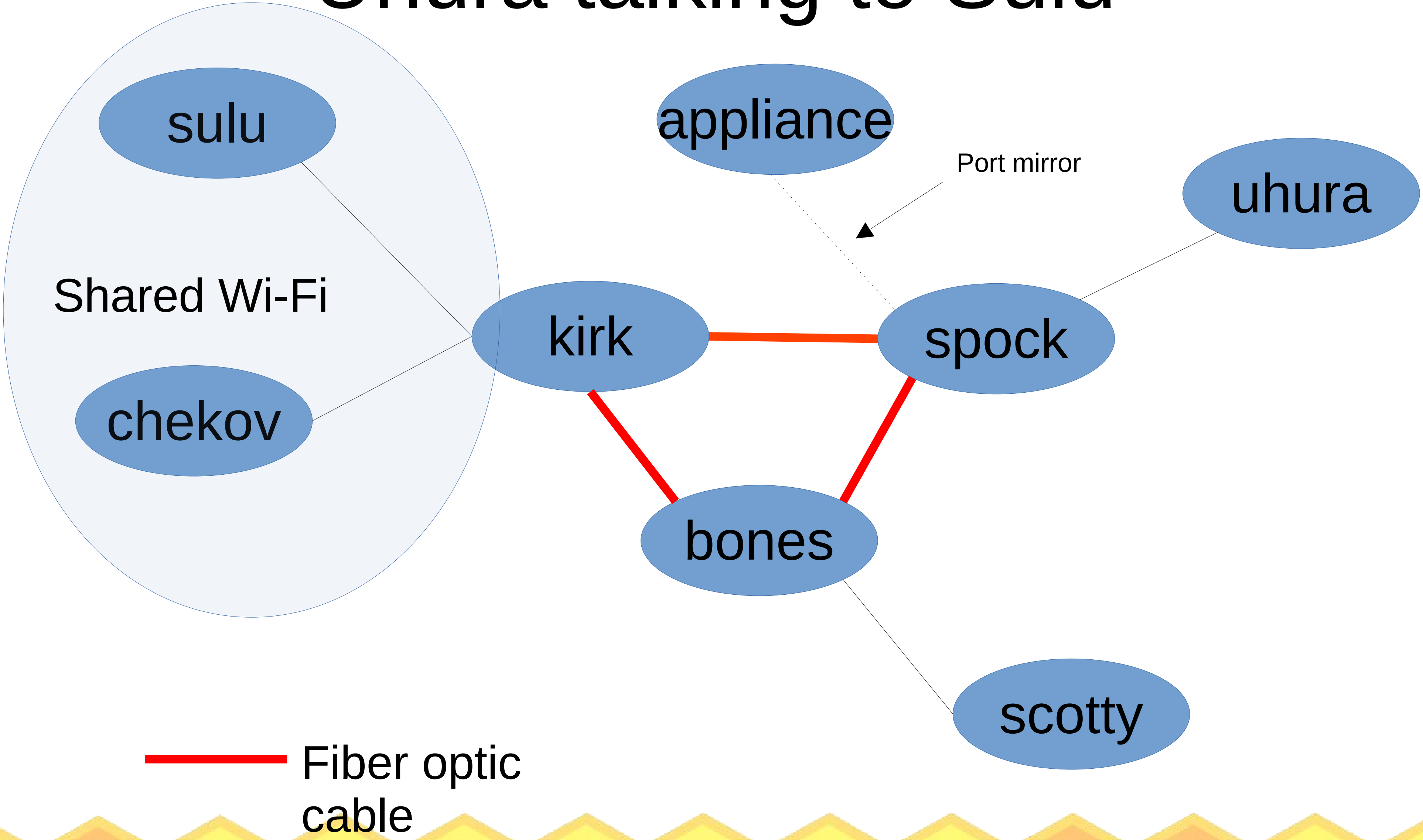
OSI model

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

Uhura talking to Sulu

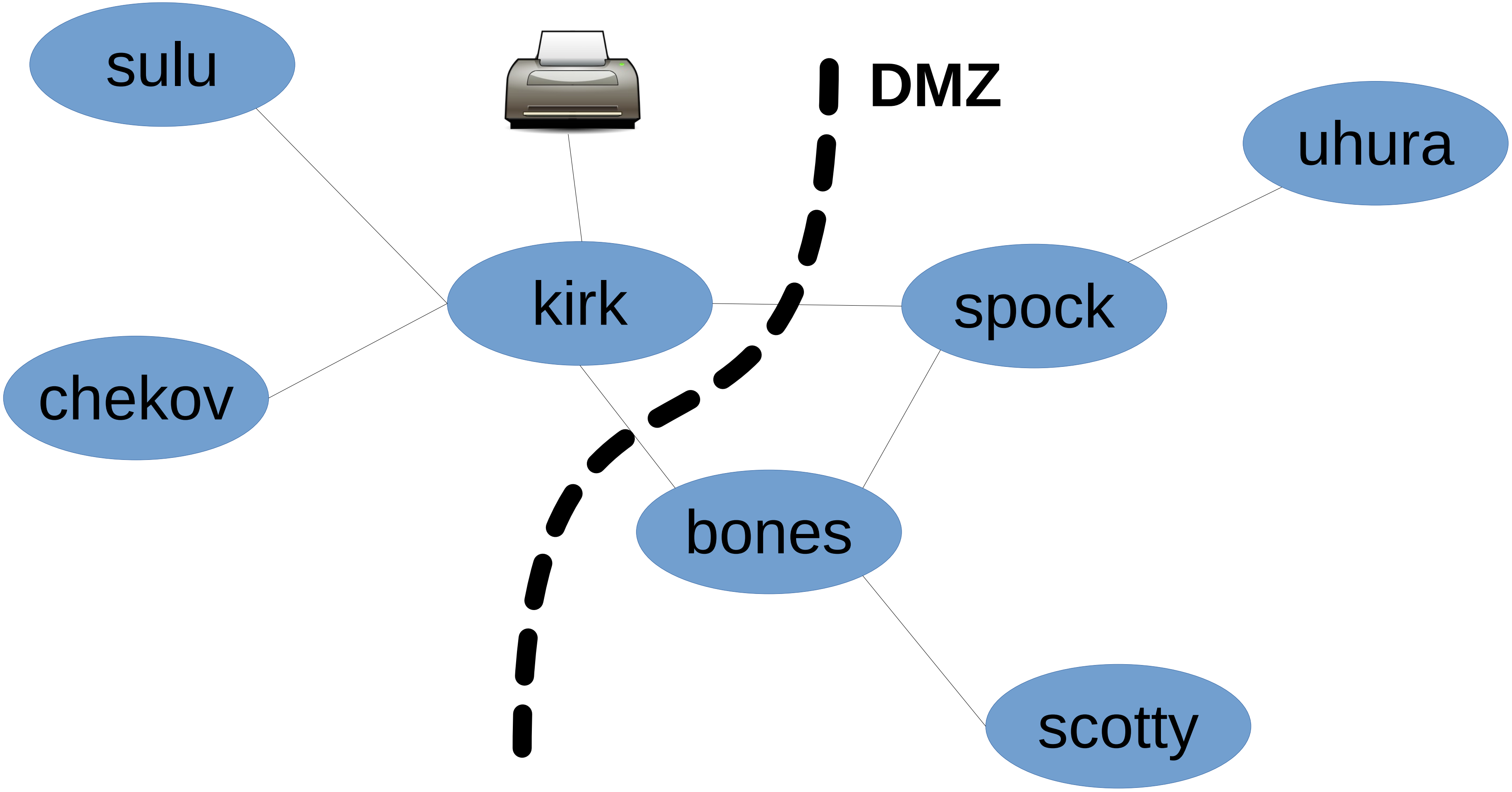


Uhura talking to Sulu



- kirk and spock are in-path
- appliance is on-path
  - Gets a copy of the packets from the port mirror on kirk
- chekov is on-path
  - Shared Wi-Fi with sulu, kirk has a wireless interface and two fiber optic interfaces
- scotty and bones are off-path

DMZ example



Secure Hash Functions Basics...

Preview...

https://media.ccc.de/v/25c3-3023-en-making_the_theoretical_possible

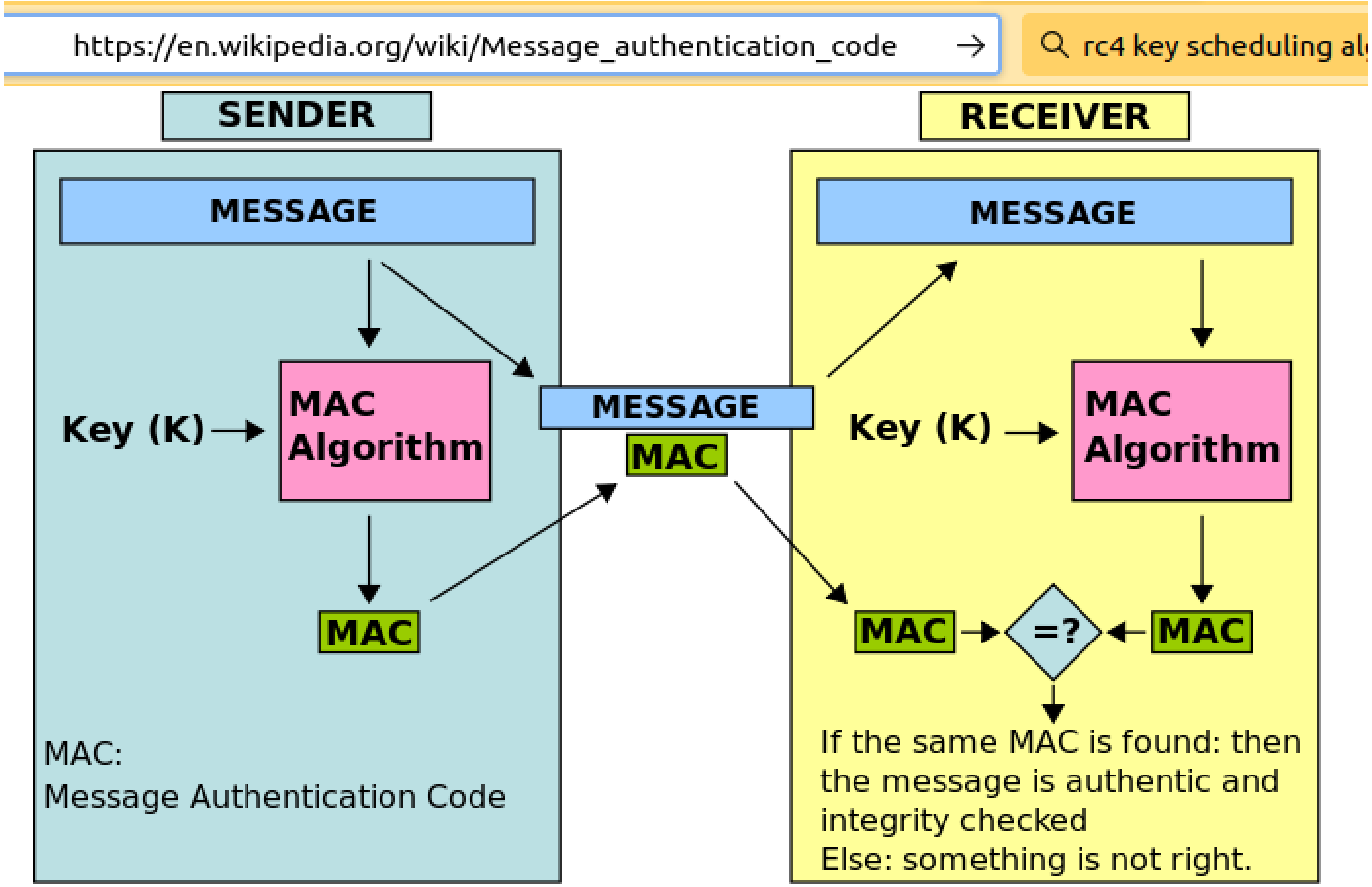
Also check out:
https://www.win.tue.nl/hashclash/rogue-ca/

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

Why cryptographic hash functions?

- Unique identifier for an object
- Integrity of an object
  - *E.g.*, message authentication codes
- Digital signatures
  - Sign the digest
    - E.g., 1024-bit RSA, 100MB message, 256-bit digest
- Passwords
- Proof of work

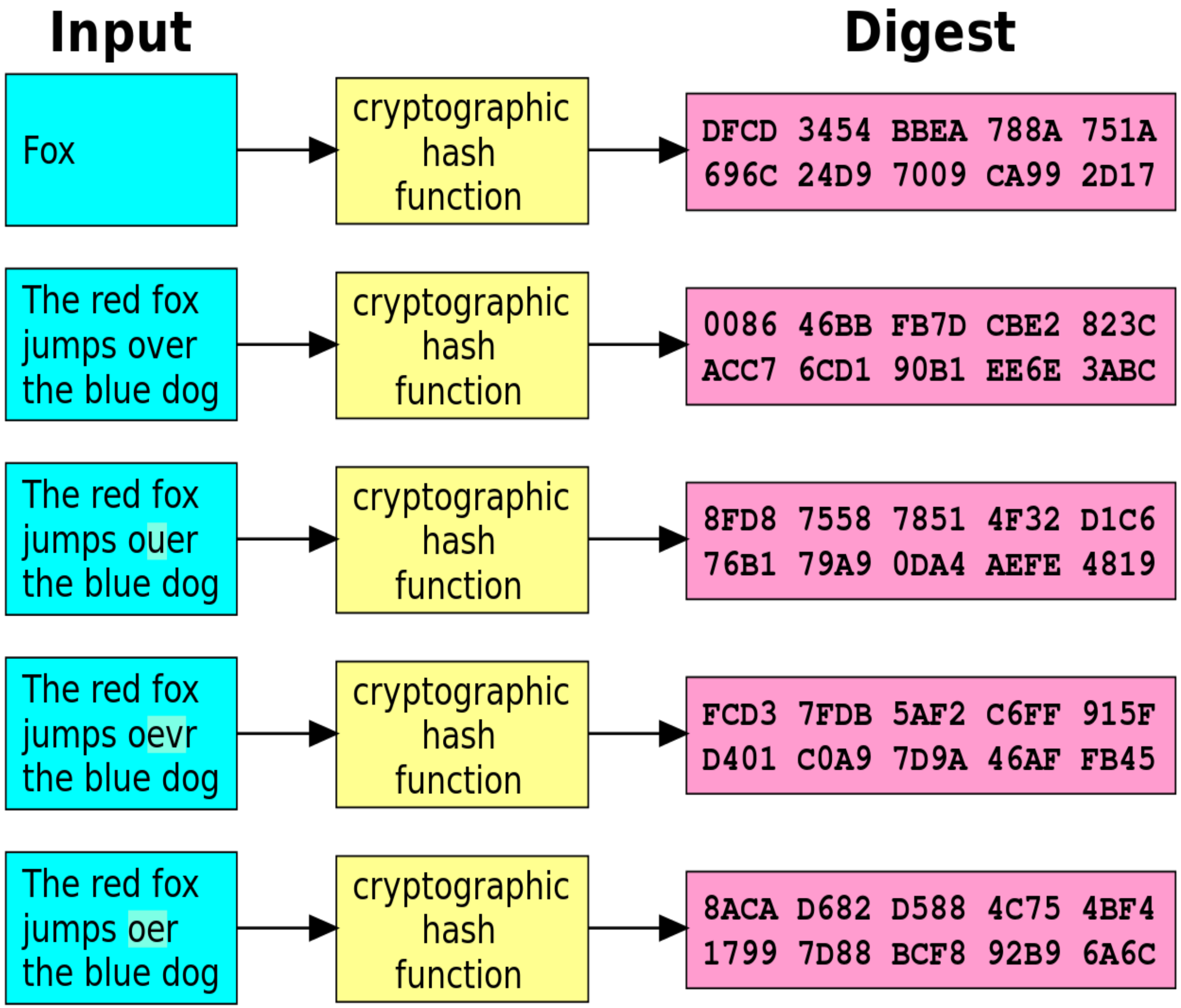


https://en.wikipedia.org/wiki/Message_authentication_code

MAC:
Message Authentication Code

If the same MAC is found: then the message is authentic and integrity checked
Else: something is not right.

Cryptographic hash function example...



