Technologie a nástroje kybernetického boje

BSS152, 5.10. 2017

Jakub Drmola


KAL
Q.
WHAT WILL THE WARRIOR-GUARDIAN OF THE FUTURE LOOK LIKE?
YO! DUDE... BACK HERE
CYBER SECURITY

Vymezení

- **kybernetické** útoky

- tj. mimo EWar, InfoWar
  - satelity, C3, drony, atp.

Archetypy útoků

- akvizice informací
  - a následná diseminace/exploitace
- šíření informací
  - propaganda
- disrupce
  - procesů a služeb
- destrukce
  - dat/zařízení

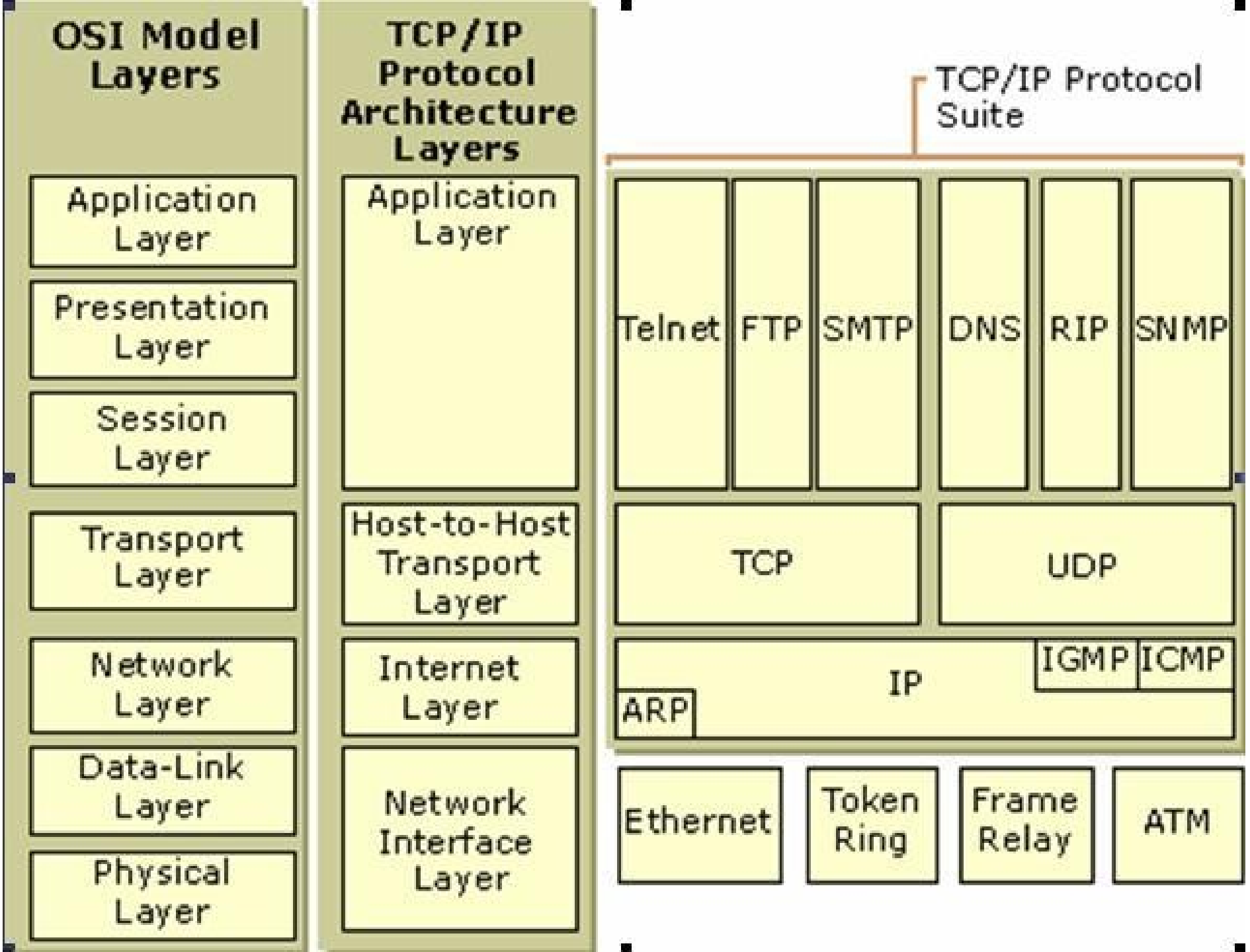
Co chráníme

- CIA

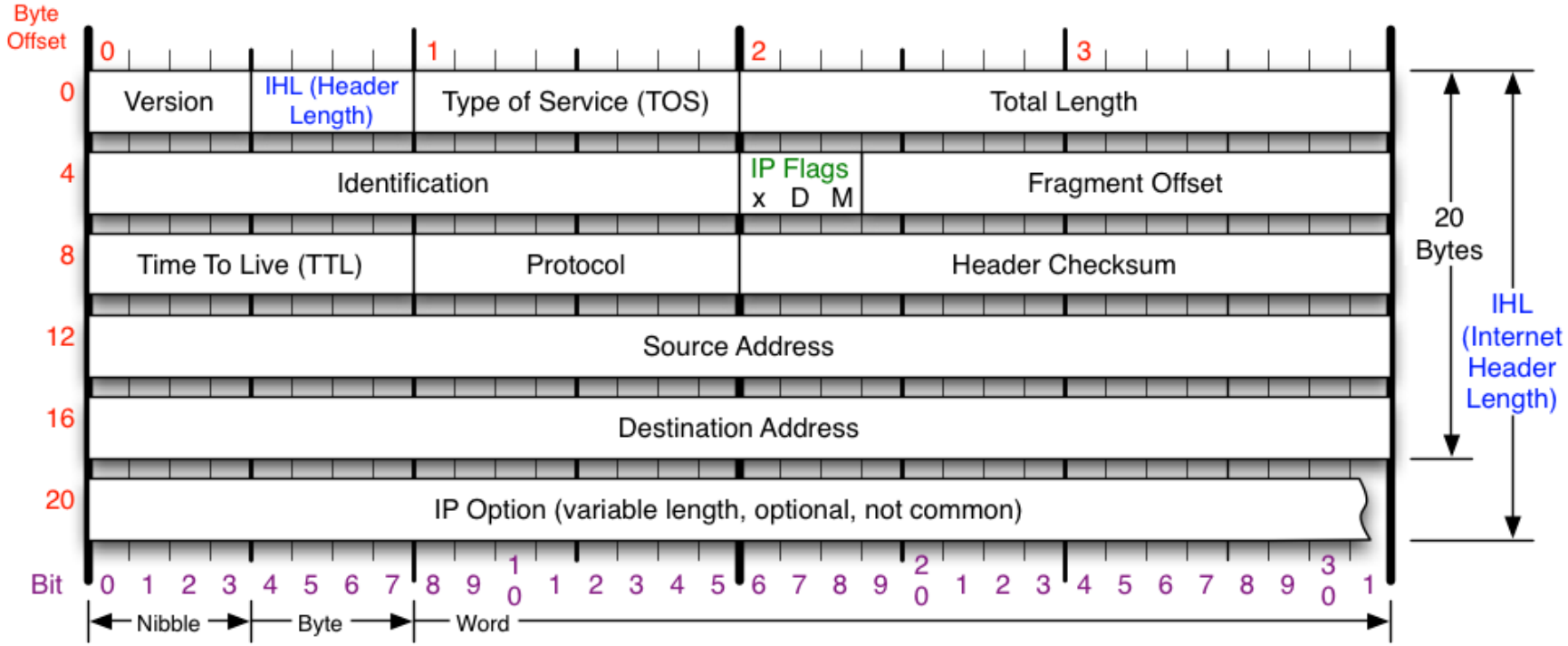
- Confidentiality
- Integrity
- Availability

Technické minimum

- aneb jak funguje internet
- a některé další důležité technologie


OSI Model Layers
Application Layer
Presentation Layer
Session Layer
Transport Layer
Network Layer
Data-Link Layer
Physical Layer
TCP/IP Protocol Architecture Layers
Application Layer
Host-to-Host Transport Layer
Internet Layer
Network Interface Layer
TCP/IP Protocol Suite
Telnet
FTP
SMTP
DNS
RIP
SNMP
TCP
UDP
IGMP
ICMP
IP
ARP
Ethernet
Token Ring
Frame Relay
ATM

IPv4 Header



Version

Version of IP Protocol. 4 and 6 are valid. This diagram represents version 4 structure only.

Header Length

Number of 32-bit words in TCP header, minimum value of 5. Multiply by 4 to get byte count.

Protocol

IP Protocol ID. Including (but not limited to):

1 ICMP	17 UDP	57 SKIP
2 IGMP	47 GRE	88 EIGRP
6 TCP	50 ESP	89 OSPF
9 IGRP	51 AH	115 L2TP

Total Length

Total length of IP datagram, or IP fragment if fragmented. Measured in Bytes.

