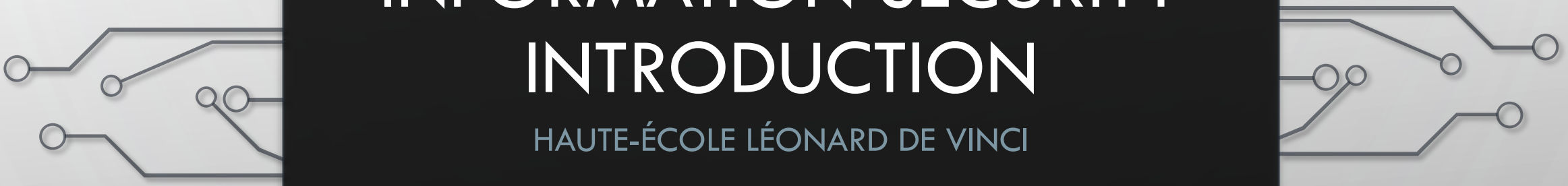


INFORMATION SECURITY INTRODUCTION

HAUTE-ÉCOLE LÉONARD DE VINCI

CHAPTER 4 – CRYPTOGRAPHY

CHAPTER 4

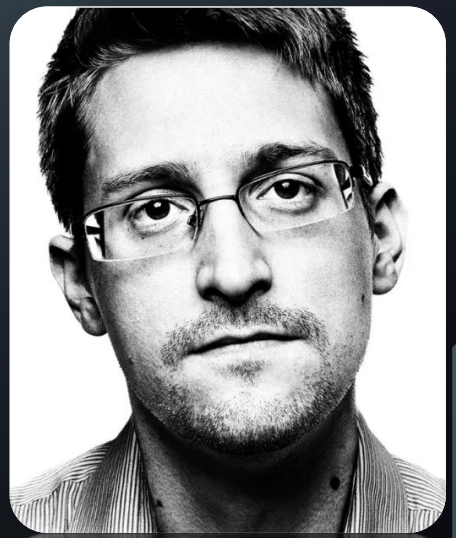
- 4.1 Definition & History
- 4.2 Cryptography Objectives
- 4.3 Steganography
- 4.4 Substitution & Poly Substitution
- 4.5 Symmetric
- 4.6 Asymmetric
- 4.7 Hashing
- 4.8 Digital Signature
- 4.9 Public Key Infrastructure
- 4.10 Post-Quantum

CHAPTER 4

- How are we able to maintain confidentiality ?
- What are the different types of encryption ?
- What is the difference between symmetric and assymetric ?
- Which type of encryption to use and when?
- What are the possible attacks ?

Encryption works. Properly implemented strong crypto systems are one of the few things that you can rely on. Unfortunately, endpoint security is so terrifically weak that NSA can frequently find ways around it.