Input		Digest
Fox	cryptographic hash function	DFCD 3454 BBEA 788A 751A 696C 24D9 7009 CA99 2D17
The red fox jumps over the blue dog	cryptographic hash function	0086 46BB FB7D CBE2 823C ACC7 6CD1 90B1 EE6E 3ABC
The red fox jumps ouer the blue dog	cryptographic hash function	8FD8 7558 7851 4F32 D1C6 76B1 79A9 0DA4 AEFE 4819
The red fox jumps oevr the blue dog	cryptographic hash function	FCD3 7FDB 5AF2 C6FF 915F D401 C0A9 7D9A 46AF FB45
The red fox jumps oer the blue dog	cryptographic hash function	8ACA D682 D588 4C75 4BF4 1799 7D88 BCF8 92B9 6A6C

By User:Jorge Stolfi based on Image:Hash_function.svg by Helix84 - Original work for Wikipedia, Public Domain, https://commons.wikimedia.org/w/index.php?curid=5290240

What makes a hash function cryptographic?

- One-way function
- Deterministic (same input, same output)
- Infeasible to find message that digests to specific hash value
- Infeasible to find two messages that digest to the same hash
- Avalanche effect (small change in message leads to big changes in digest---digests seemingly uncorrelated)
- *Still want it to be quick*

Example algorithms

- MD5: 128-bit digest
  - seriously broken
- SHA-1: 160-bit digest
  - not secure against well-funded adversaries
- SHA-2: 224 to 512 bit digest
  - Merkle–Damgård construction
- SHA-3: 224 to 512 bit digest
  - Sponge construction
  - adopted in August of 2015
- CRC32: not cryptographic, very poor choice

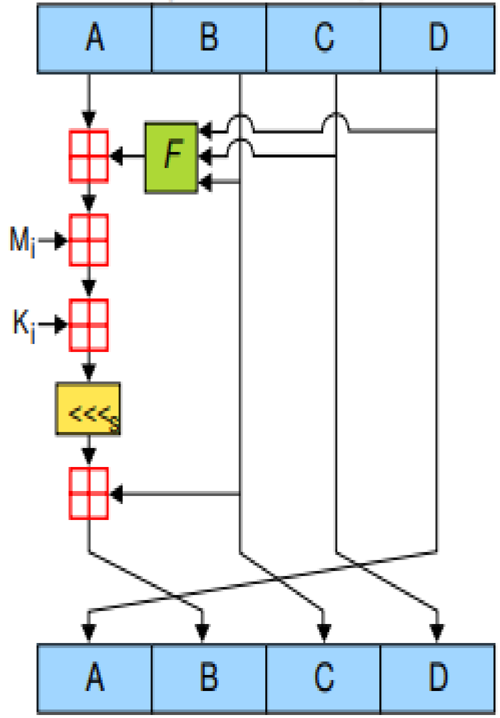
Example algorithms

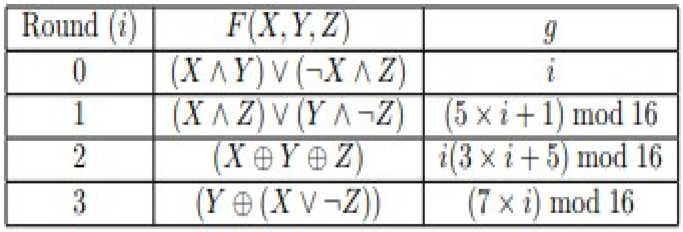
- MD5: 128-bit digest, seriously broken
- SHA-1: 160-bit digest, not secure against well-funded adversaries
- SHA-3: 224 to 512 bit digest, adopted in August of 2015
- CRC32: not cryptographic, very poor choice

MD5

- Pad to multiple of 512 bits
- 4 rounds
- 4 32-bit words at a time
- Concatenate them at the end for a 128-bit digest
- F is non-linear, varies by round

Fig. 1. One MD5 step





Round (i)	$F(X,Y,Z)$	g
0	$(X \wedge Y) \vee (\neg X \wedge Z)$	i
1	$(X \wedge Z) \vee (Y \wedge \neg Z)$	$(5 \times i + 1) \bmod 16$
2	$(X \oplus Y \oplus Z)$	$i(3 \times i + 5) \bmod 16$
3	$(Y \oplus (X \vee \neg Z))$	$(7 \times i) \bmod 16$

http://koclab.cs.ucsb.edu/teaching/cren/project/2008/savage.pdf

Property #1

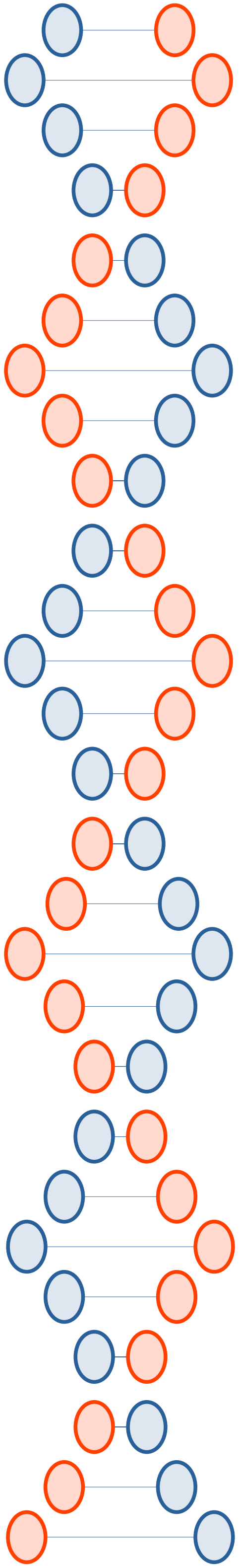
- Pre-image resistance
- Given *h*, it should be infeasible to find *m* such that *h = hash(m)*

Neither MD5 nor SHA-3 are broken in this way, but MD5 digests are small.

Property #2

- Second pre-image resistance
- Given a message m_1, it should be infeasible to find another message m_2 such that... $hash(m_1) = hash(m_2)$

Neither MD5 nor SHA-3 are broken in this way, but MD5 digests are small.



Property #3

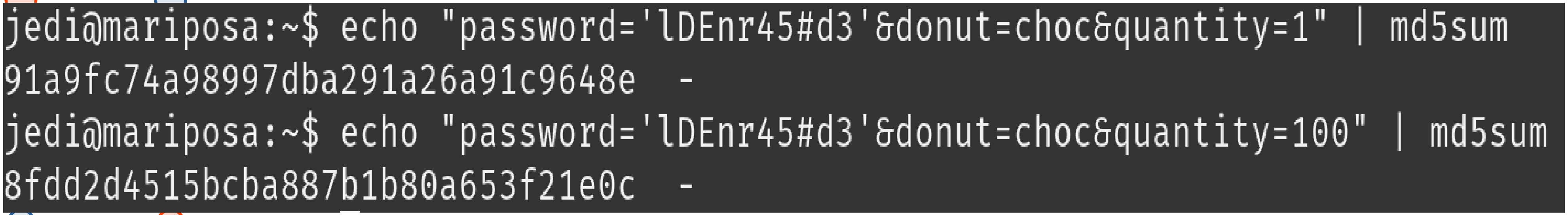
- Collision resistance
- It should be infeasible to find two messages, m_1 *and* m_2 such that...
  $hash(m_1) = hash(m_2)$

SHA-3 is not broken in this way, MD5 broken in seconds on your laptop, SHA-1 with $100K or so.

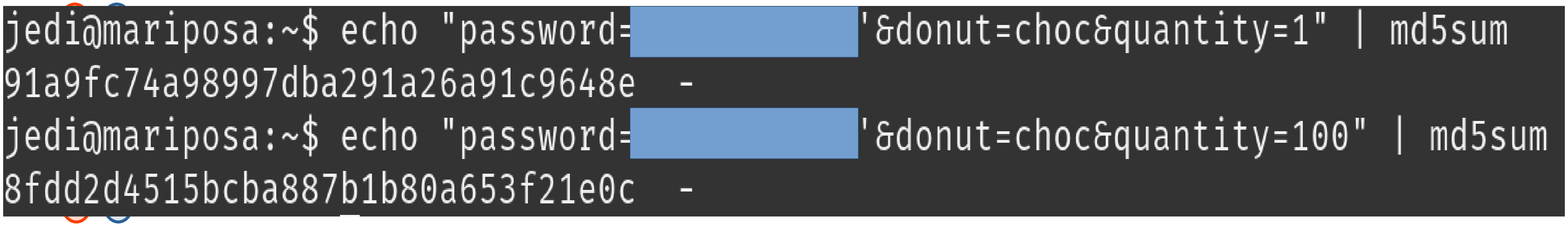
Wang Xiaoyun

- Tsinghua University
- Contributed a lot of ideas to cracking MD5, SHA-0, and SHA-1

Length extension attack



```
jedi@mariposa:~$ echo "password='lDEnr45#d3'&donut=choc&quantity=1" | md5sum
91a9fc74a98997dba291a26a91c9648e  -
jedi@mariposa:~$ echo "password='lDEnr45#d3'&donut=choc&quantity=100" | md5sum
8fdd2d4515bcba887b1b80a653f21e0c  -
```

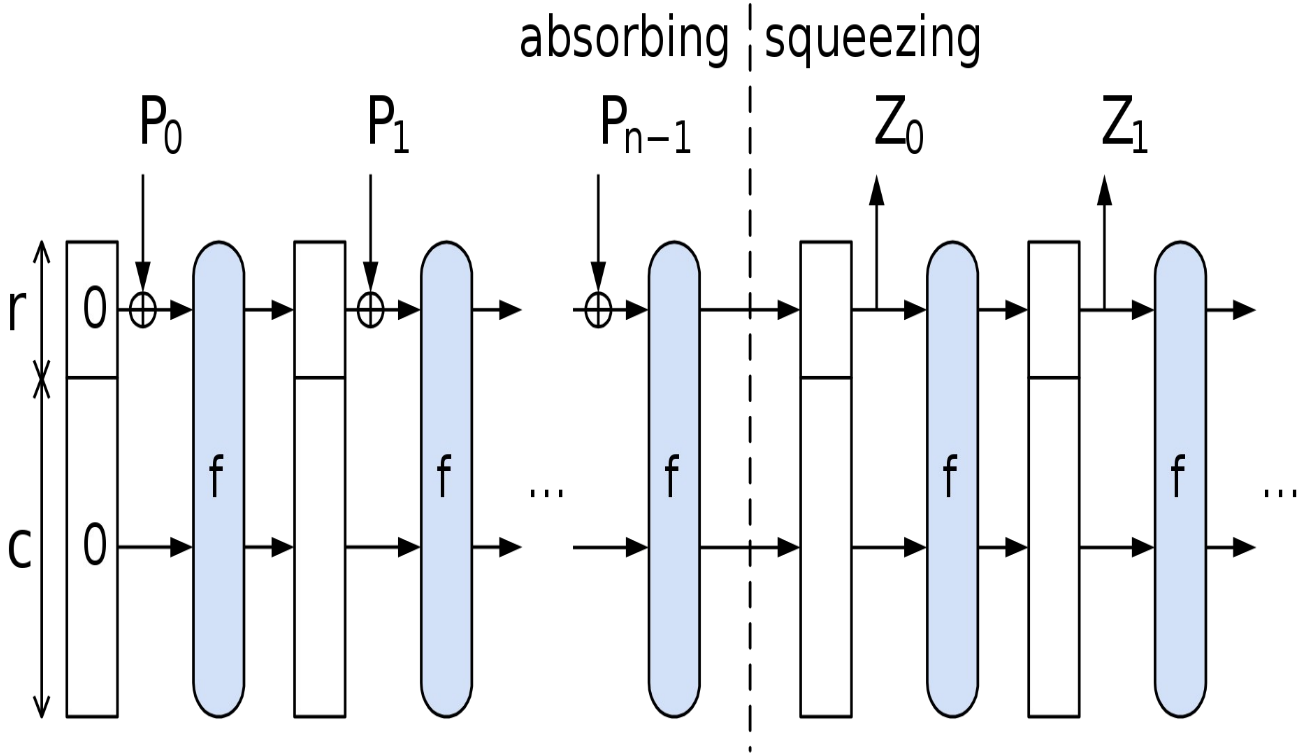


```
jedi@mariposa:~$ echo "password=[redacted]'&donut=choc&quantity=1" | md5sum
91a9fc74a98997dba291a26a91c9648e  -
jedi@mariposa:~$ echo "password=[redacted]'&donut=choc&quantity=100" | md5sum
8fdd2d4515bcba887b1b80a653f21e0c  -
```

MD5 and SHA-1 vulnerable, SHA-2 basically is, SHA-3 is not

SHA-3

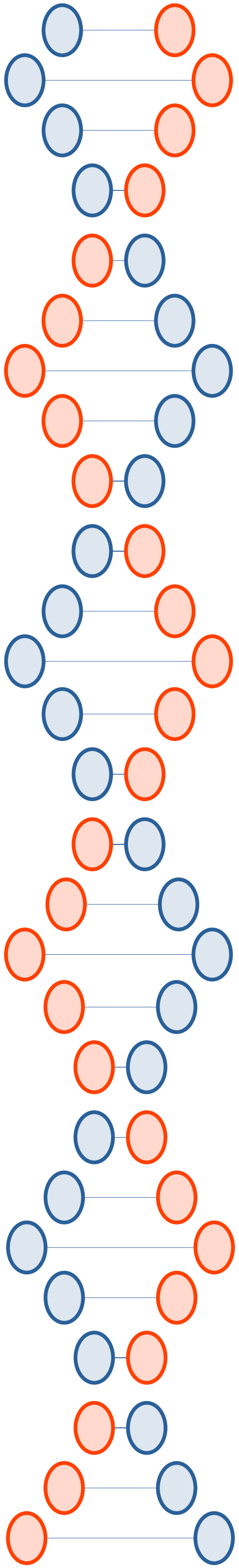
- Sponge construction, 1600 bits of internal state



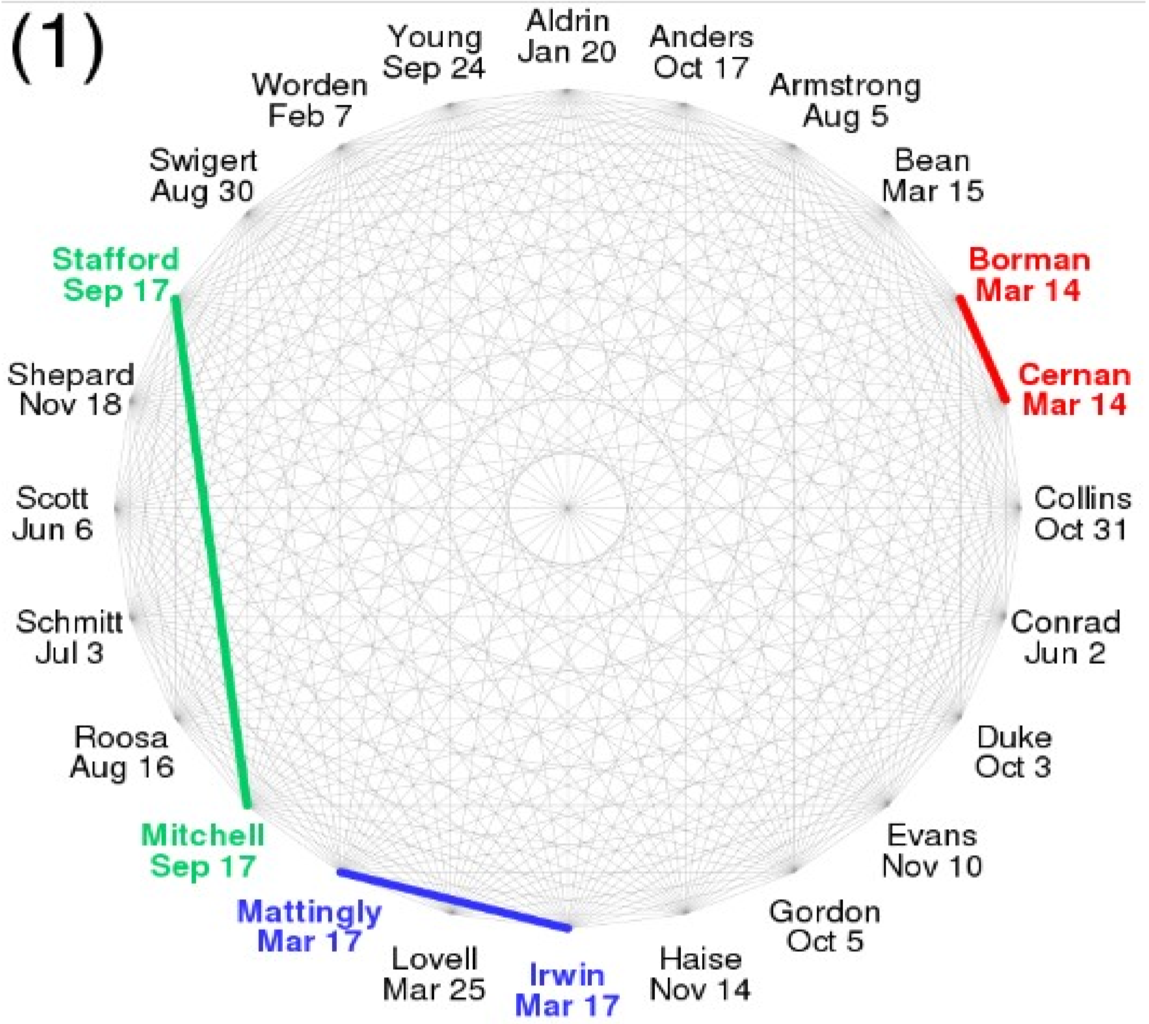
https://en.wikipedia.org/wiki/SHA-3

Preview: Birthday attack

- Probability of collision is *1* in 2^n, but the expected number of hashes until two of them collide is $sqrt(2^n)=2^{n/2}$
  - Why? Third try has two opportunities to collide, fourth has three opportunities, fifth has six, and so on...