Fragment Offset

Fragment offset from start of IP datagram. Measured in 8 byte (2 words, 64 bits) increments. If IP datagram is fragmented, fragment size (Total Length) must be a multiple of 8 bytes.

Header Checksum

Checksum of entire IP header

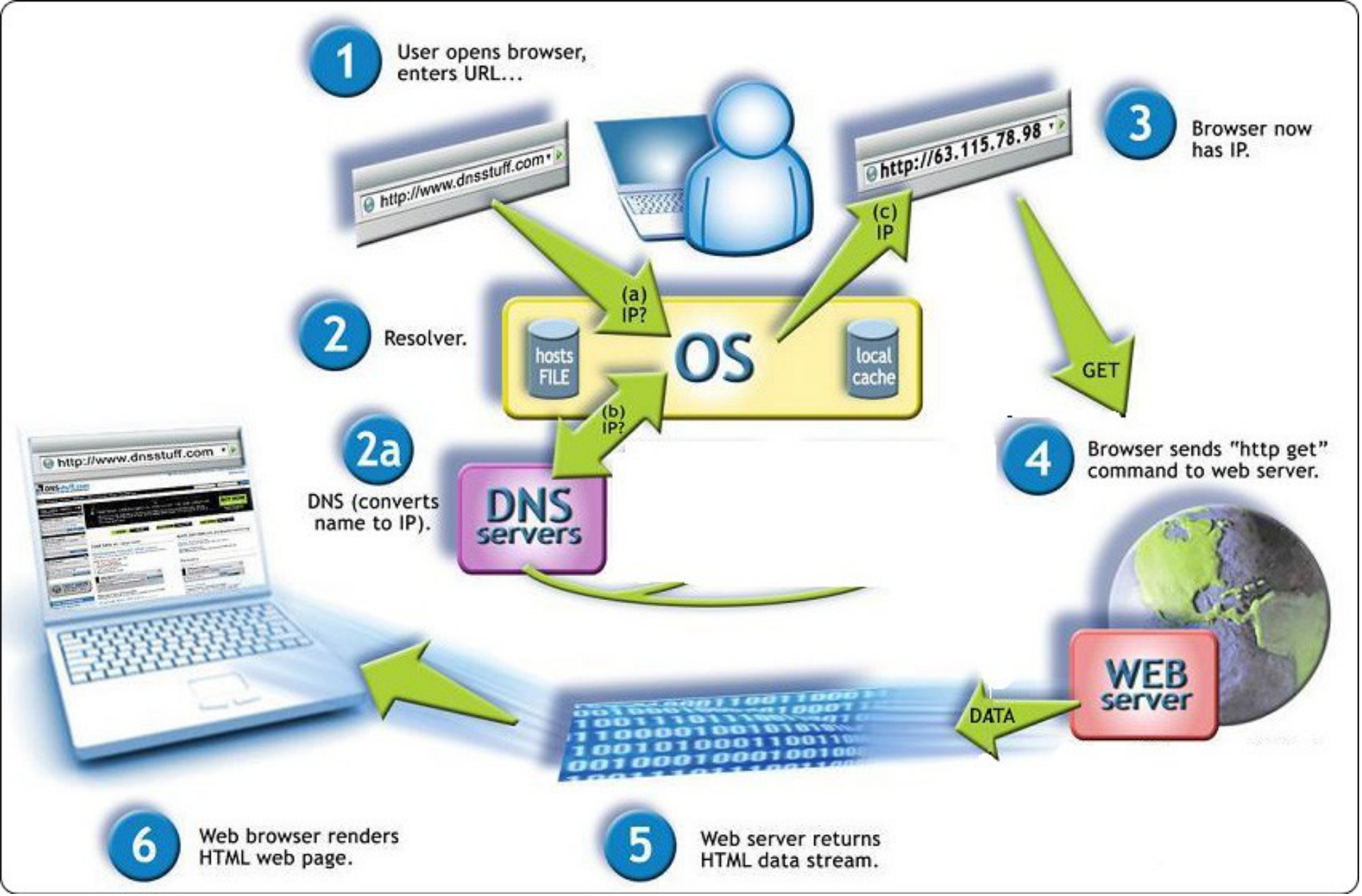
IP Flags

x D M

x 0x80 reserved (evil bit)
D 0x40 Do Not Fragment
M 0x20 More Fragments follow

RFC 791

Please refer to RFC 791 for the complete Internet Protocol (IP) Specification.


1
User opens browser, enters URL...
http://www.dnsstuff.com
2
Resolver.
(a) IP?
hosts FILE
OS
local cache
(b) IP?
(c) IP
http://63.115.78.98
3
Browser now has IP.
GET
2a
DNS (converts name to IP).
DNS servers
4
Browser sends "http get" command to web server.
http://www.dnsstuff.com
WEB server
DATA
6
Web browser renders HTML web page.
5
Web server returns HTML data stream.

Východiska

- většina škod neúmyslná
  - bugy, nehody, přírodní katastrofy, ...
- případně útoky zevnitř
  - např. nespokojení zaměstnanci

- útoky v zásadě spočívají v nalezení a využití nějaké existující slabiny
  - lidské, strukturální, implementační, technické
  - neexistuje dokonalý systém

Častá tvrzení

- „biliony útoků“
- „jsme čím dál zranitelnější“
- airgap

Síťové útoky

- DDoS
  - botnet
  - LOIC
  - IRC
  - https://threatmap.fortiguard.com/
- spoofing
- Man in the Middle

Low Orbit Ion Cannon | U dun goofed | v. 1.1.0.9

p.s cocks

Manual Mode (for pussies) | FUCKING HIVE MIND | IRC server | Port: 6667 | Channel: #loic | Connected!