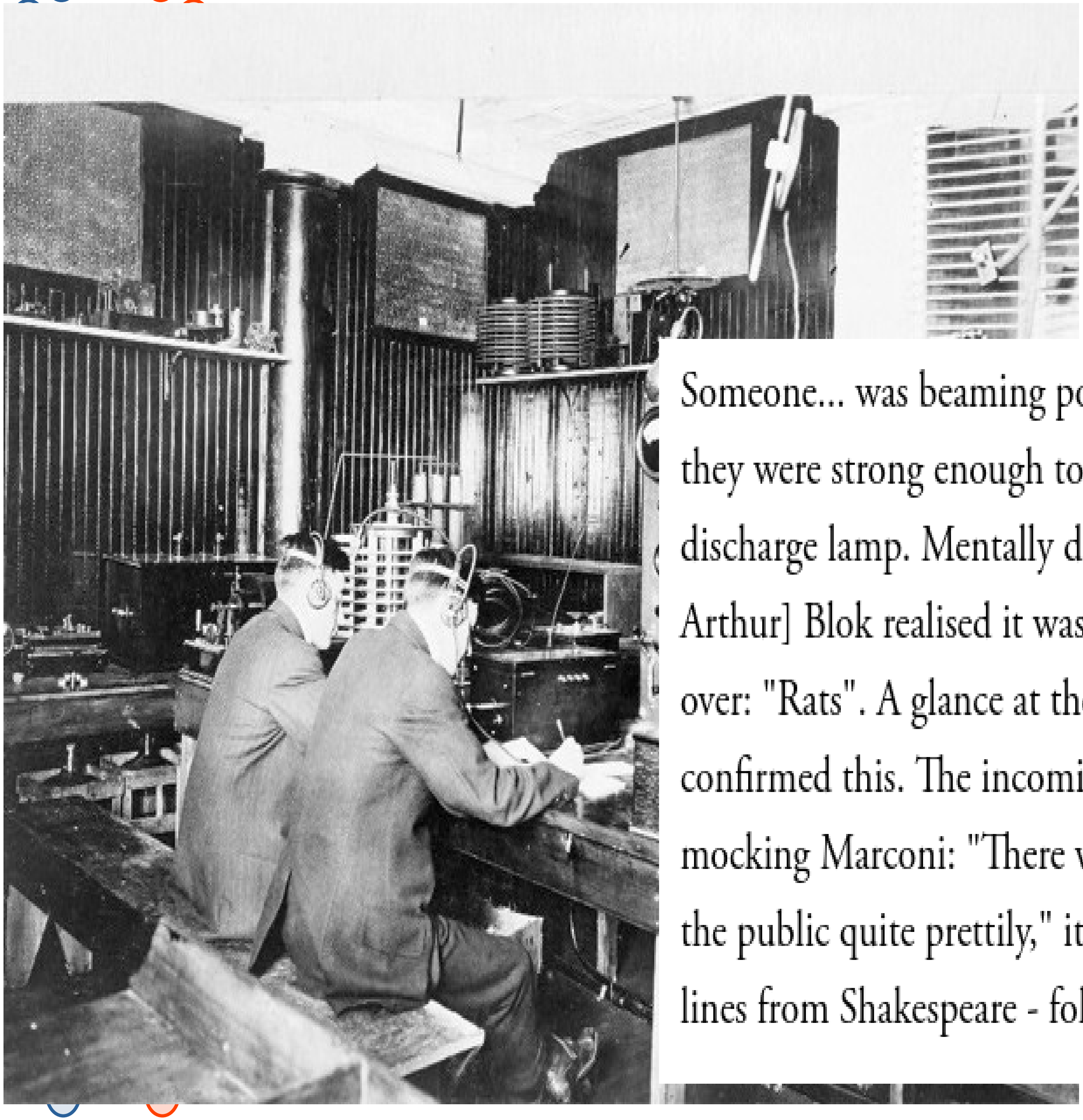


24 people, same birthday?



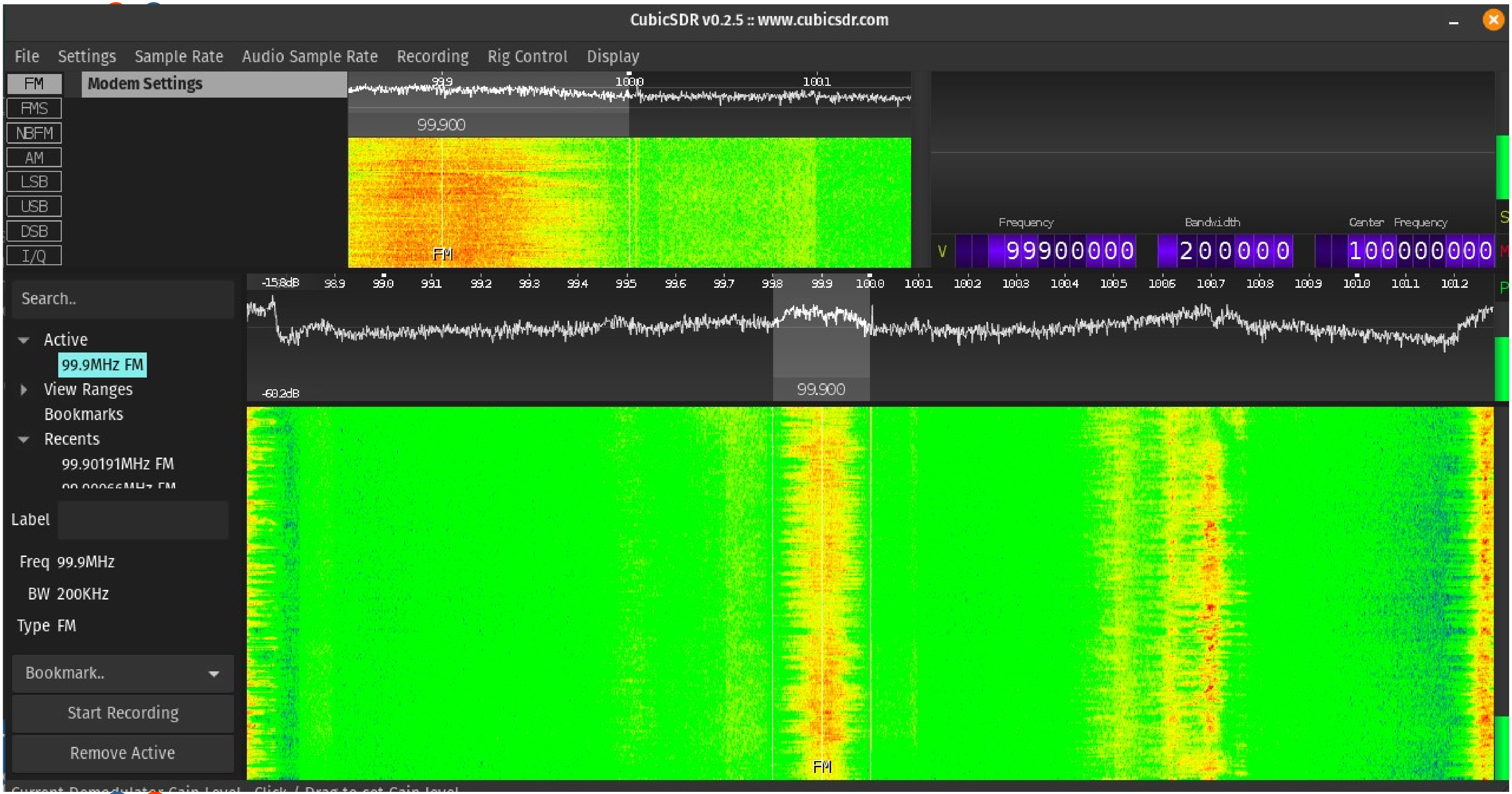
https://commons.wikimedia.org/wiki/File:Birthday_attack_vs_paradox.svg