1. Select your target

URL: www.davenportlyons.com — Lock on

IP: — Lock on

2. Ready?

Stop flooding

Selected target

85.116.9.83

3. Attack options

Timeout: 4000

HTTP Subsite: /119/

Append random chars to the URL

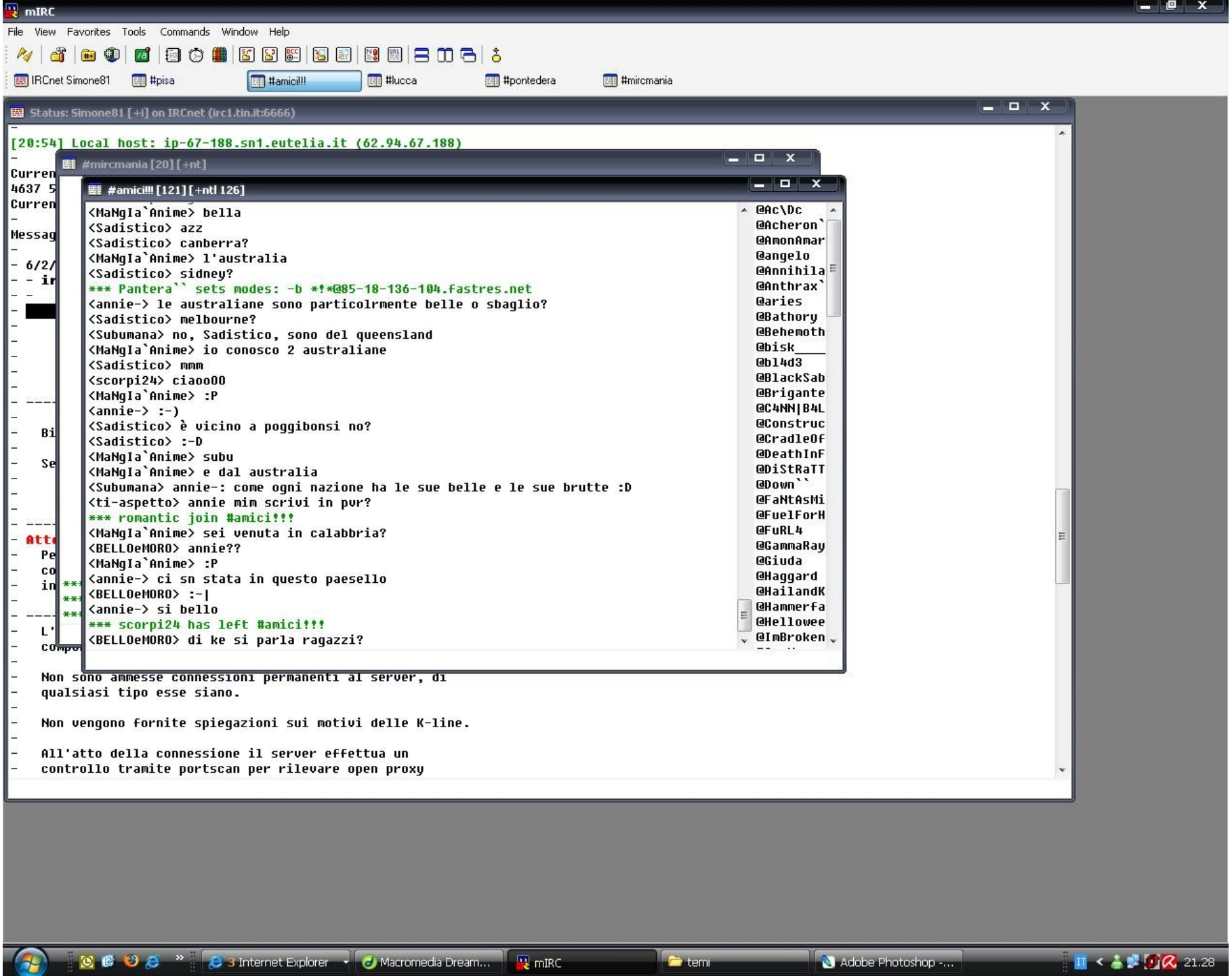
TCP / UDP message: U dun goofed

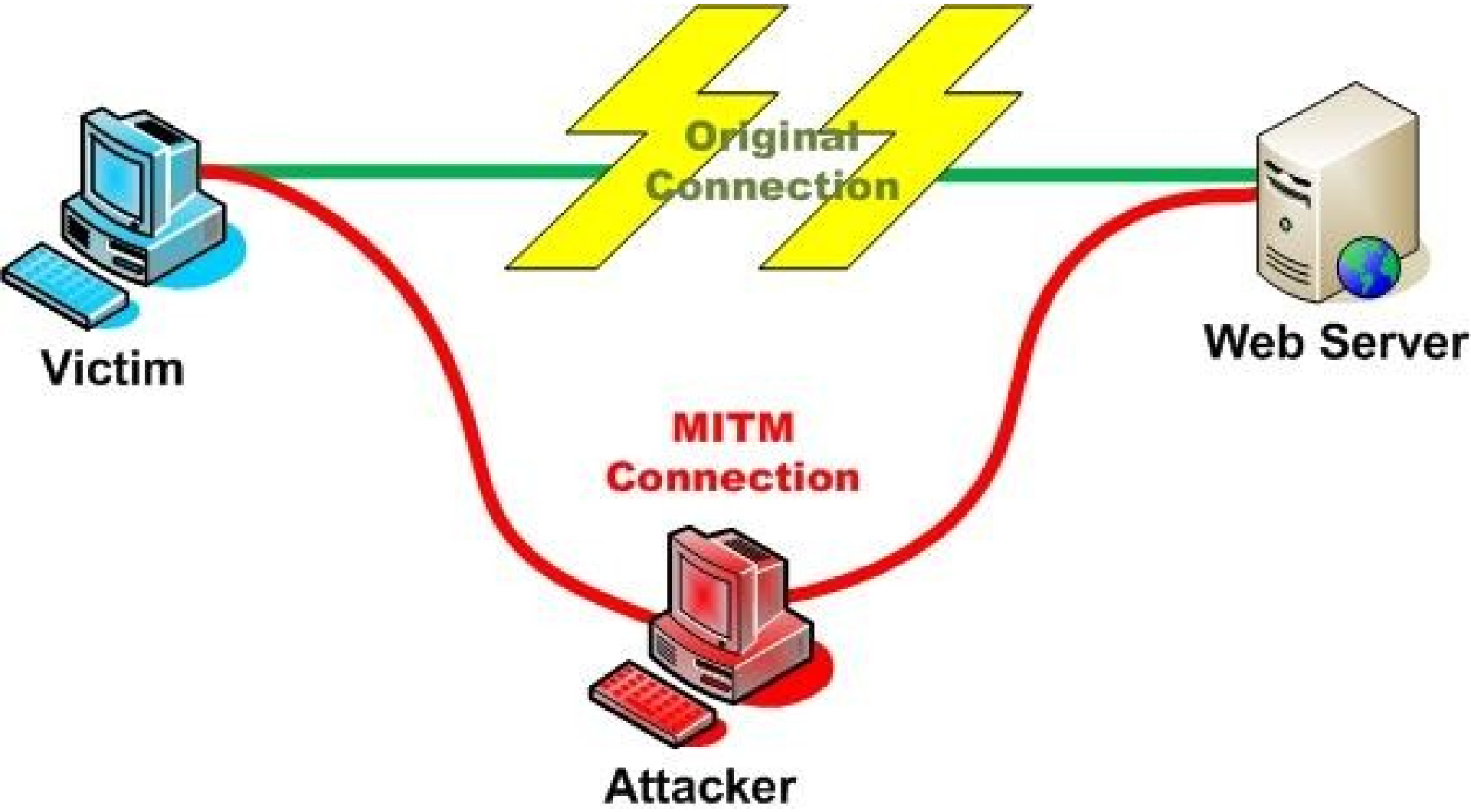
Port: 80 | Method: HTTP | Threads: 10 | Wait for reply

<= faster Speed slower =>

Attack status

Idle	Connecting	Requesting	Downloading	Downloaded	Requested	Failed
1	9	0	0	419	419	9


mIRC
File View Favorites Tools Commands Window Help
IRCnet Simone81
#pisa
#amici!!!
#lucca
#pontedera
#mircmania
Status: Simone81 [+i] on IRCnet (irc1.tin.it:6666)
[20:54] Local host: ip-67-188.sn1.eutelia.it (62.94.67.188)
#mircmania [20] [+nt]
#amici!!! [121] [+ntl 126]
<MaNgIa`Anime> bella
<Sadistico> azz
<Sadistico> canberra?
<MaNgIa`Anime> l'australia
<Sadistico> sidney?
*** Pantera`` sets modes: -b *!*@85-18-136-104.fastres.net
<annie-> le australiane sono particolrmente belle o sbaglio?
<Sadistico> melbourne?
<Subumana> no, Sadistico, sono del queensland
<MaNgIa`Anime> io conosco 2 australiane
<Sadistico> mmm
<scorpi24> ciaooOO
<MaNgIa`Anime> :P
<annie-> :-)
<Sadistico> è vicino a poggibonsi no?
<Sadistico> :-D
<MaNgIa`Anime> subu
<MaNgIa`Anime> e dal australia
<Subumana> annie-: come ogni nazione ha le sue belle e le sue brutte :D
<ti-aspetto> annie mim scrivi in pvr?
*** romantic join #amici!!!
<MaNgIa`Anime> sei venuta in calabbria?
<BELLOeMORO> annie??
<MaNgIa`Anime> :P
<annie-> ci sn stata in questo paesello
<BELLOeMORO> :-|
<annie-> si bello
*** scorpi24 has left #amici!!!
<BELLOeMORO> di ke si parla ragazzi?
@Ac\Dc
@Acheron`
@AmonAmar
@angelo
@Annihila
@Anthrax`
@aries
@Bathory
@Behemoth
@bisk____
@bl4d3
@BlackSab
@Brigante
@C4NN|B4L
@Construc
@CradleOf
@DeathInF
@DiStRaTT
@Down``
@FaNtAsMi
@FuelForH
@FuRL4
@GammaRay
@Giuda
@Haggard
@HailandK
@Hammerfa
@Hellowee
@ImBroken
Non sono ammesse connessioni permanenti al server, di
qualsiasi tipo esse siano.
Non vengono fornite spiegazioni sui motivi delle K-line.
All'atto della connessione il server effettua un
controllo tramite portscan per rilevare open proxy
Internet Explorer
Macromedia Dream...
mIRC
temi
Adobe Photoshop -...
21.28


Original Connection
Victim
Web Server
MITM Connection
Attacker

Koncové útoky

- defacement
- drive by, watering hole

- ransomware/spyware
- zero-day exploits

XSS Defacement - Opera

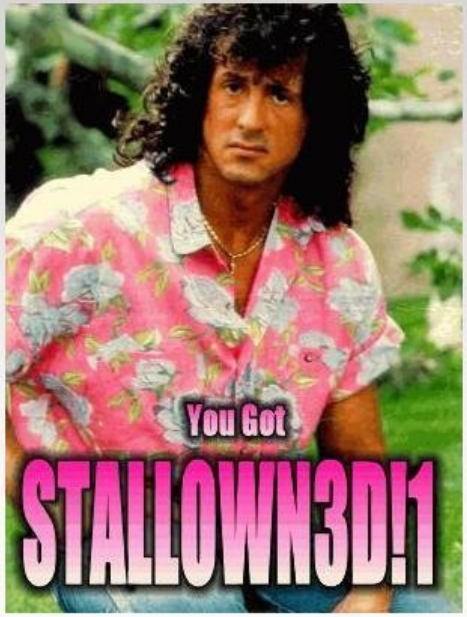
File Edit View Bookmarks Widgets Feeds Chat Tools Help

XSS Defacement | d3v1l (securityshell) o... | Security-Shell

http://www.saintcorporation.com/cgi-bin/archive.pl?cmd=index&list=%22%3E%3Cscript%20src%3d//ckers.org/s%3E%3C/script%3E

Search with Google

This page has been Hacked!



XSS Defacement

"> Search

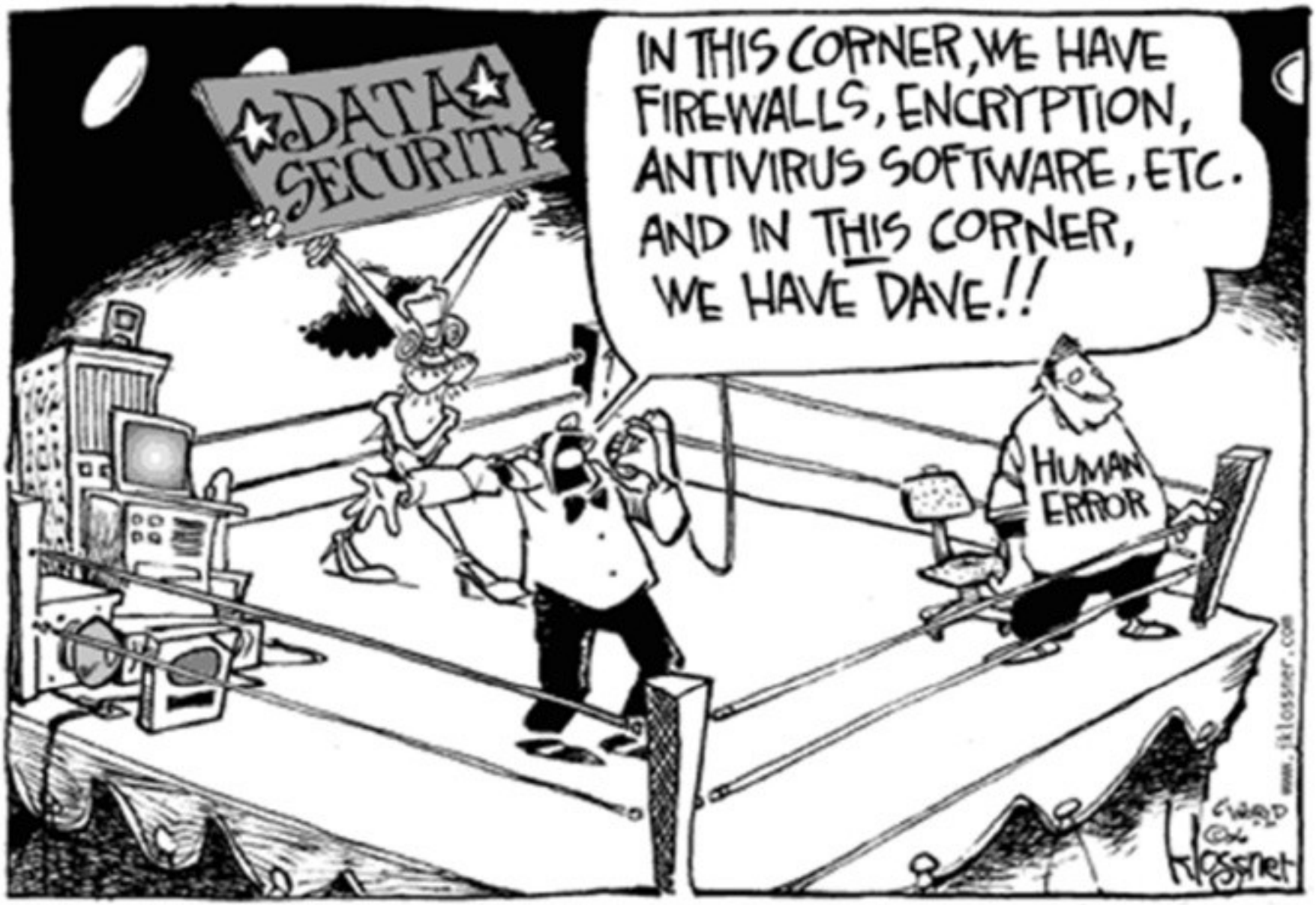
Invalid list name.

Sociální inženýrství

- využívání lidské hlouposti a naivity
- phishing, spearphishing, whalephising

- slabost a opakování hesel
- přenosná média

- uživatelská podpora, servis, snaha pomoci
- na živo, po telefonu, mailem, IM


DATA SECURITY
IN THIS CORNER, WE HAVE FIREWALLS, ENCRYPTION, ANTIVIRUS SOFTWARE, ETC.
AND IN THIS CORNER, WE HAVE DAVE!!
HUMAN ERROR
www.flossner.com
Flossner

Vypočetní síla

- kryptografie vs. mooreův zákon
- quantum computing

Kryptologie a bezpečnost

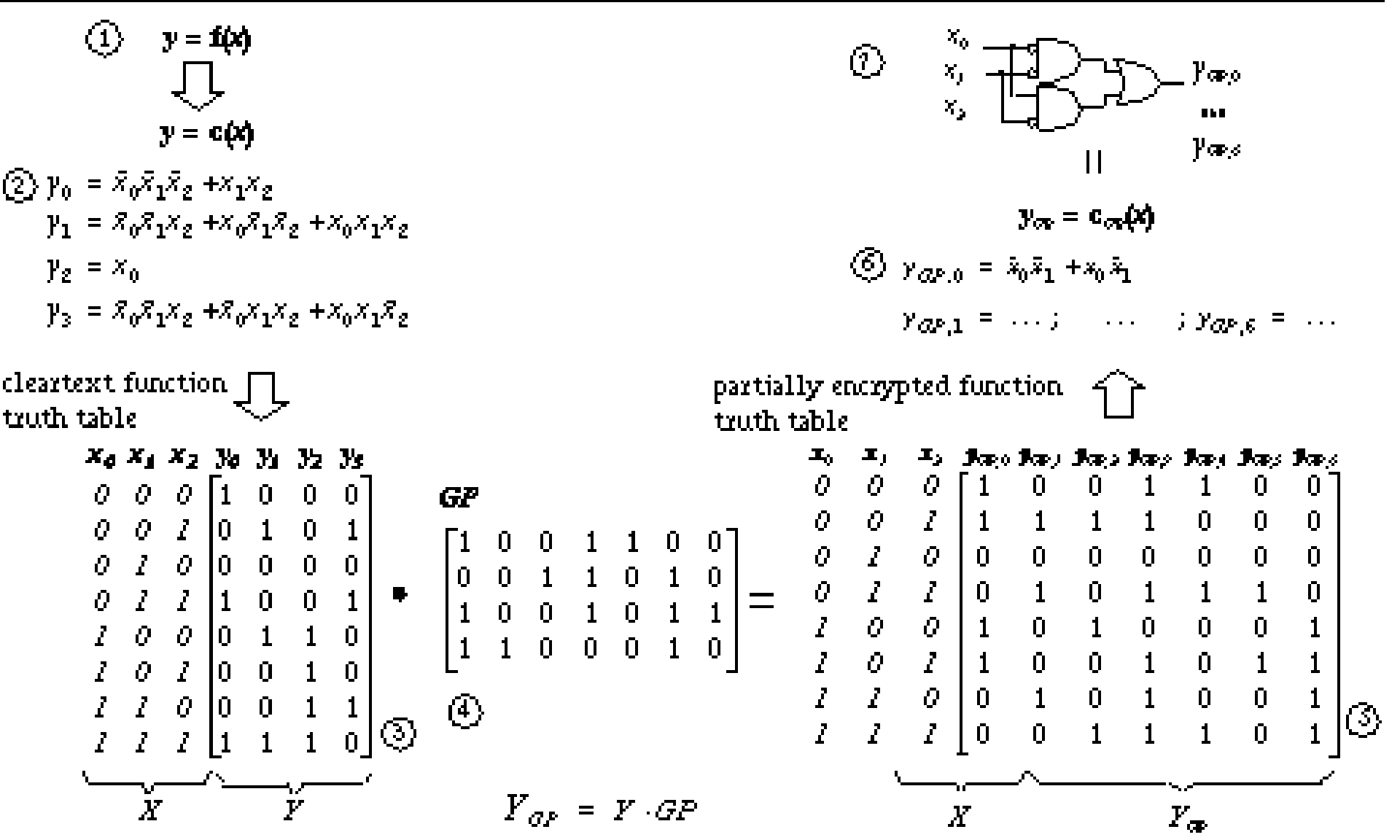


Figure 3: Encrypting a circuit : basic steps

For clarity sake, only *GP* matrix multiplication is represented. It produces a partially encrypted circuit c_{CP}. To obtain the encrypted circuit c', it necessary to use *S* and *z* too. The function to encrypt (1) is represented as a Boolean circuit *c* (2). The output matrix *Y* (3) is multiplied by *GP* (4). The result (5) is the partially encrypted output matrix Y_{CP}. It can be represented by the corresponding Boolean equations (6) or as a "partially encrypted circuit" c_{CP} (7).