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/



Frequency 99900000

Bandwidth 200000

Center Frequency 100000000

Active

99.9MHz FM

Recents

99.90191MHz FM

99.90066MHz FM

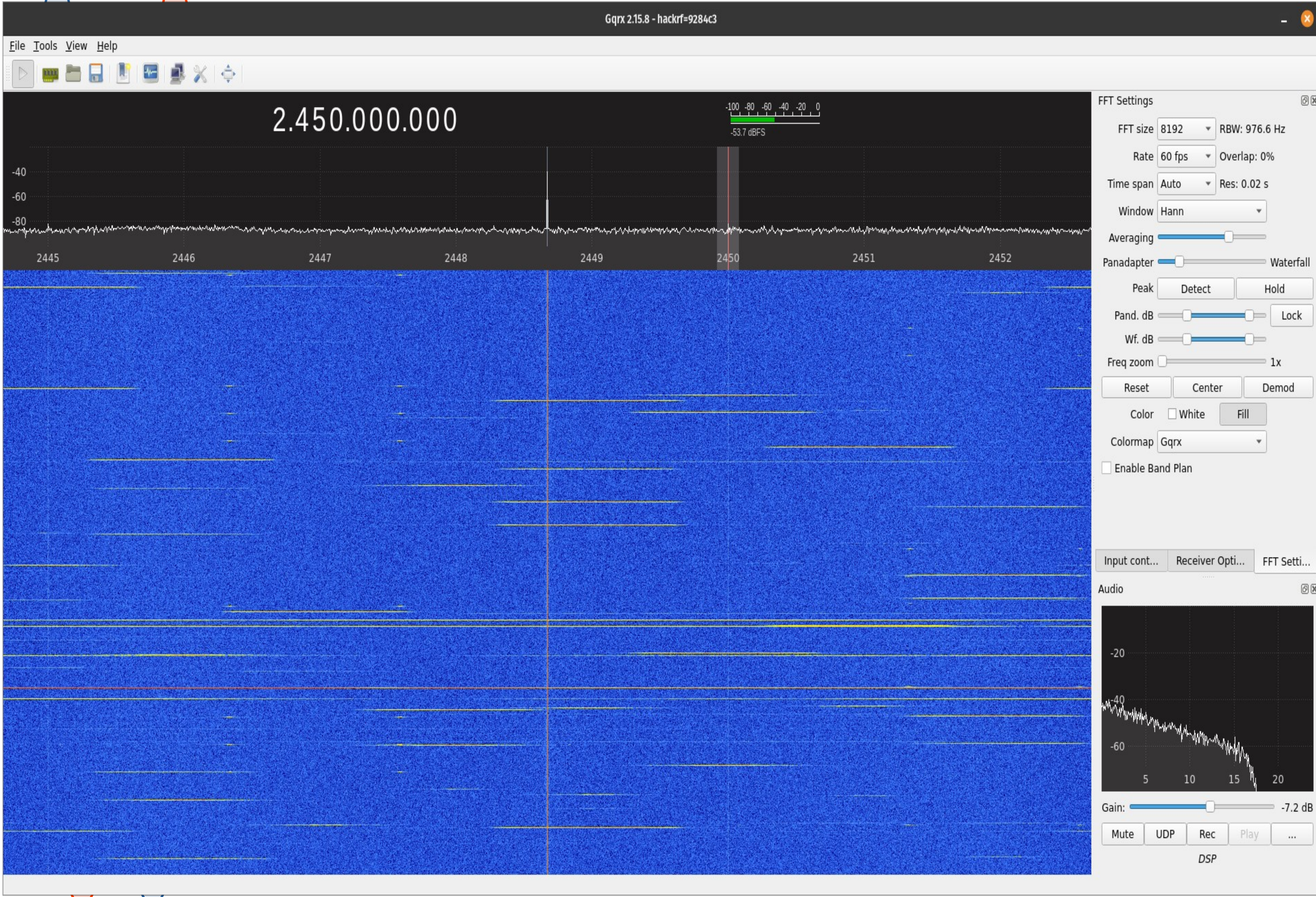
Label

Freq 99.9MHz

BW 200KHz

Type FM

Current Demodulator Gain Level - Click / Drag to set Gain level



Gqrx 2.15.8 - hackrf=9284c3

2.450.000.000

-53.7 dBFS

FFT Settings

FFT size 8192 RBW: 976.6 Hz

Rate 60 fps Overlap: 0%

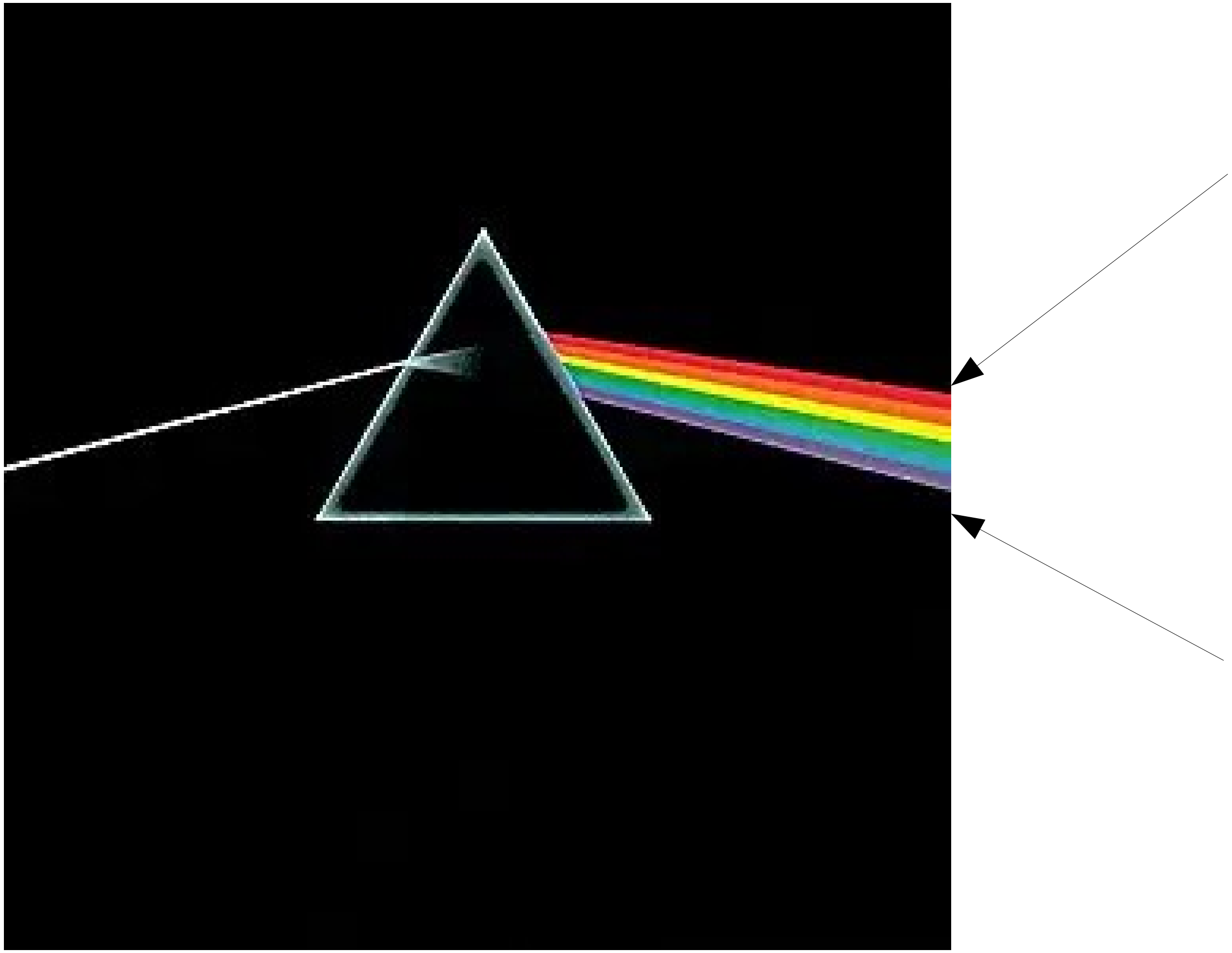
Time span Auto Res: 0.02 s

Window Hann

Colormap Gqrx

Audio

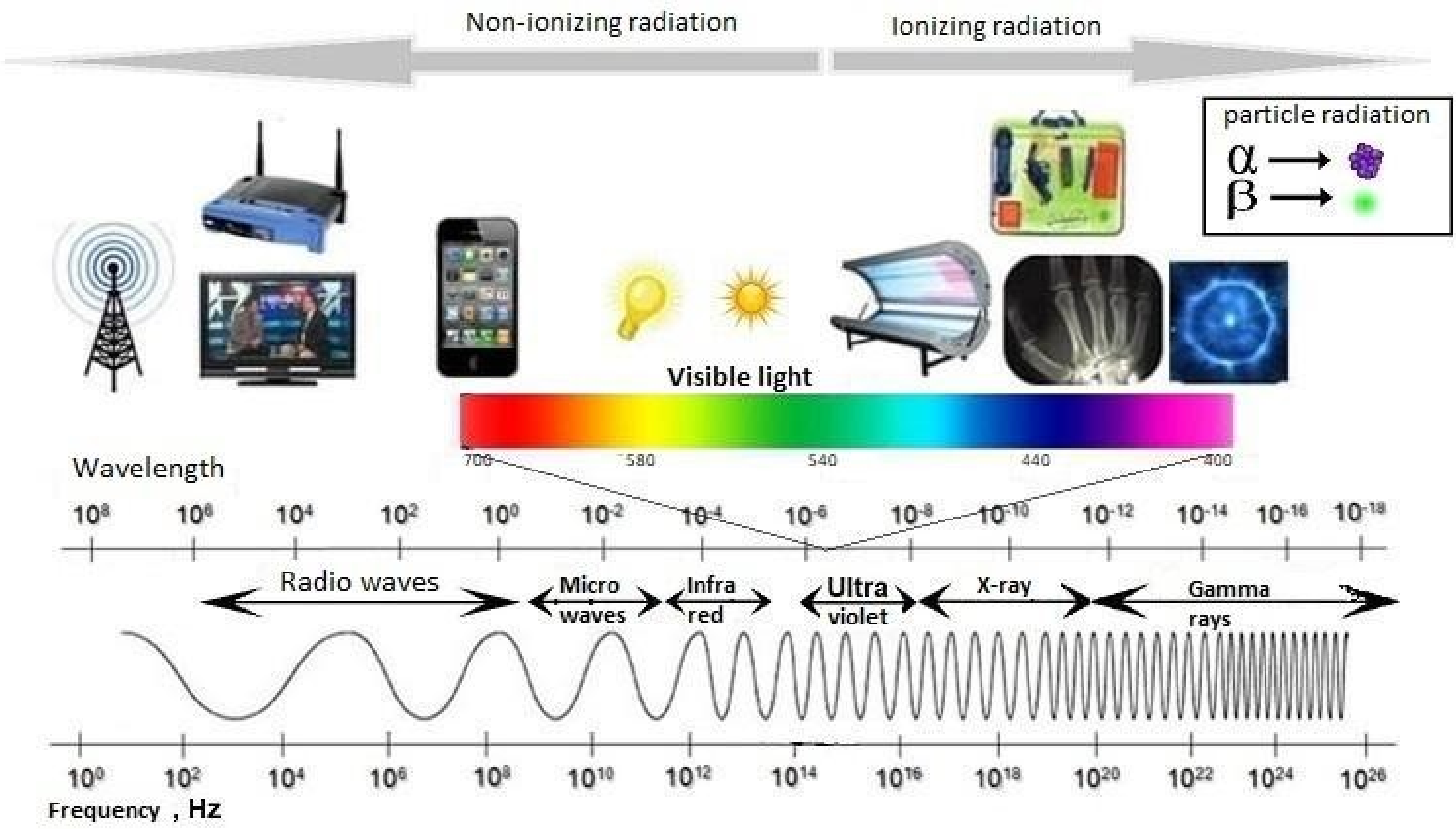
Gain: -7.2 dB



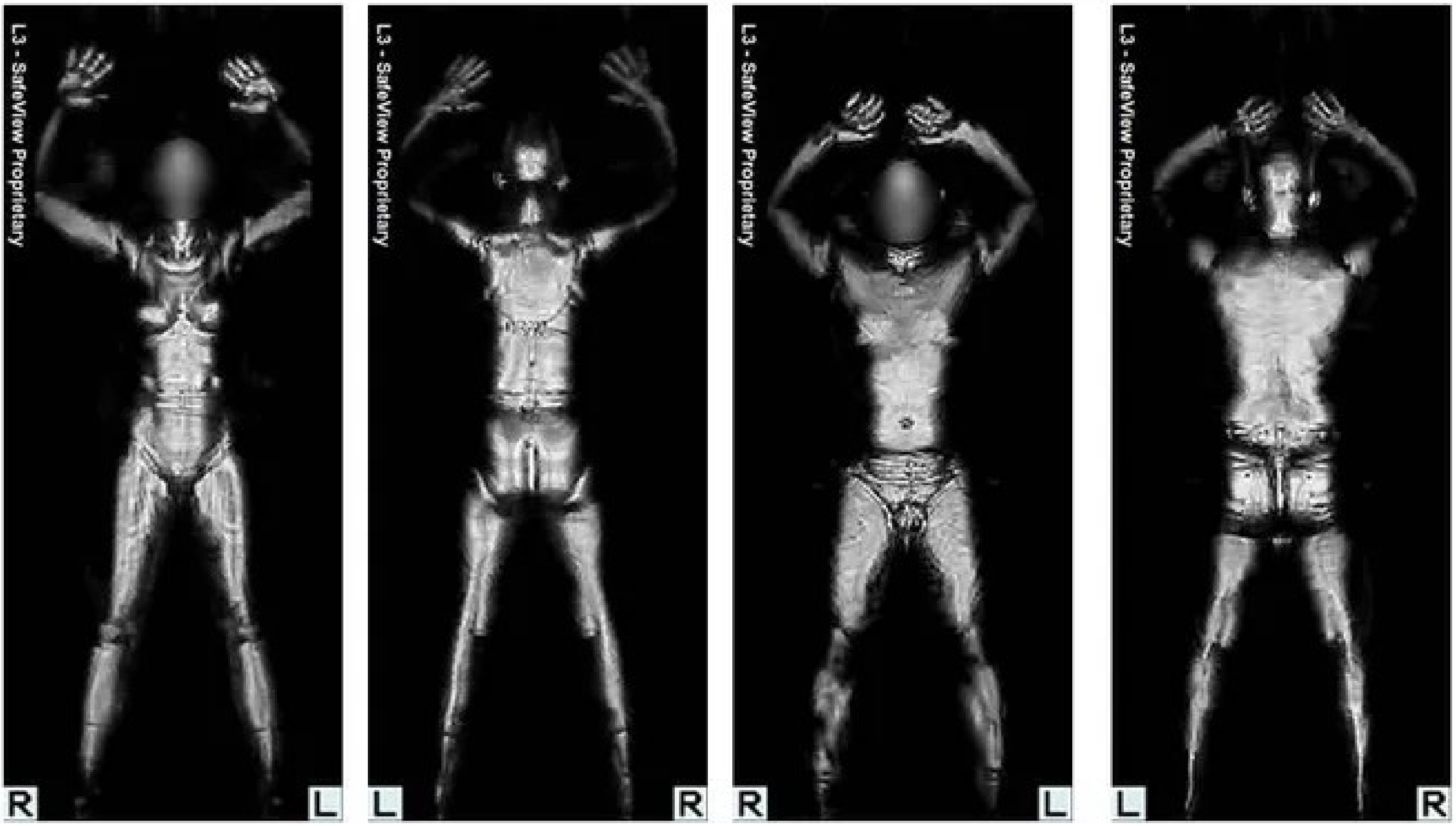
Warmth

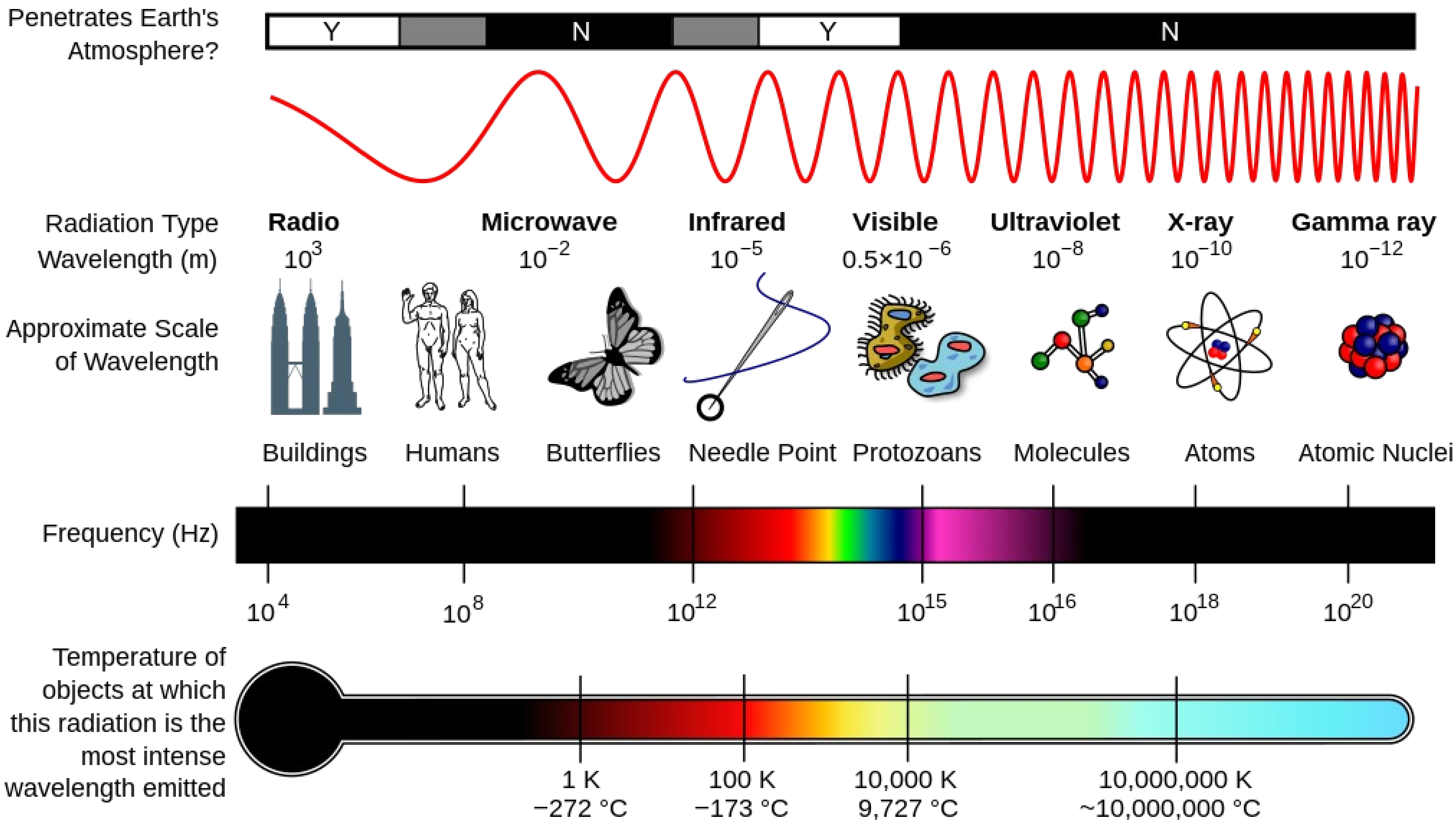
Sunburns

The electromagnetic spectrum

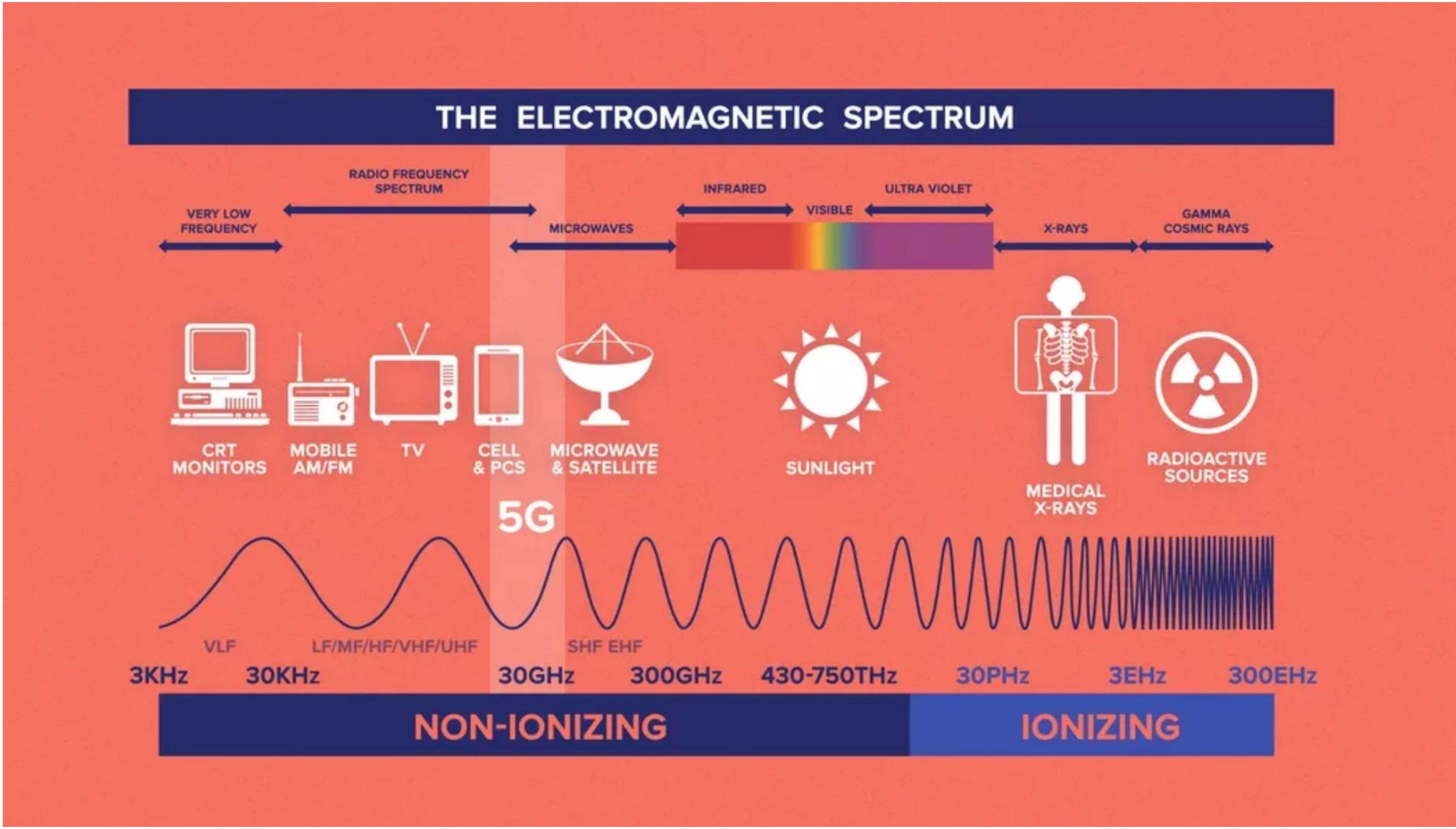


https://www.uib.no/en/hms-portalen/75292/electromagnetic-spectrum https://www.usatoday.com/story/travel/roadwarriorvoices/2015/08/17/tsa-has-spent-160-million-on-body-scanners-and-theyre-still-terrible/83288622/


L3 - SafeView Proprietary
R
L
L3 - SafeView Proprietary
L
R
L3 - SafeView Proprietary
R
L
L3 - SafeView Proprietary
L
R