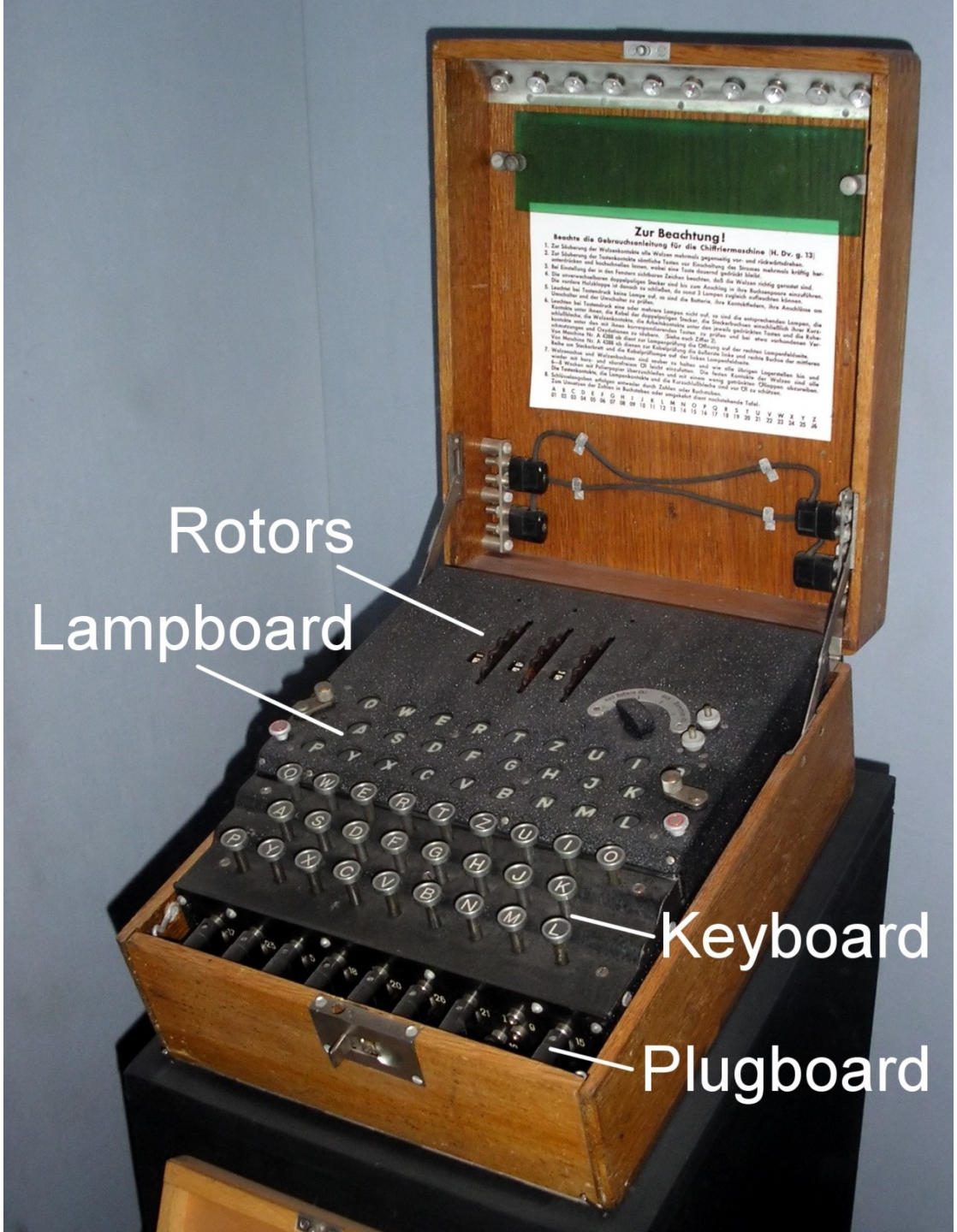
Základní úvod

- bez matematiky
- a s obrázky

- kryptologie, kryptografie, kryptoanalýza

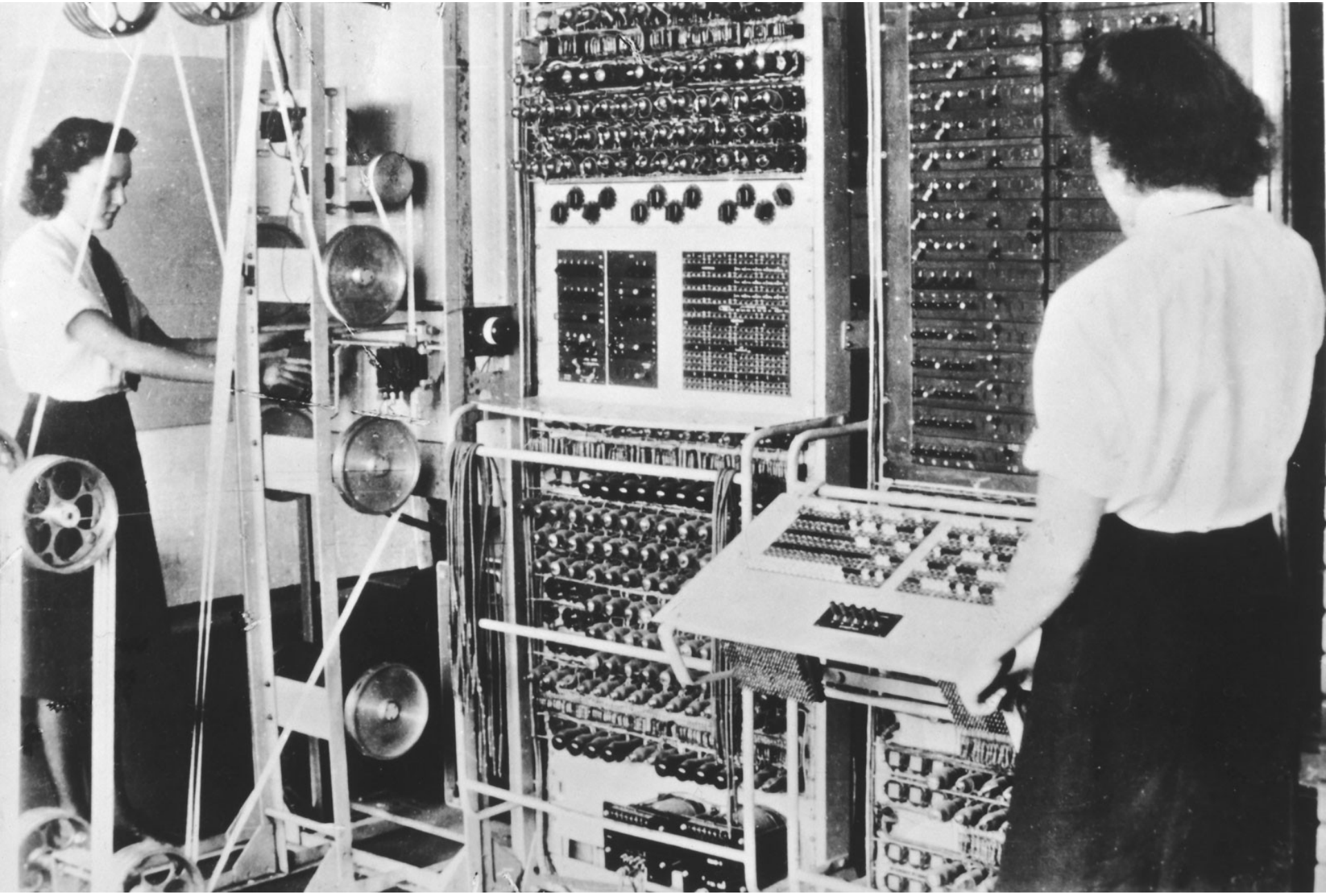
Historie

- od antiky
- pozvolný vývoj až do novověku
- revoluce ve 20. století (války)
- současnost


Rotors
Lampboard
Keyboard
Plugboard

Prolamování kódů

- frekvenční analýza
- repetice
- chyby operátorů
- kódové knihy
- hrubá síla



Některé pojmy

- Steganografie
  - kdysi a dnes
  - text, obrázky, hudba, neviditelný inkoust…
- Hash
  - + salt
- „Security through obscurity“
  - dat, algoritmu, klíče
- Symetrie a asymetrie šifer
  - „handshake“

Examples of steganography

Example 1: Coded message

Apparently neutral's protest is thoroughly discounted and ignored.
Isman hard hit. Blockade issue affects pretext for embargo on byproducts,
ejecting suets and vegetable oils.

Take second letter of each word to get message:
Pershing sails from NY June 1

Example 2: Coded images: Least Significant Bits (LSB) insertion

Original image

Altered image

▫ Areas where binary code of pixel has been altered

Binary code from original image pixel 1

10000000 10100100 10110101 10110101 11110011 10110111 11100111 10110011 00110000

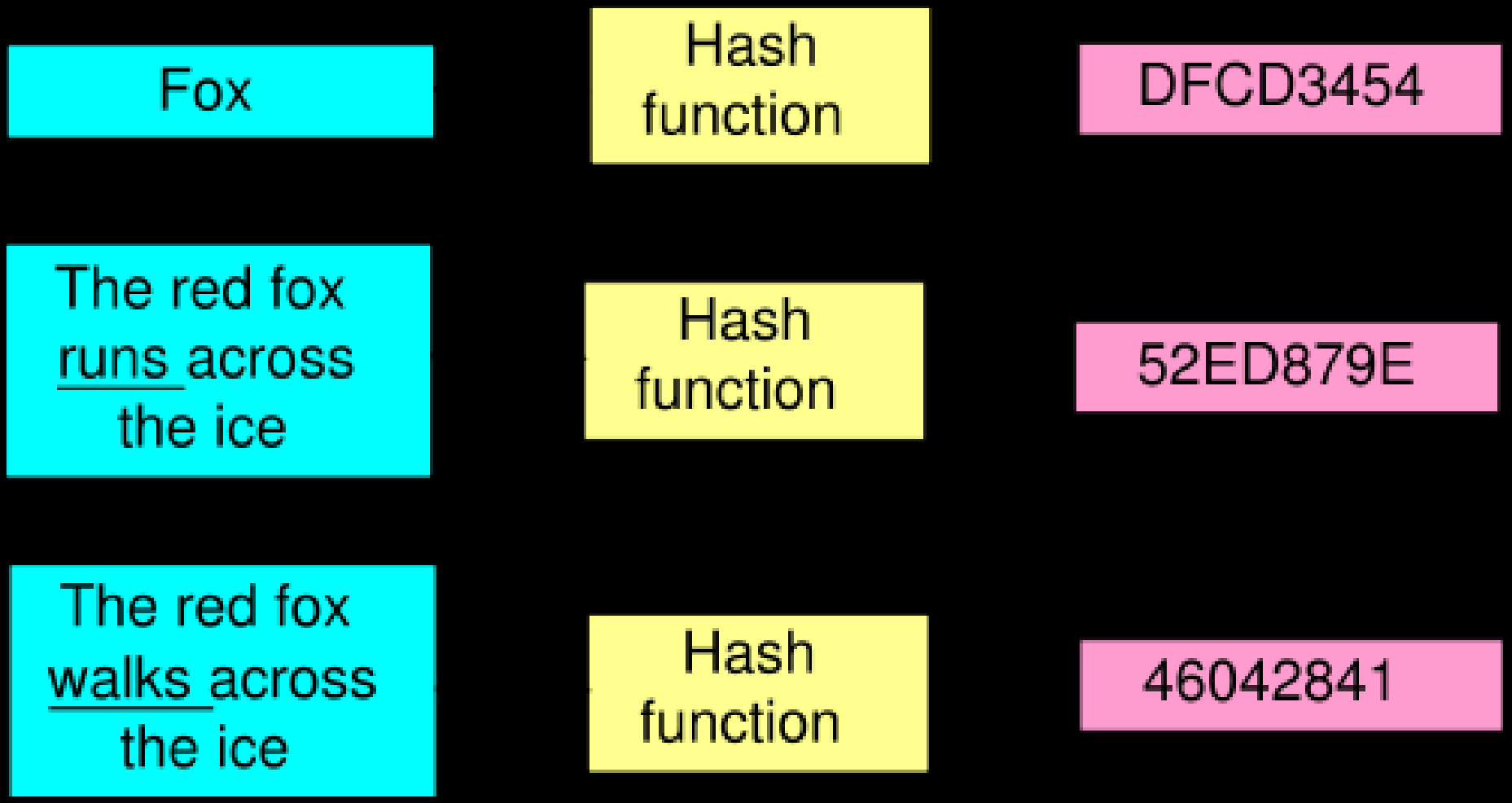
Changes made on altered image pixel 1

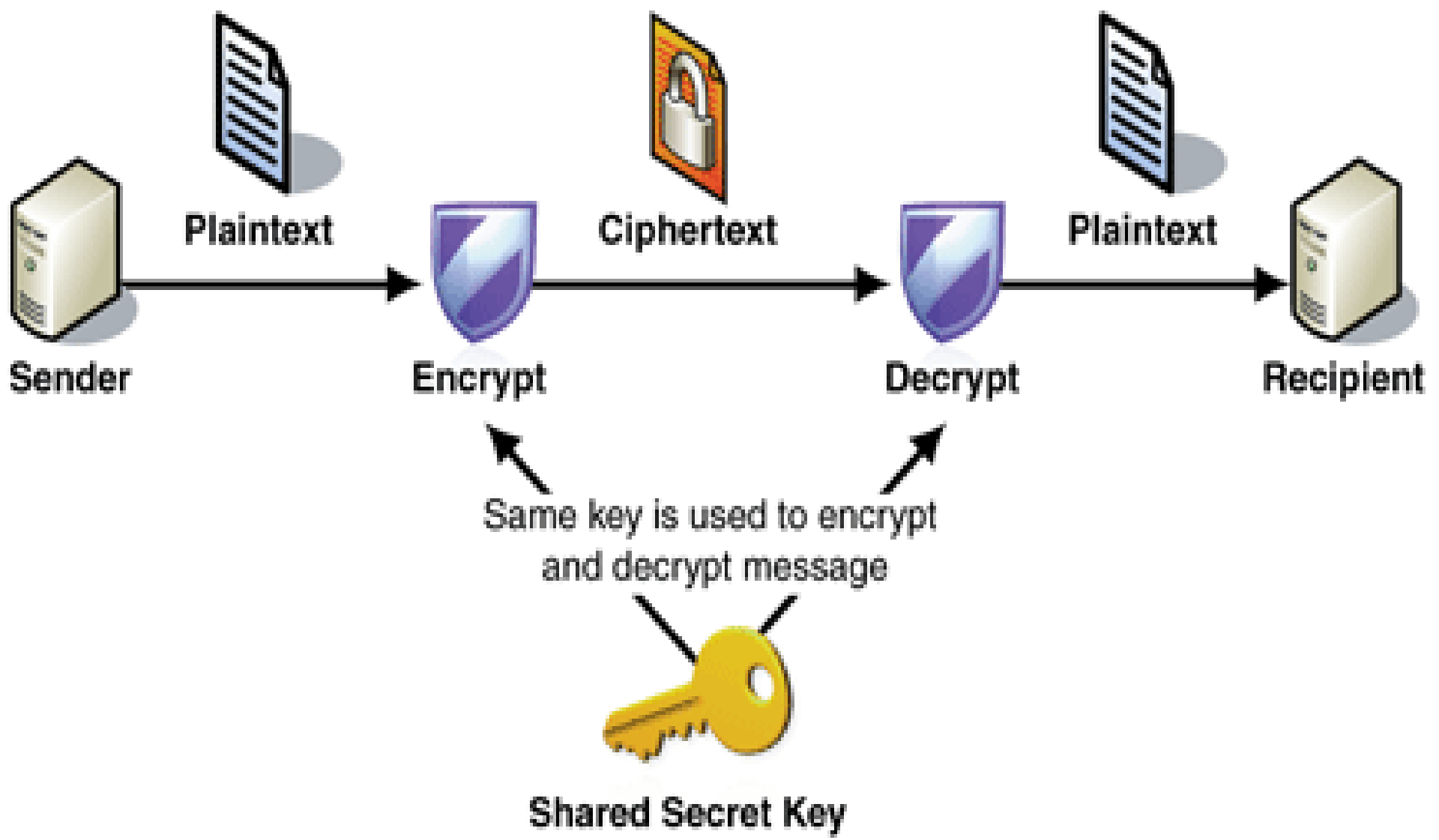
10000001 10100100 10110100 10110100 11110010 10110110 11100110 10110011 00110011