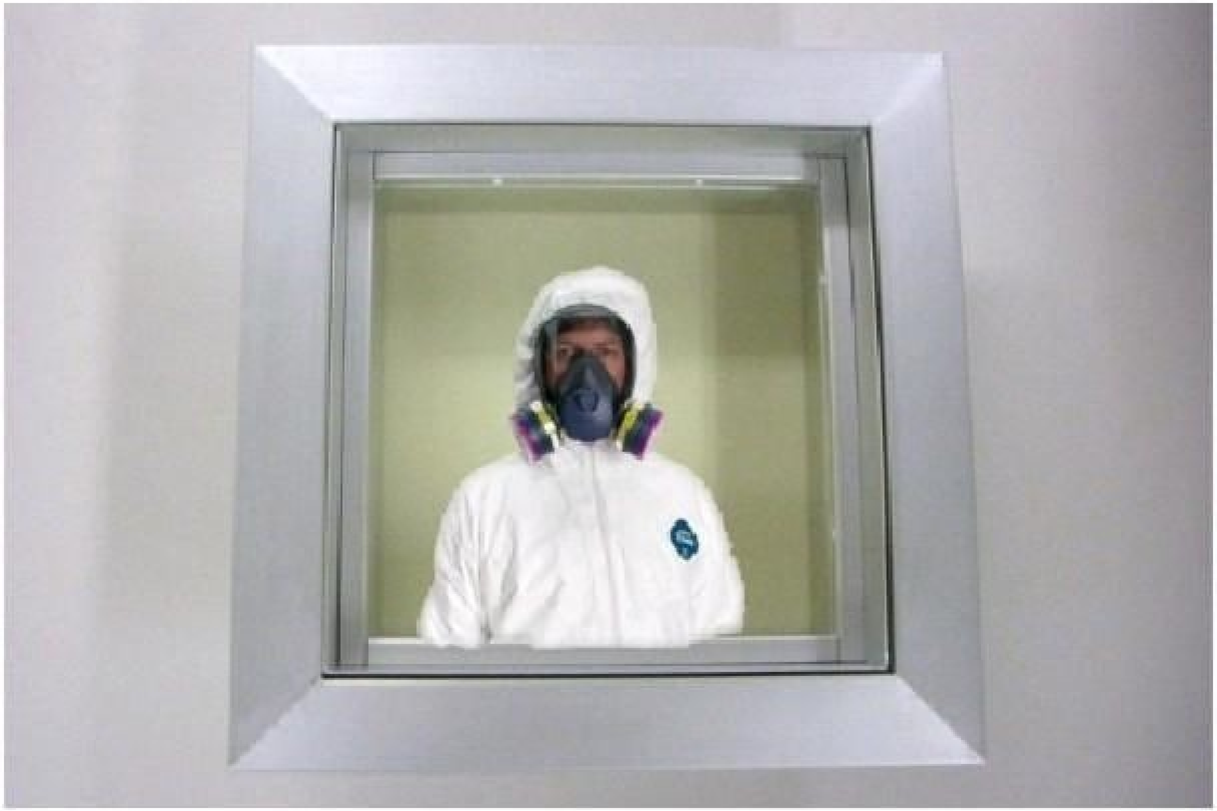
https://commons.wikimedia.org/wiki/File:EM_Spectrum_Properties_edit.svg



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"

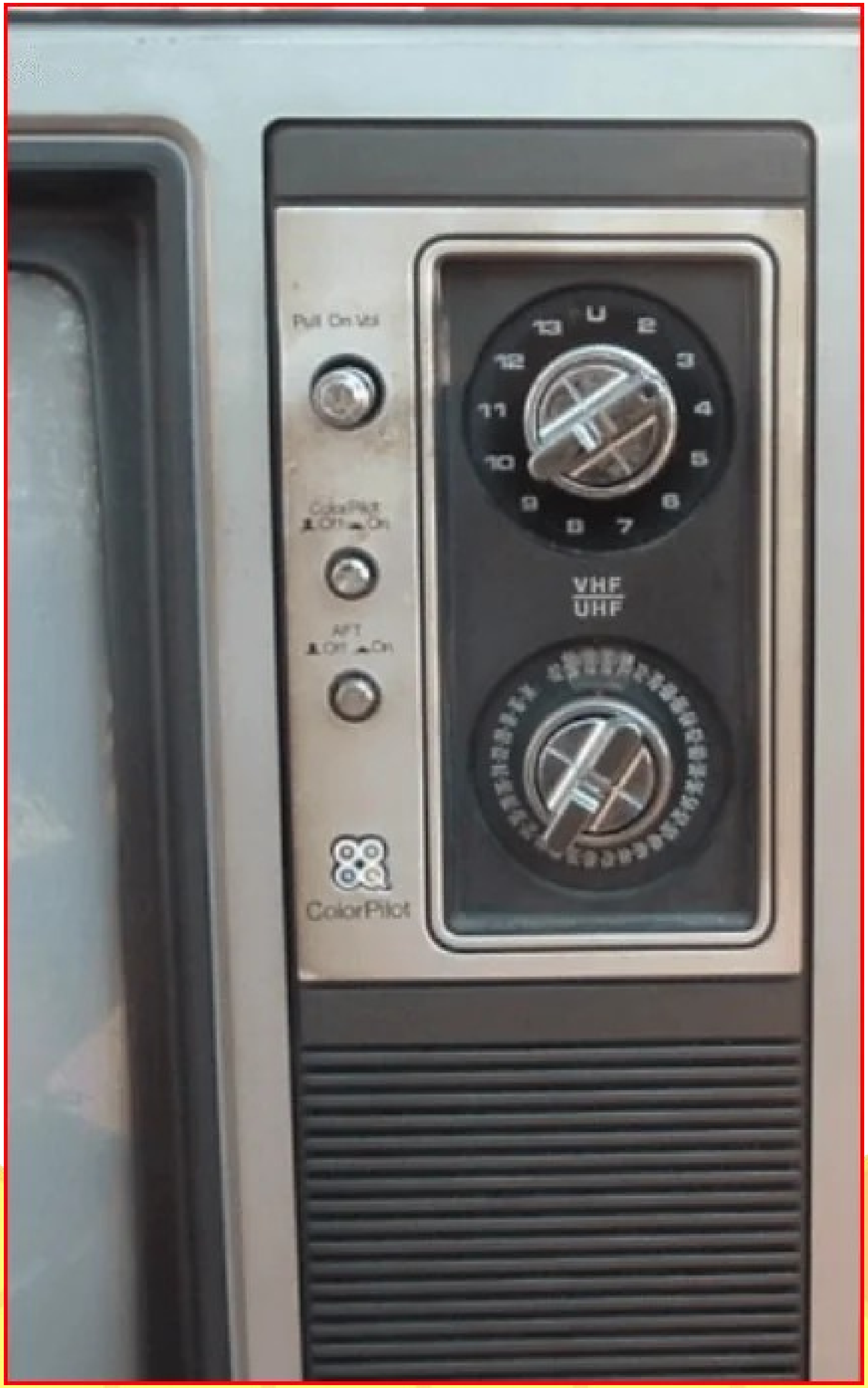
Also doctors at the X-Ray:



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

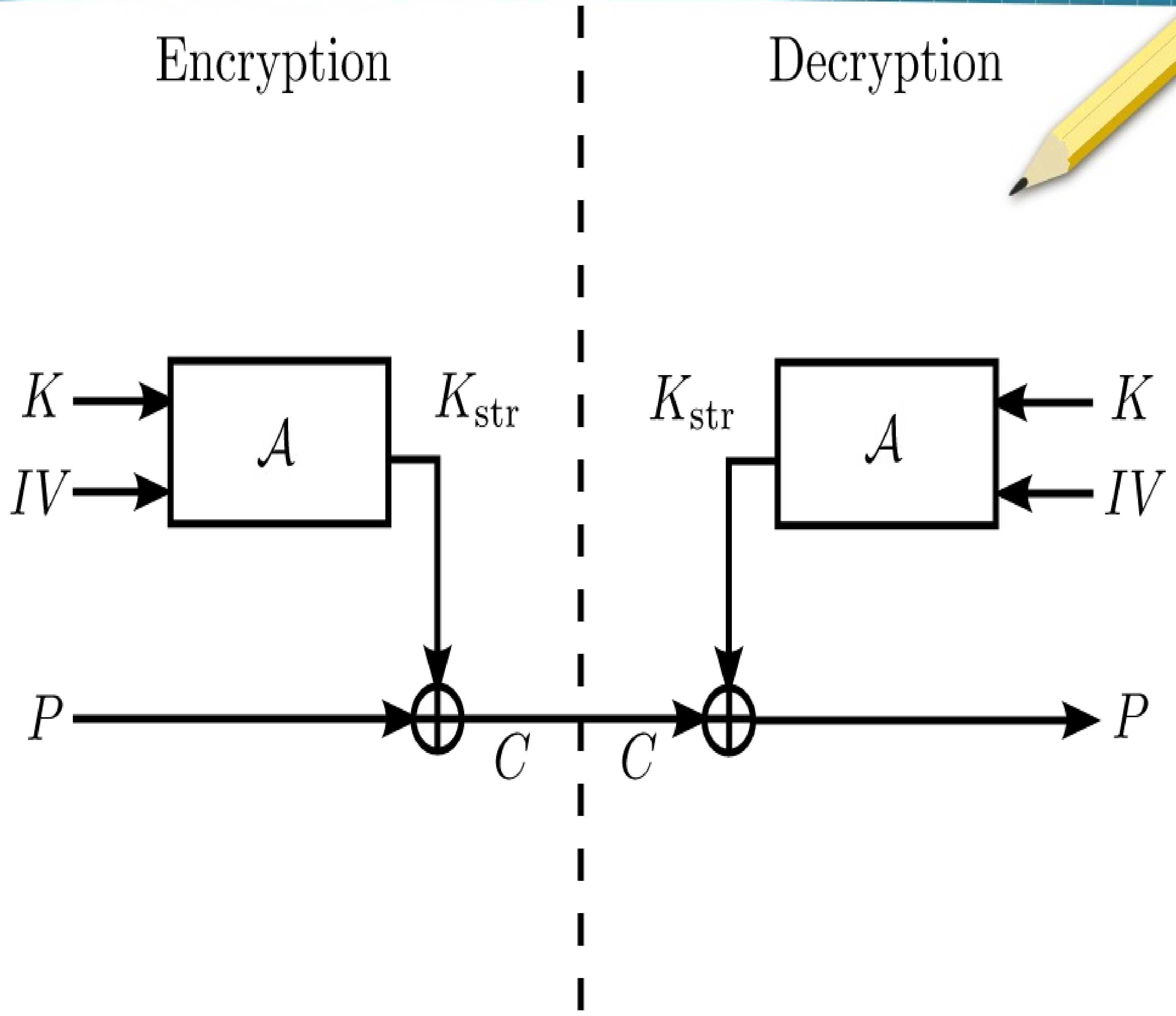
- VHF – 30MHz to 300MHz
  - Line of sight, but refracted up to 100 miles or so
  - FM radio, TV, amateur radio
- HF – 3MHz to 30MHz
  - Reflected off the ionosphere
  - Military, amateur radio, maritime, CB radio
- MF – 300KHz to 3 MHz
  - AM radio, maritime

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

A theme we will see in asymmetric cryptography…

Crypto protocols and network protocols sometimes don’t 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

WEP encryption

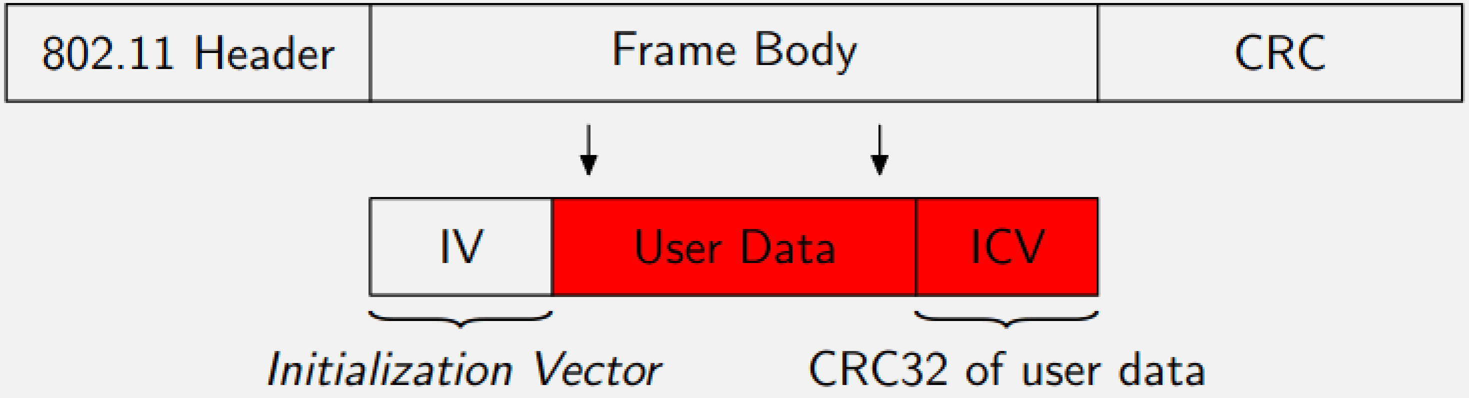
“Wired Equivalent Privacy”