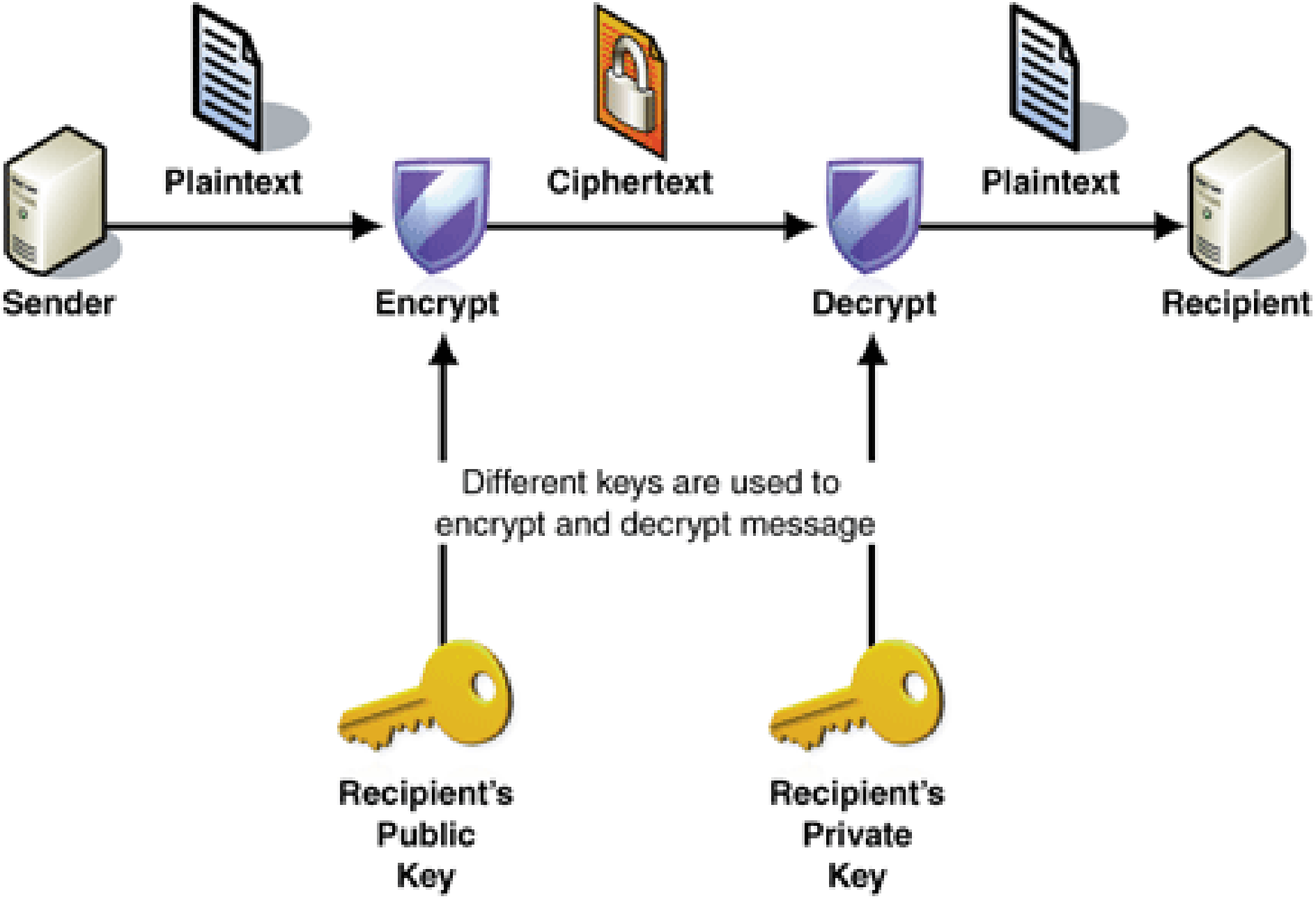
Read last digit:

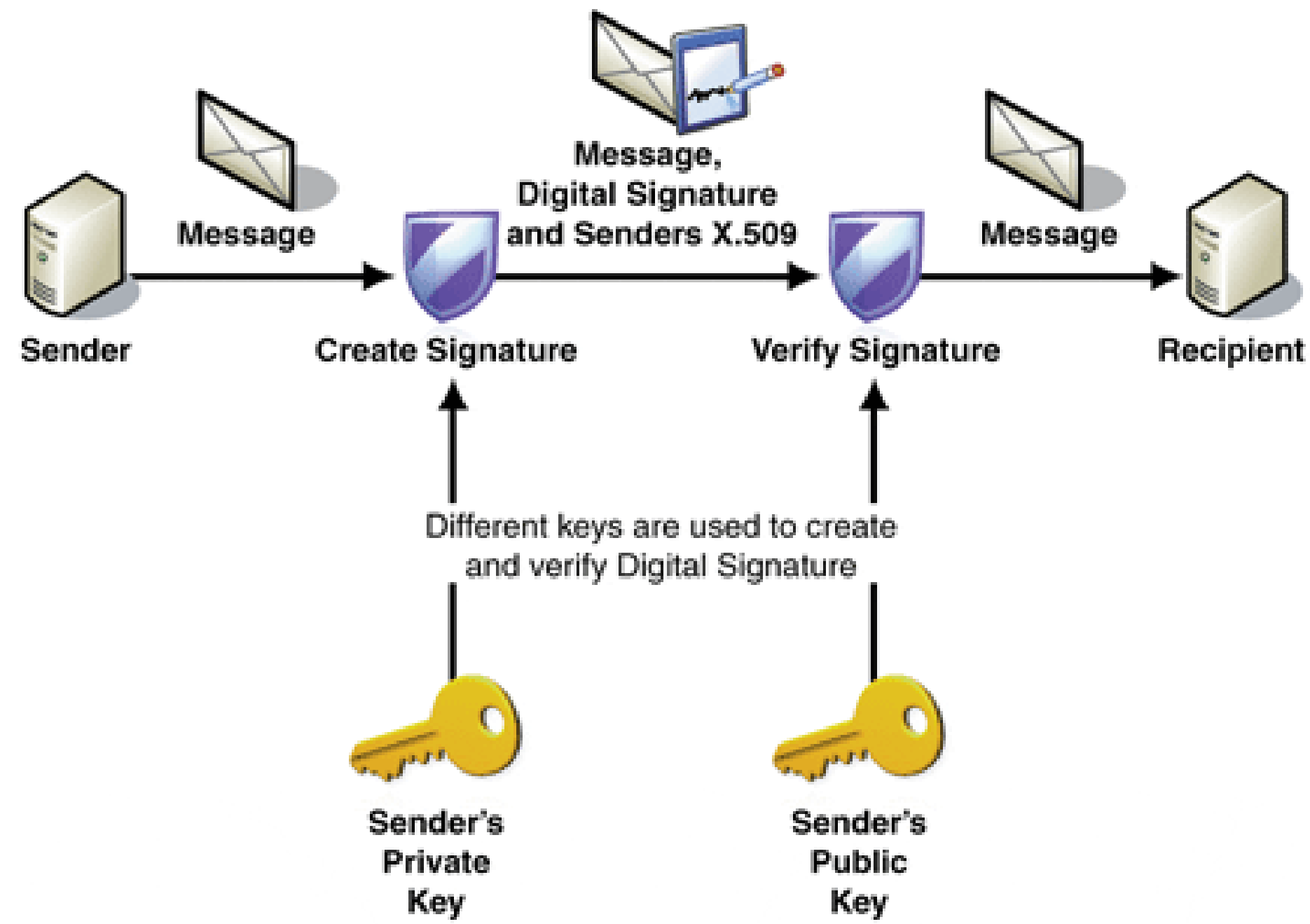
1000001 which is ASCII binary code for A

1 2 3 4


Fox
Hash function
DFCD3454
The red fox runs across the ice
Hash function
52ED879E
The red fox walks across the ice
Hash function
46042841


Plaintext
Ciphertext
Plaintext
Sender
Encrypt
Decrypt
Recipient
Same key is used to encrypt
and decrypt message
Shared Secret Key


Plaintext
Ciphertext
Plaintext
Sender
Encrypt
Decrypt
Recipient
Different keys are used to
encrypt and decrypt message
Recipient's
Public
Key
Recipient's
Private
Key

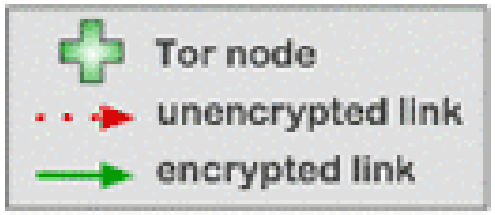

Message
Message,
Digital Signature
and Senders X.509
Message
Sender
Create Signature
Verify Signature
Recipient
Different keys are used to create
and verify Digital Signature
Sender's
Private
Key
Sender's
Public
Key

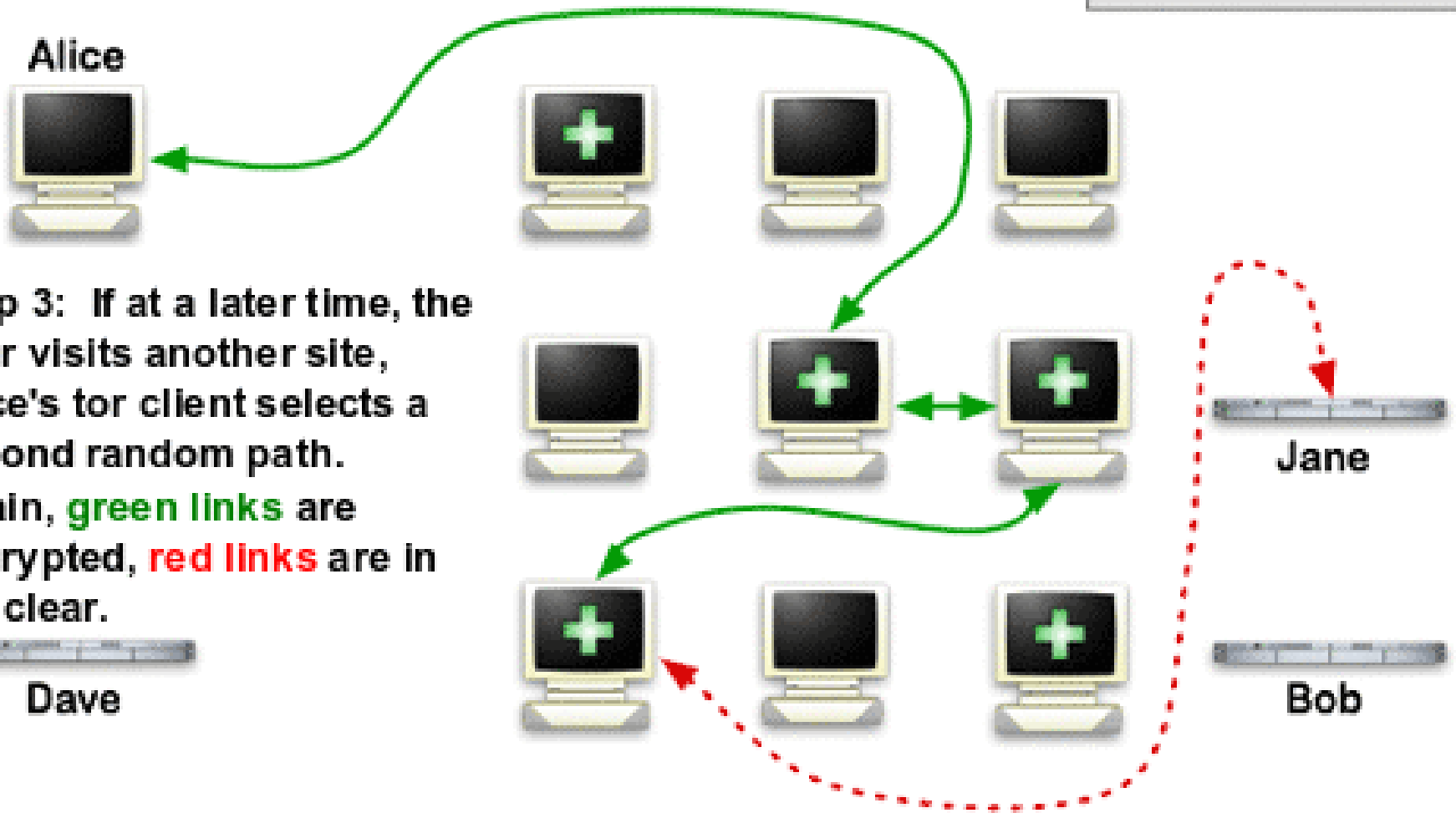
Současné využití

- všude a pořád
- digitální podpis
- bankovnictví
- komunikace

- TOR

How Tor Works: 3



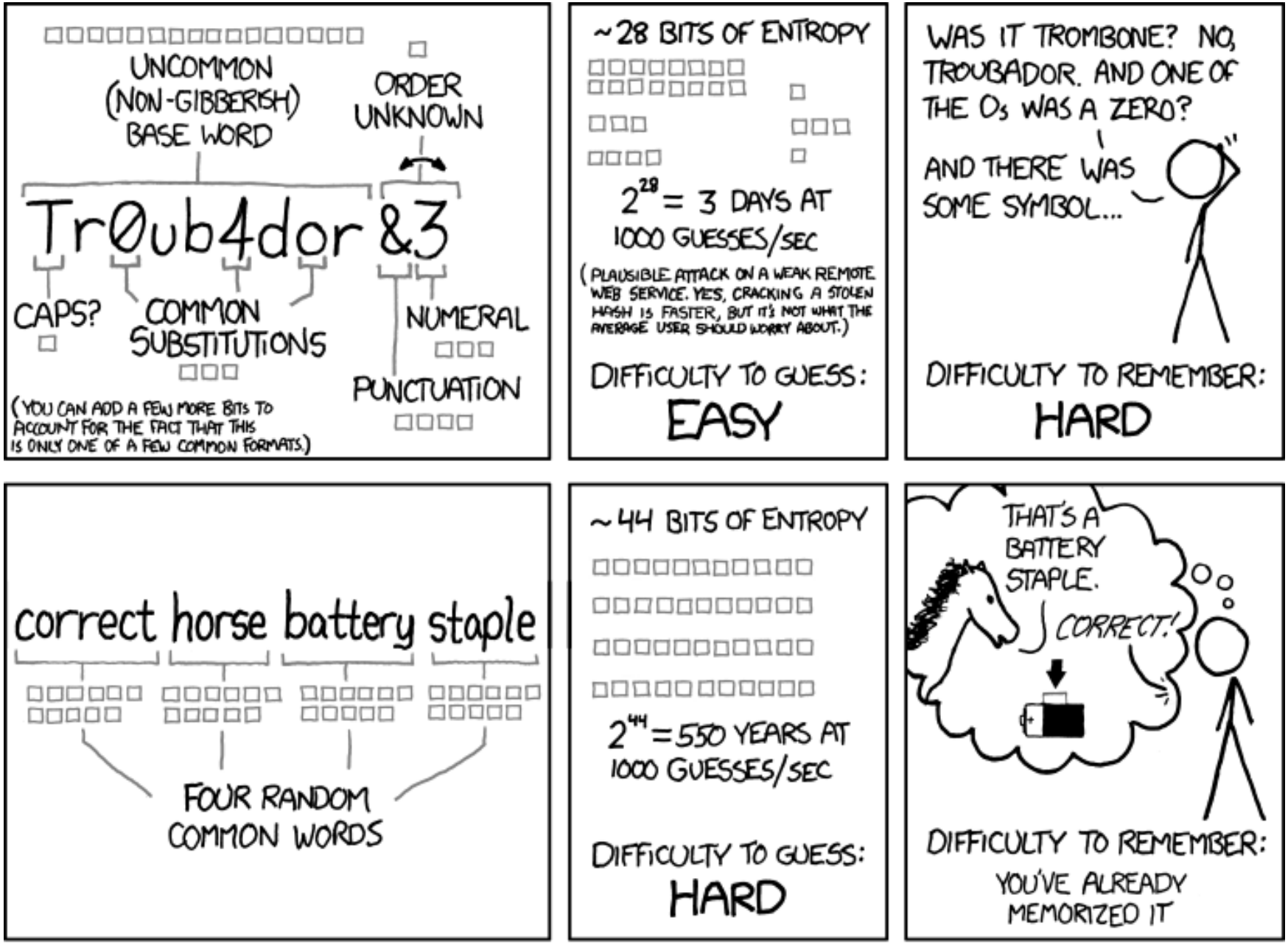


Step 3: If at a later time, the user visits another site, Alice's tor client selects a second random path.

Again, green links are encrypted, red links are in the clear.

password
123456
12345678
1234
letmein
12345
qwerty
dragon
696969
football
pussy
baseball
michael
mustang
master
monkey
jennifer
abc123
superman
111111
2000
shadow
jordan
654321
asshole
jessica
access
ranger
computer
666666
michelle
nicole
buster
george
killer
hockey
robert
orange
thomas
amanda
fucker
123123
taylor
hunter
heather
andrew
batman
charlie
yankees
daniel
maggie
sexy
william
trustno1
hello
1234567
starwars
merlin
test
ashley
corvette
pepper
austin
love
harley
hammer
123456789
sunshine
fuck
fuckyou
fuckme
joshua
matthew
1111
thunder
tigger
silver
6969
biteme
summer
ginger
pass
dallas
freedom
soccer
source: xato.net

	PIN	Freq
#1	1234	10.713%
#2	1111	6.016%
#3	0000	1.881%
#4	1212	1.197%
#5	7777	0.745%
#6	1004	0.616%
#7	2000	0.613%
#8	4444	0.526%
#9	2222	0.516%
#10	6969	0.512%
#11	9999	0.451%
#12	3333	0.419%
#13	5555	0.395%
#14	6666	0.391%
#15	1122	0.366%
#16	1313	0.304%
#17	8888	0.303%
#18	4321	0.293%
#19	2001	0.290%



THROUGH 20 YEARS OF EFFORT, WE'VE SUCCESSFULLY TRAINED EVERYONE TO USE PASSWORDS THAT ARE HARD FOR HUMANS TO REMEMBER, BUT EASY FOR COMPUTERS TO GUESS.

Možná řešení

- password managers
- password policies
  - komplexita
  - neopakování

Výpočetní síla

- stále delší klíče
- Moore's Law
- kvantové procesory?

CIA(N)

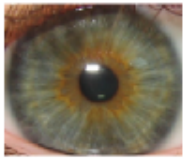
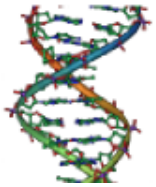
- confidentiality
- integrity
- authentication
- non-repudiation

Řízení přístupu

- identifikace, autorizace, autentizace
- co jste, znáte, máte
- biometrika
  - výhody, nevýhody
  - FAR, FRR

Biometrics

Physiological

- face 
- fingerprint 
- hand 
- iris 
- DNA 

Behavioral

- keystroke 
- signature 
- voice