- 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



802.11 Header

Frame Body

CRC

IV

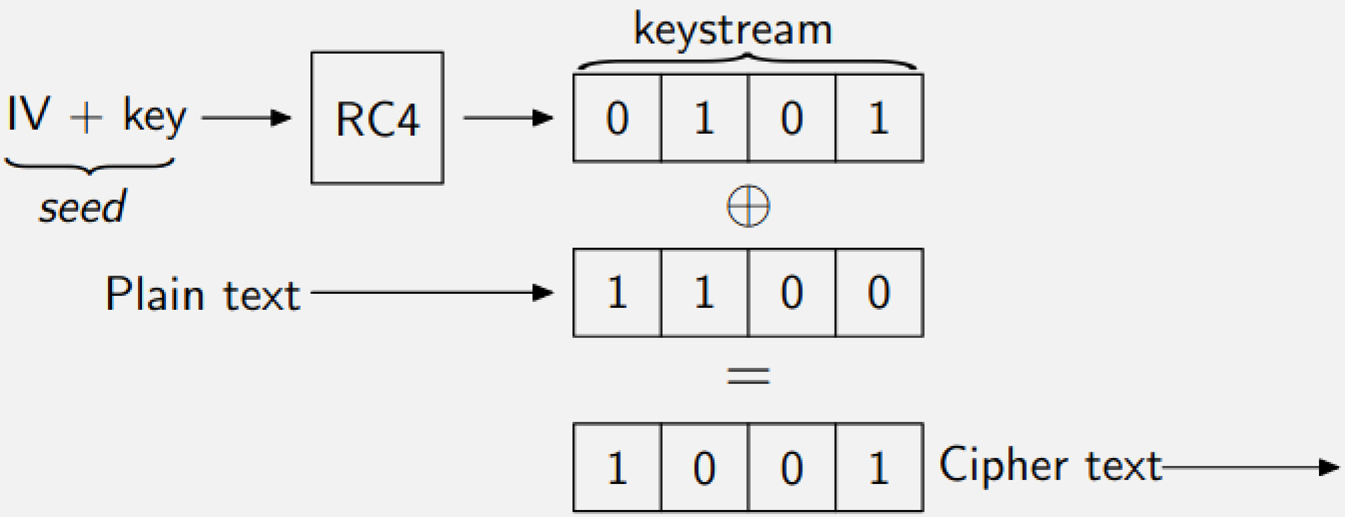
User Data

ICV

Initialization Vector

CRC32 of user data

Encryption



keystream

IV + key

seed

RC4

0 1 0 1

⊕

Plain text

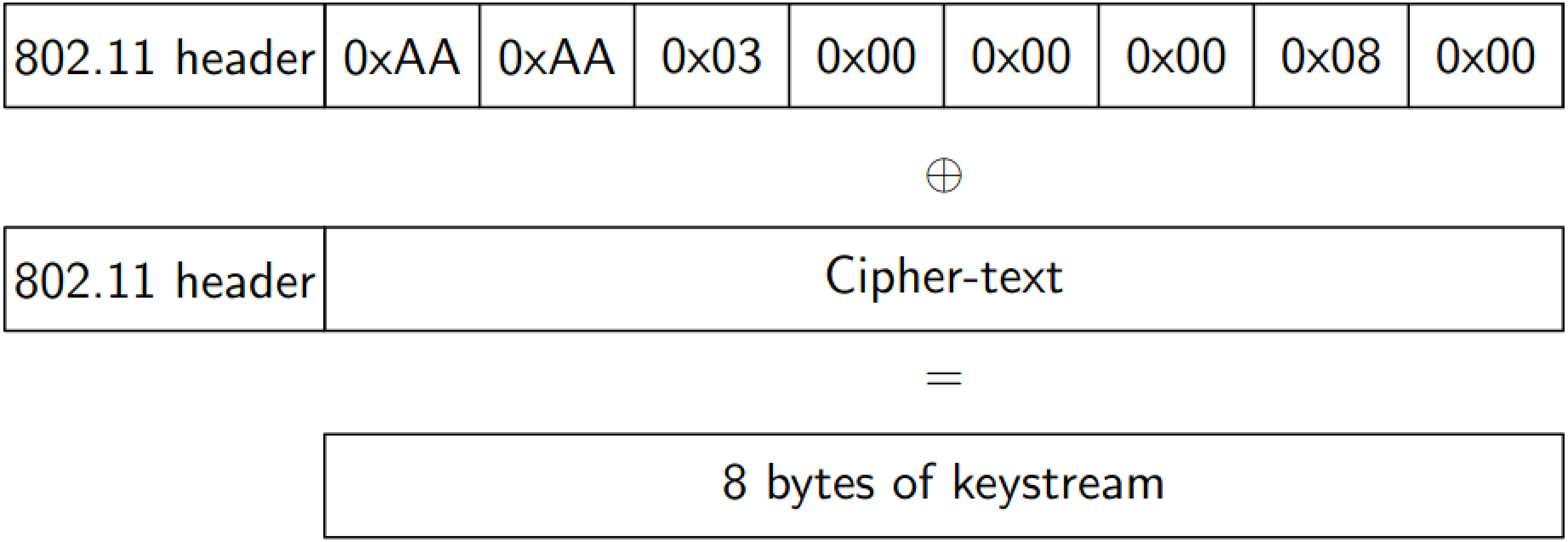
1 1 0 0

=

1 0 0 1

Cipher text

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

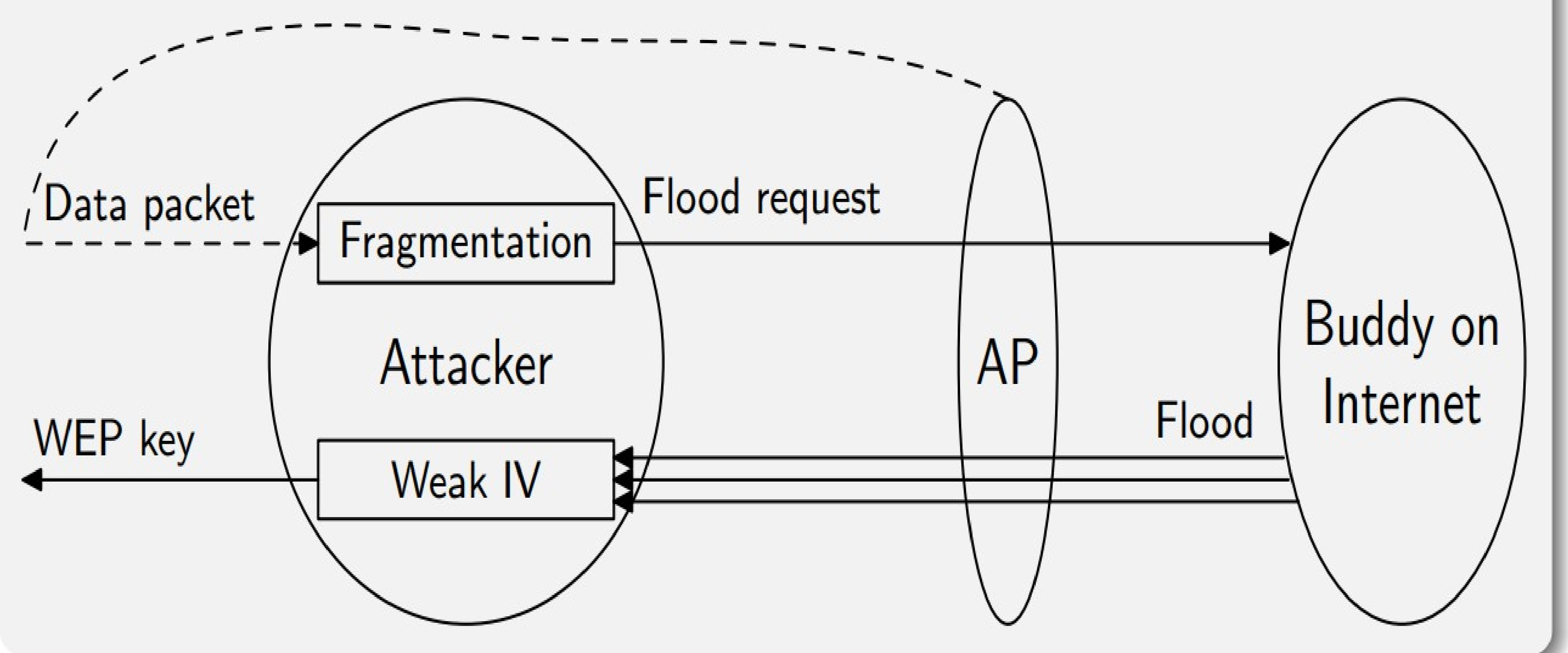
Possible to create statistical biases in the Key Scheduling Algorithm (KSA)

More info:

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

Crack WEP key in minutes…

Operation of wesside



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

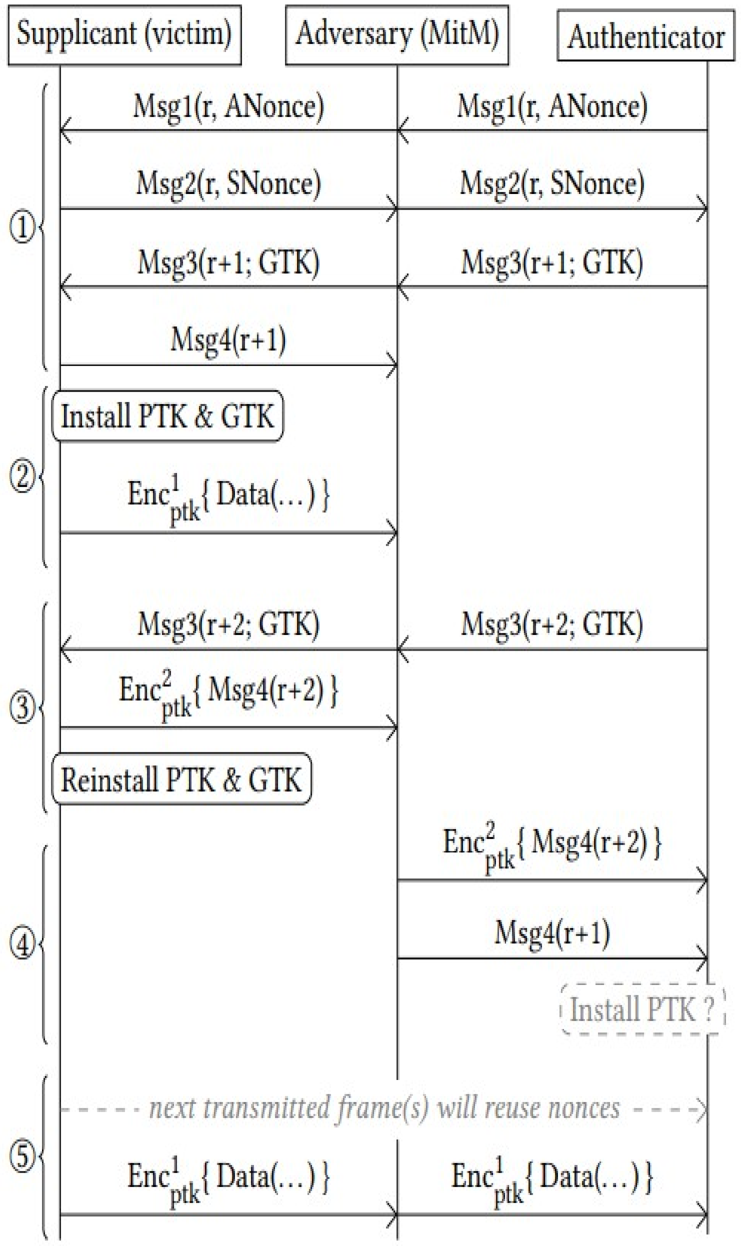

Supplicant (victim)
Adversary (MitM)
Authenticator
①
Msg1(r, ANonce)
Msg1(r, ANonce)
Msg2(r, SNonce)
Msg2(r, SNonce)
Msg3(r+1; GTK)
Msg3(r+1; GTK)
Msg4(r+1)
②
Install PTK & GTK
$\text{Enc}^1_{\text{ptk}}\{\text{Data}(\ldots)\}$
③
Msg3(r+2; GTK)
Msg3(r+2; GTK)
$\text{Enc}^2_{\text{ptk}}\{\text{Msg4}(r+2)\}$
Reinstall PTK & GTK
④
$\text{Enc}^2_{\text{ptk}}\{\text{Msg4}(r+2)\}$
Msg4(r+1)
Install PTK ?
⑤
next transmitted frame(s) will reuse nonces
$\text{Enc}^1_{\text{ptk}}\{\text{Data}(\ldots)\}$
$\text{Enc}^1_{\text{ptk}}\{\text{Data}(\ldots)\}$

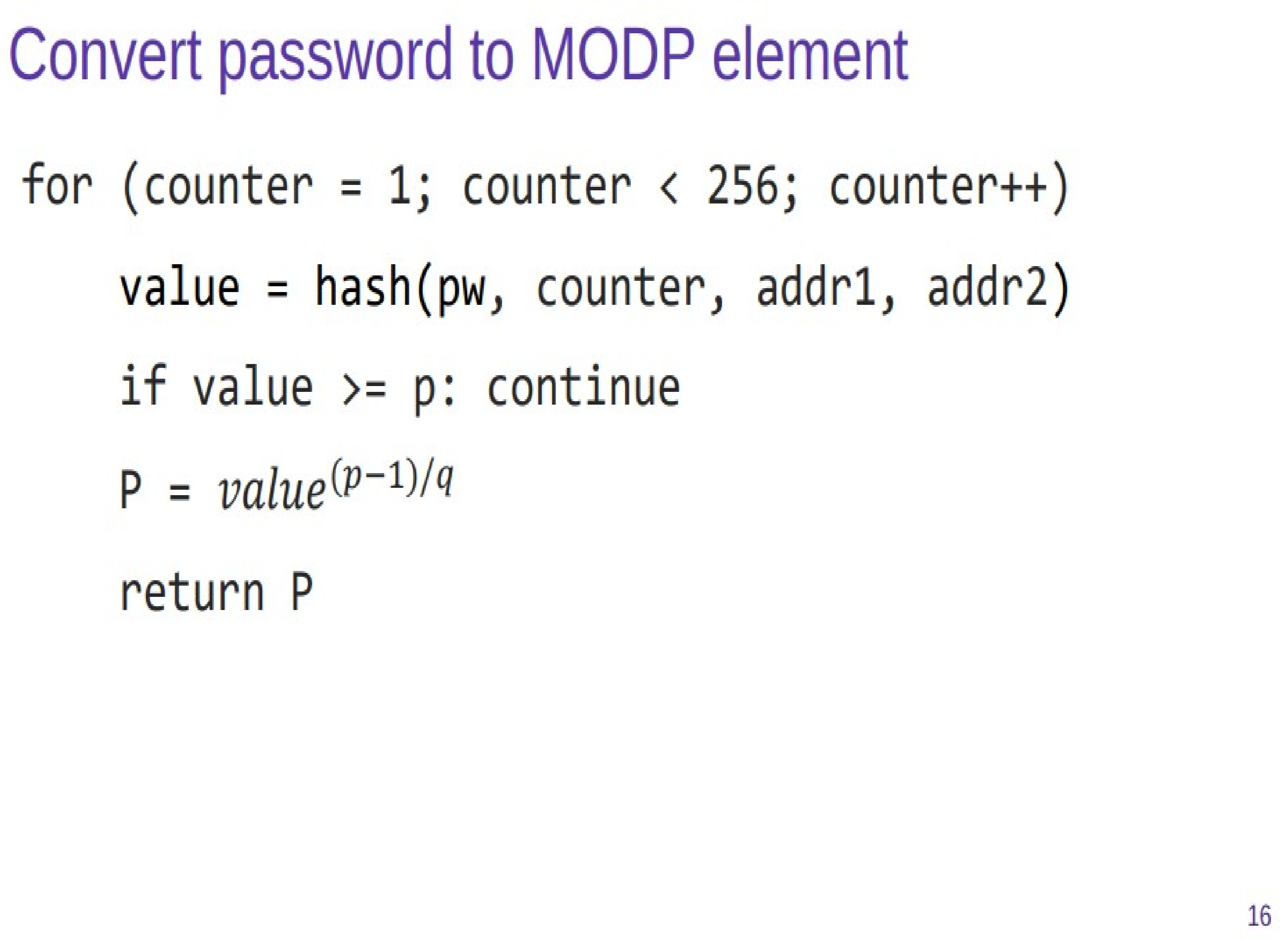
Figure 4: Key reinstallation attack against the 4-way handshake, when the supplicant (victim) still accepts plaintext retransmissions of message 3 if a PTK is installed.

KRACK attacks

Dragonblood attacks on WPA3

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

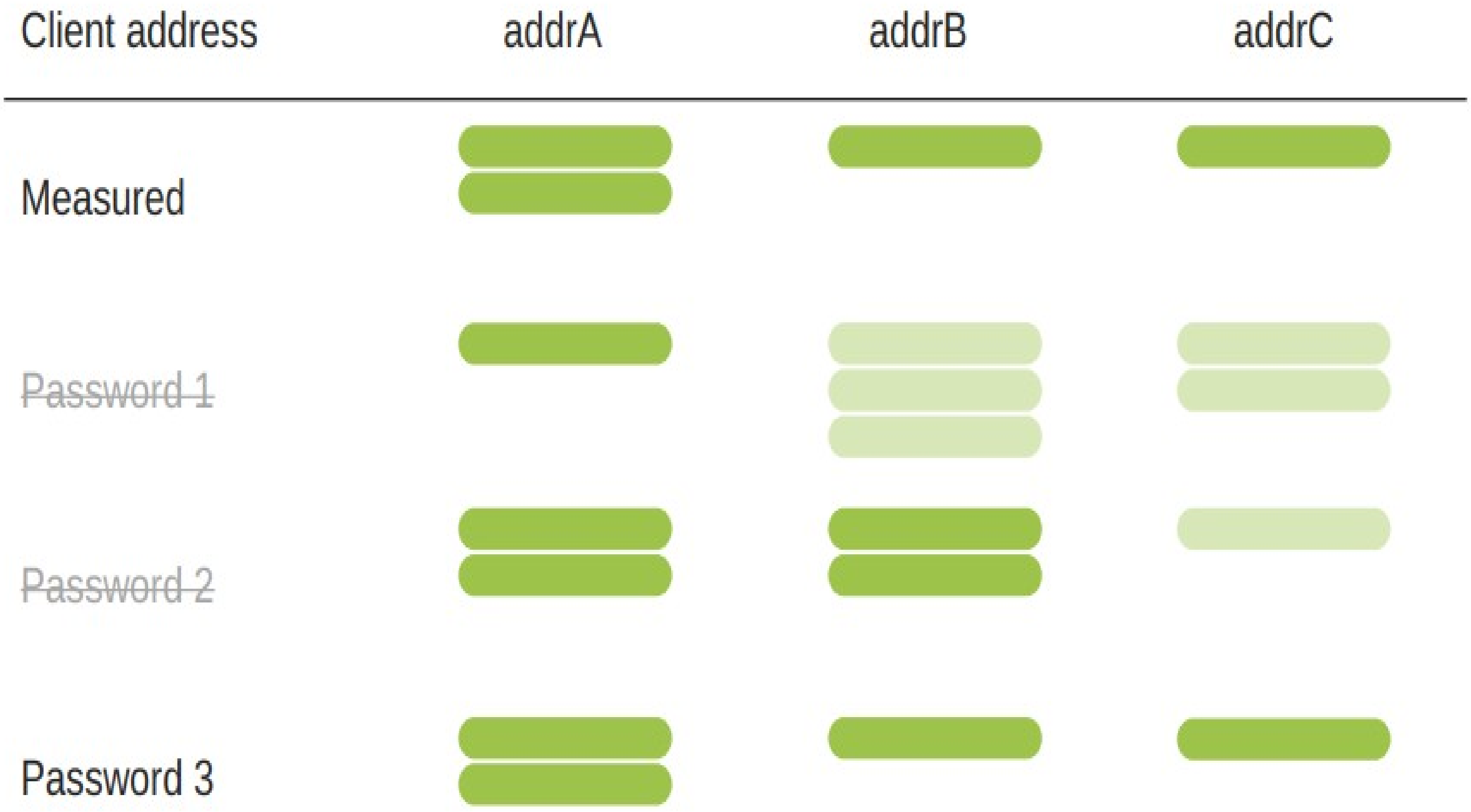
  https://papers.mathyvanhoef.com/wac2019-slides.pdf



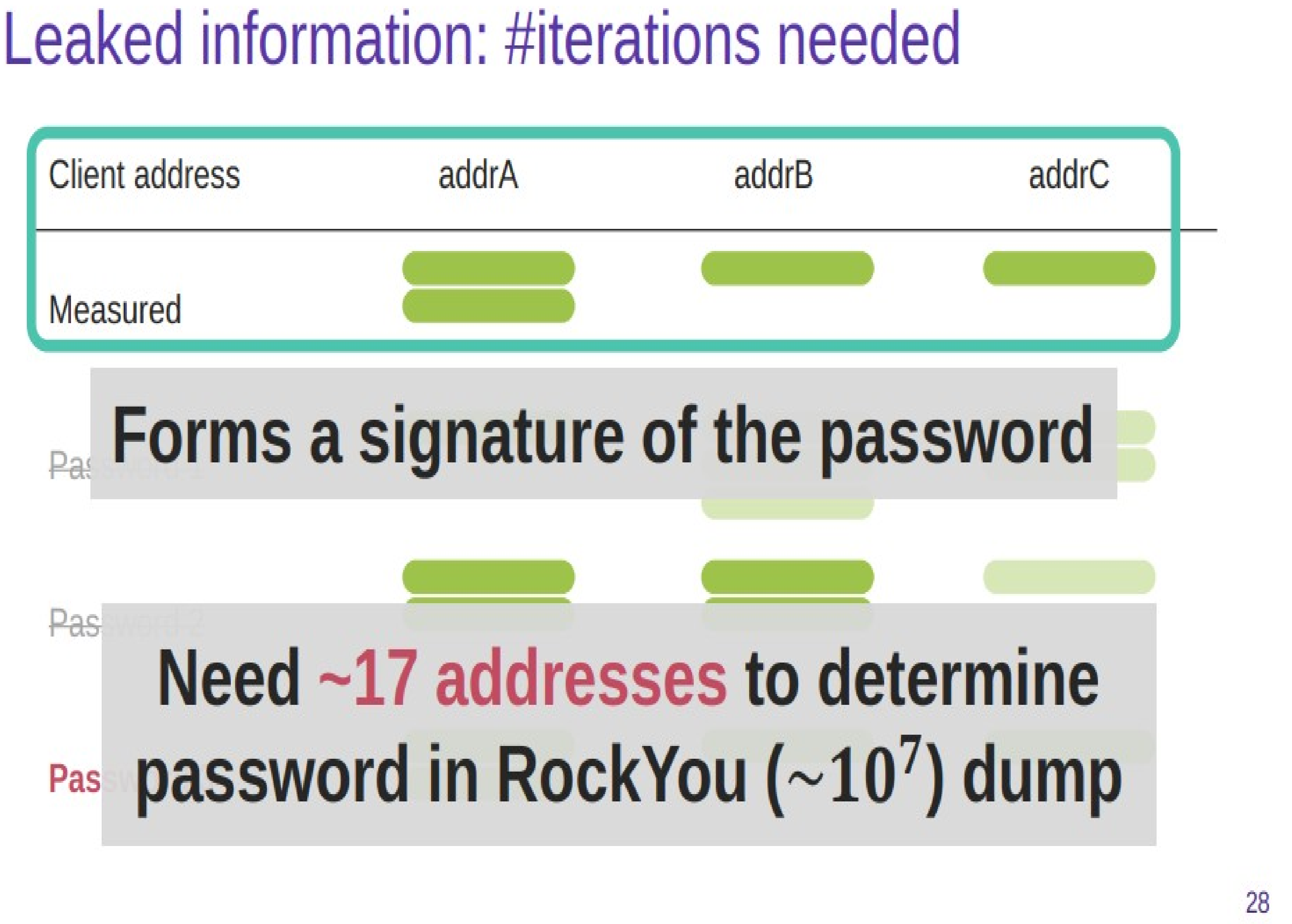
Convert password to MODP element

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

Leaked information: #iterations needed



Client address	addrA	addrB	addrC
Measured	🟩 🟩	🟩	🟩
~~Password 1~~	🟩	░ ░ ░	░ ░
~~Password 2~~	🟩 🟩	🟩 🟩	░
Password 3	🟩 🟩	🟩	🟩



Leaked information: #iterations needed

Client address	addrA	addrB	addrC
Measured	🟩 🟩	🟩	🟩

Password 1

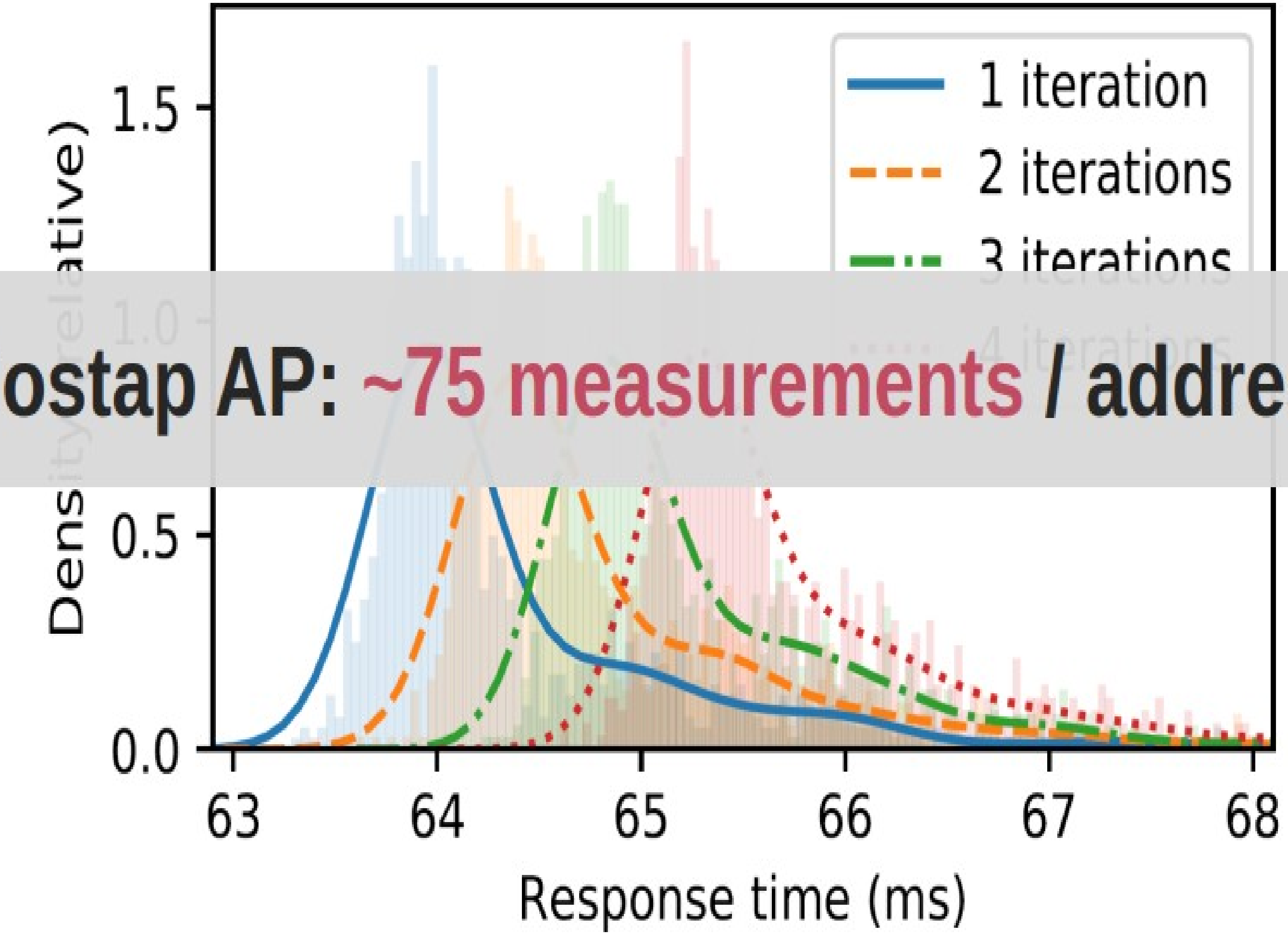
Password 2

Pas

Forms a signature of the password

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

Raspberry Pi 1 B+: differences are measurable



Hostap AP: ~75 measurements / address

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:

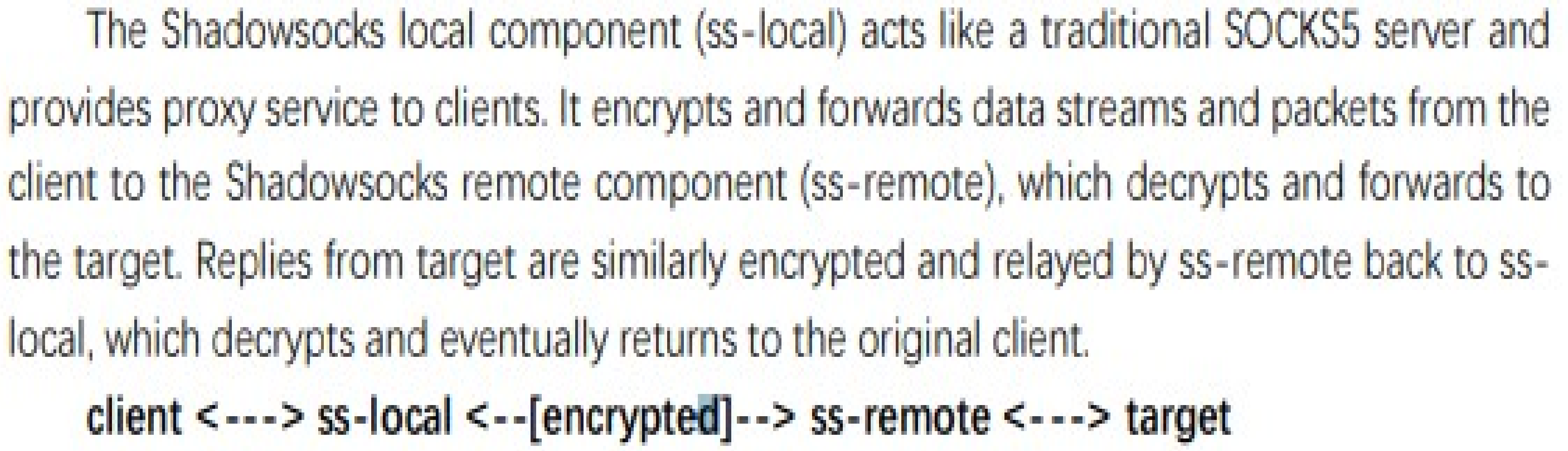
Steam ciphers (none-AEAD cipher):

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:

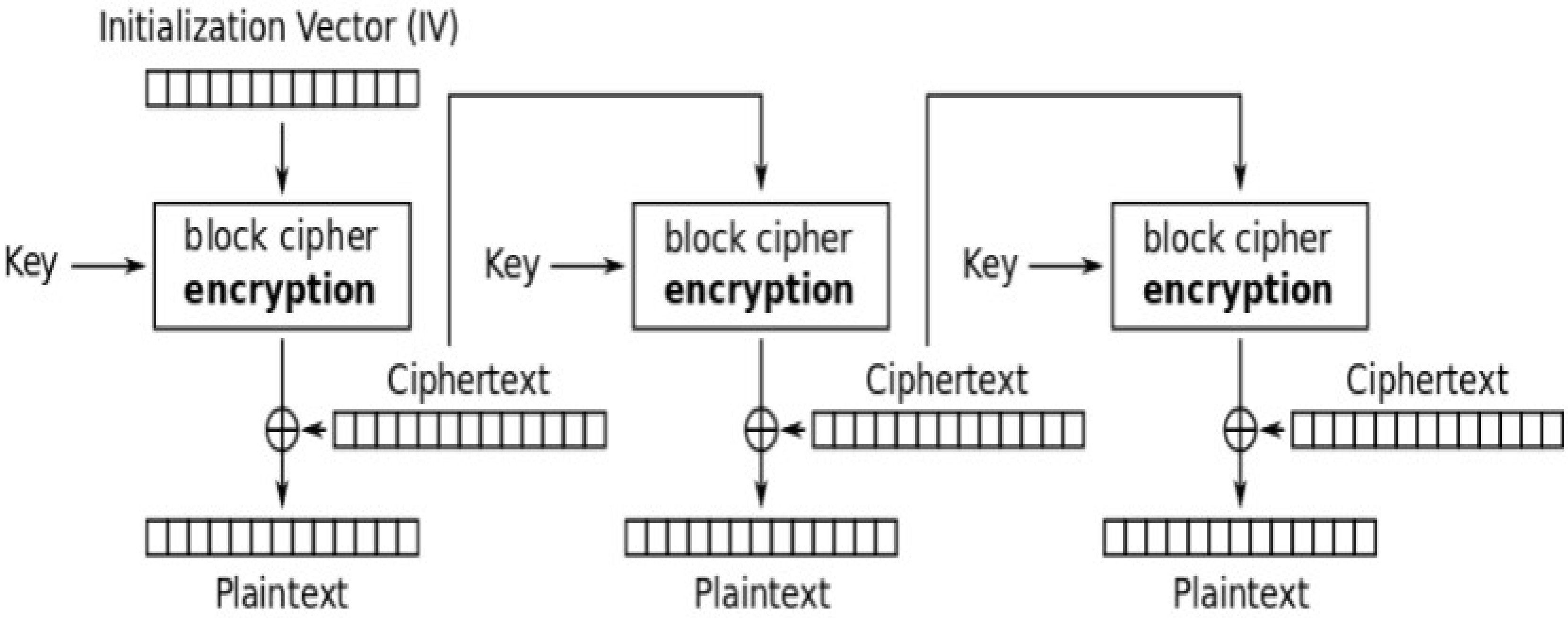
0x01: host is a 4-byte IPv4 address.

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

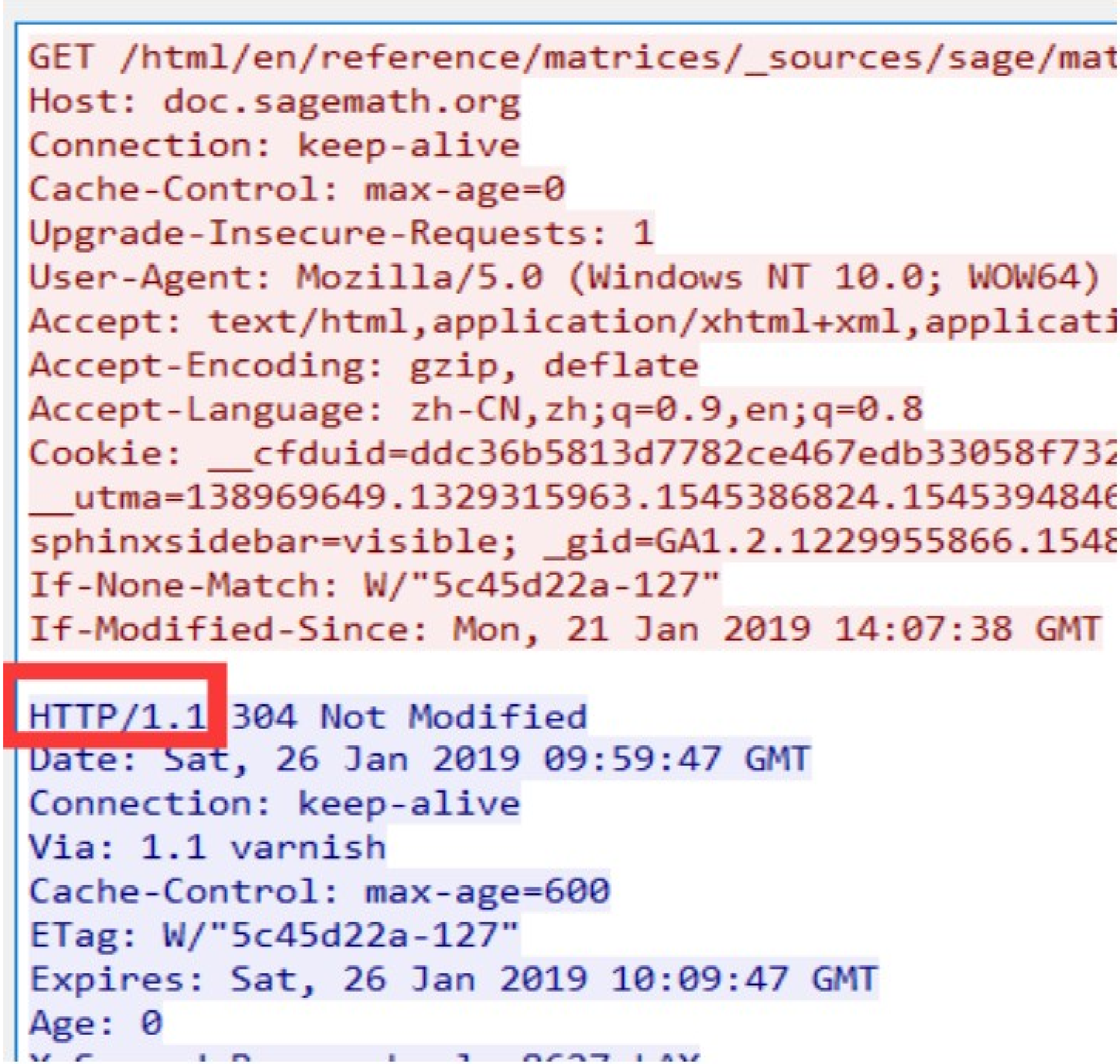
The port number is a 2-byte big-endian unsigned integer.

[IV][encrypted payload]



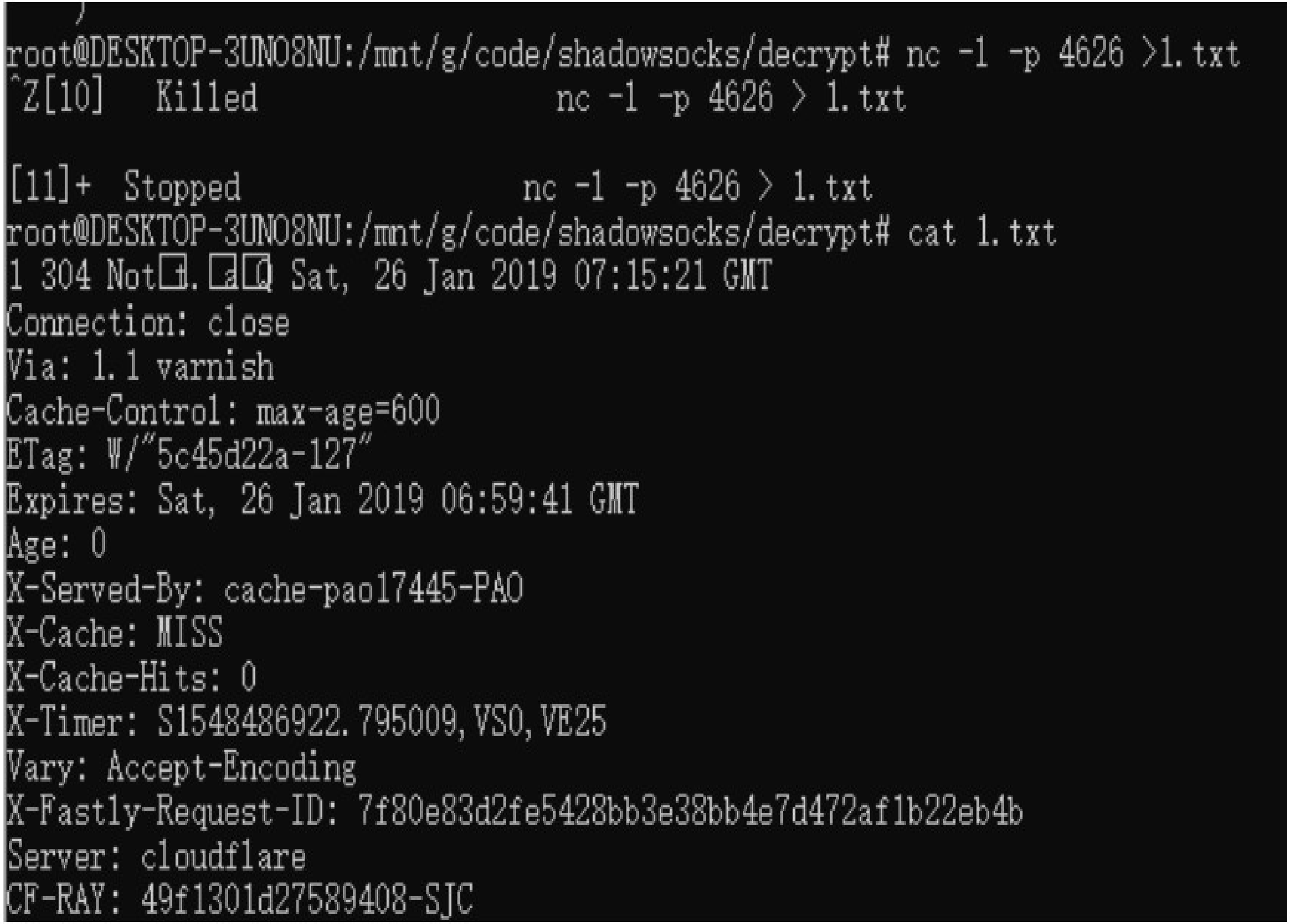
Cipher Feedback (CFB) mode decryption

IVs are chosen randomly, transmitted in plaintext.



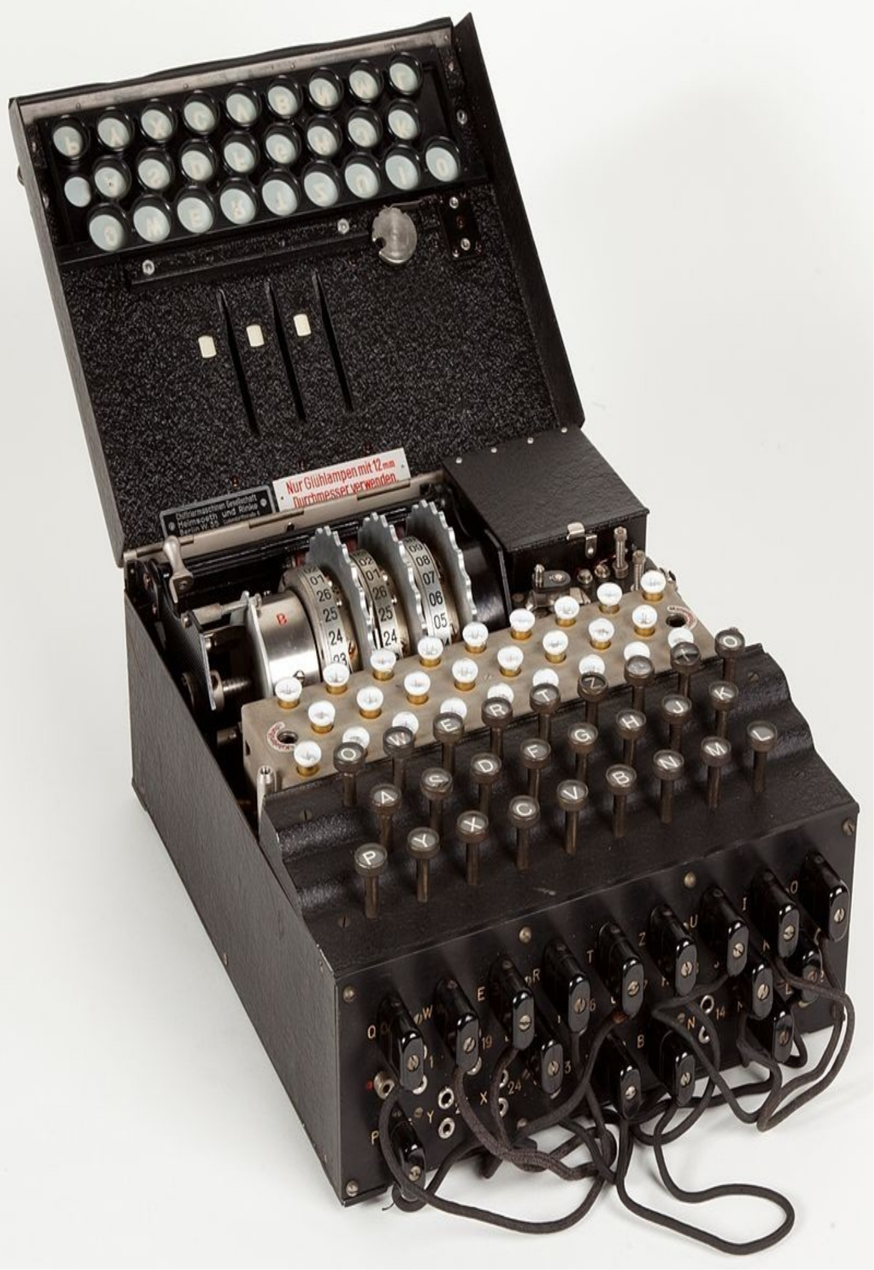
```
GET /html/en/reference/matrices/_sources/sage/mat
Host: doc.sagemath.org
Connection: keep-alive
Cache-Control: max-age=0
Upgrade-Insecure-Requests: 1
User-Agent: Mozilla/5.0 (Windows NT 10.0; WOW64)
Accept: text/html,application/xhtml+xml,applicati
Accept-Encoding: gzip, deflate
Accept-Language: zh-CN,zh;q=0.9,en;q=0.8
Cookie: __cfduid=ddc36b5813d7782ce467edb33058f732
__utma=138969649.1329315963.1545386824.154539484
sphinxsidebar=visible; _gid=GA1.2.1229955866.154
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
```



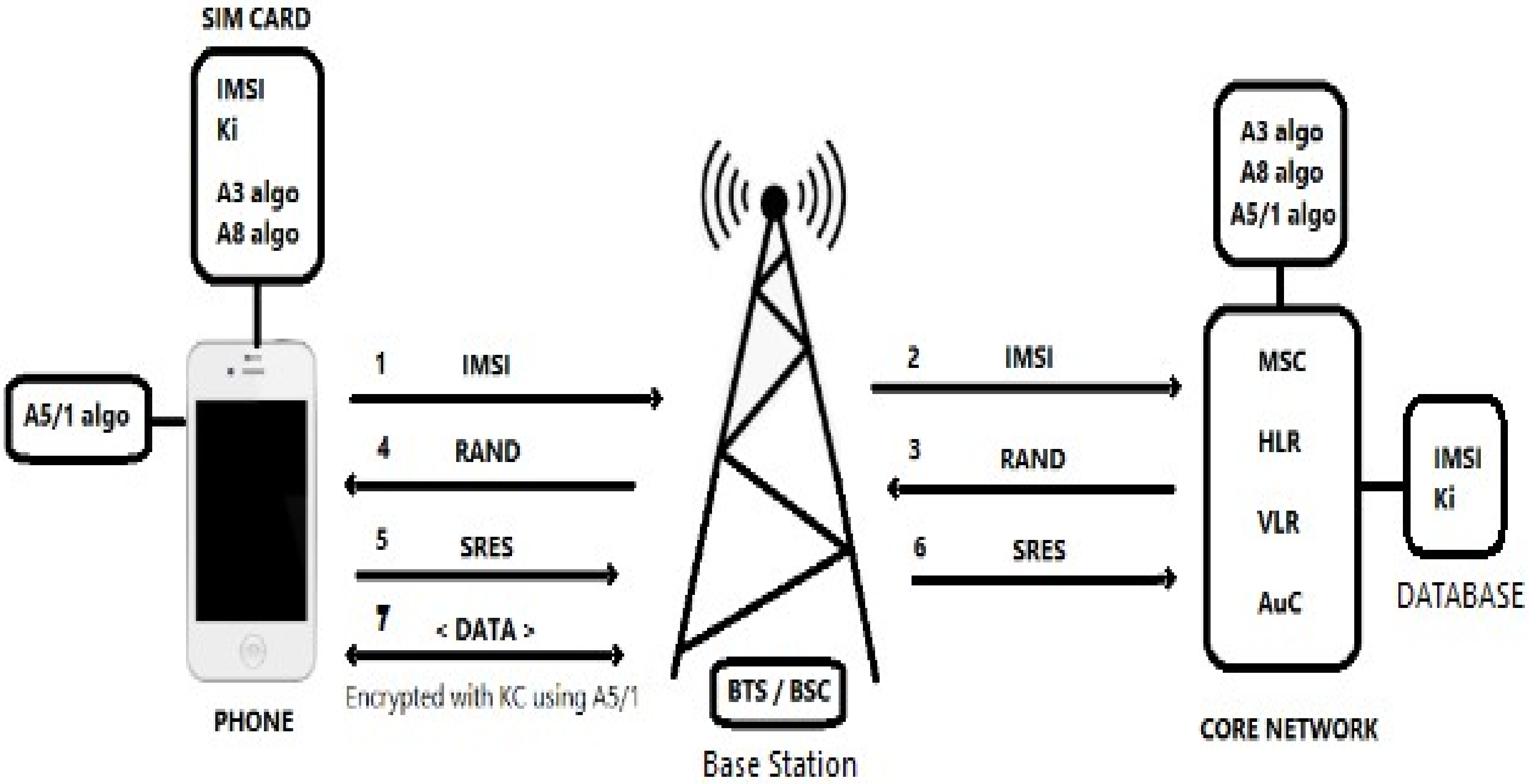
```
    )
root@DESKTOP-3UNO8NU:/mnt/g/code/shadowsocks/decrypt# nc -l -p 4626 >1.txt
^Z[10]   Killed                  nc -l -p 4626 > 1.txt

[11]+  Stopped                  nc -l -p 4626 > 1.txt
root@DESKTOP-3UNO8NU:/mnt/g/code/shadowsocks/decrypt# cat 1.txt
1 304 Not□1.□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
```



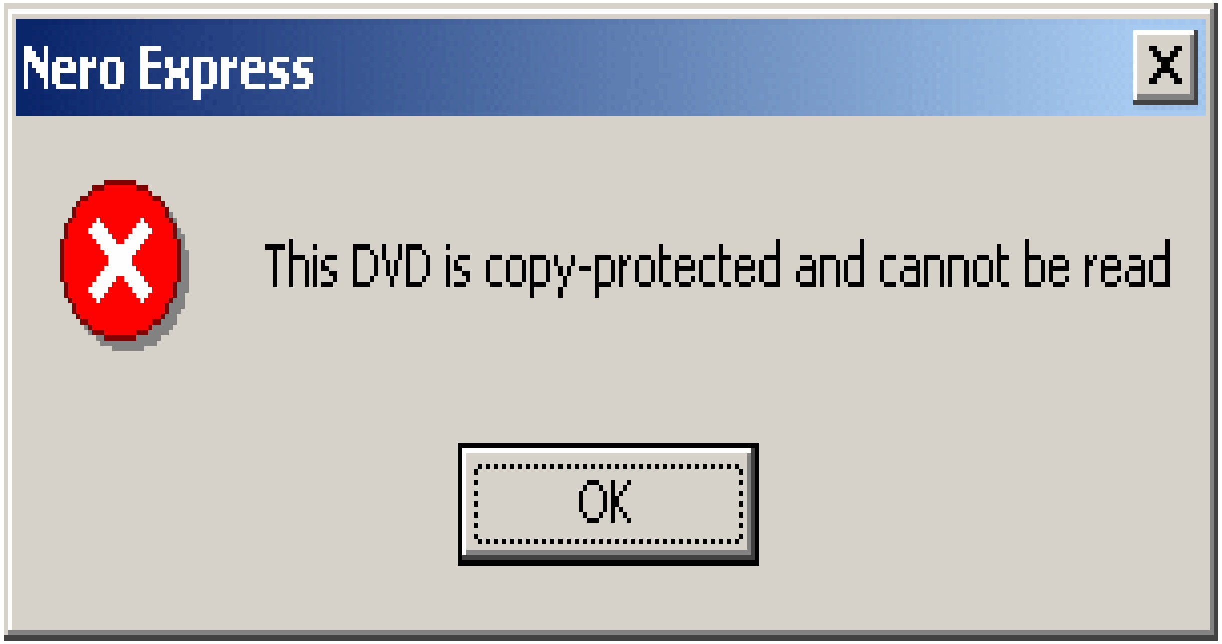
https://en.wikipedia.org/wiki/Enigma_machine#/media/File:Enigma_(crittografia)_-_Museo_scienza_e_tecnologia_Milano.jpg

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)



This DVD is copy-protected and cannot be read

High-bandwidth Digital Content Protection

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