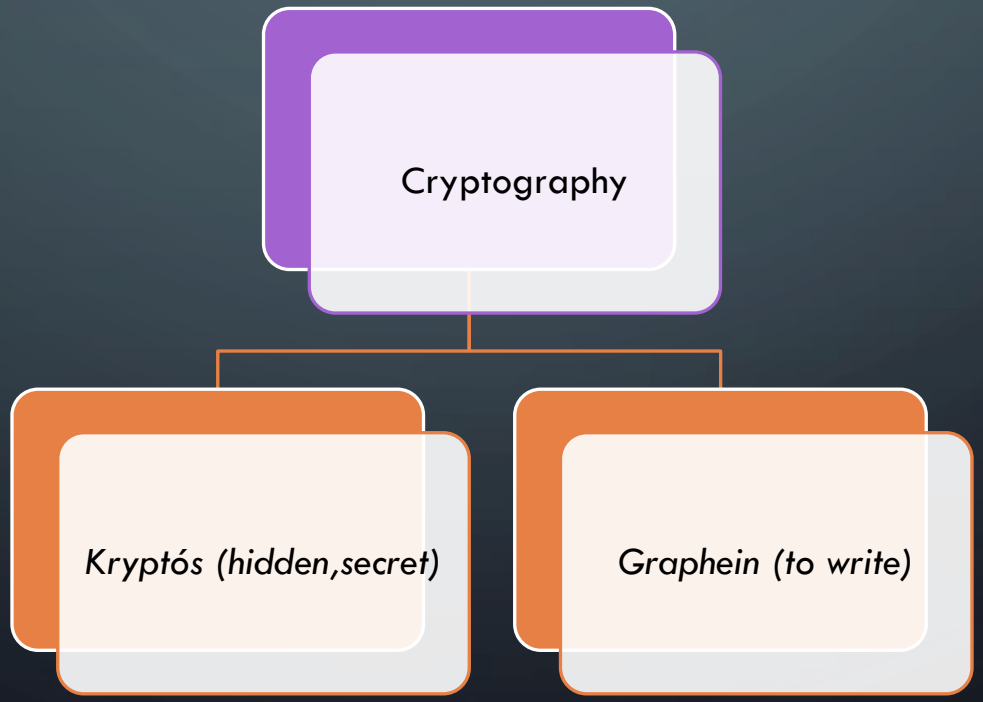
- Edward Snowden



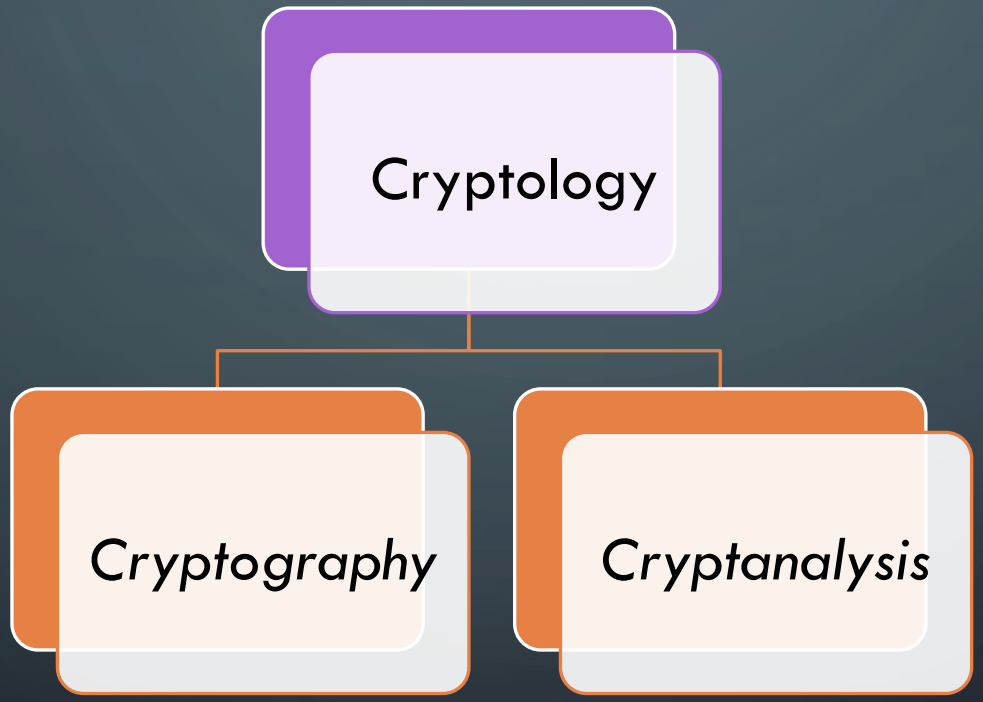
4.1 DEFINITION & HISTORY

4.1 DEFINITION

Cryptography is the practice and study of techniques of encoding information in a manner that it cannot be decoded without access to the required decryption key.



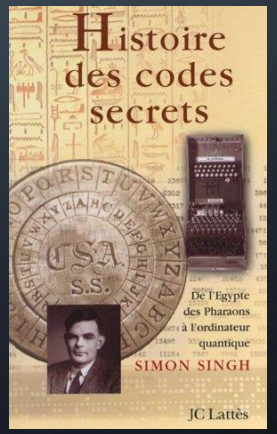
4.1 DEFINITION



4.1 HISTORY

The oldest trace of cryptography is dated back to 1.500 BC on clay tablets from Mesopotamia.

Since that date cryptography has evolved a lot in different phases and technics though millenia.



4.2 CRYPTOGRAPHY OBJECTIVES

4.2 CRYPTOGRAPHY OBJECTIVES

Nowadays, cryptography has 4 objectives to fulfill:

Confidentiality

Integrity

Authentication

Non-repudiation

Within the context of Cryptography CIA = Confidentiality, Integrity, **Authentication**

4.2 NON-REPUDIATION

Non-repudiation ensure that individuals can prove to a third party that a meessage came from its purported sender.

In other words it means:

- A way to provide proof of the integrity and origin of data
- An authentication that can be said to be genuine with high confidence

4.3 STEGANOGRAPHY

4.3 STEGANOGRAPHY

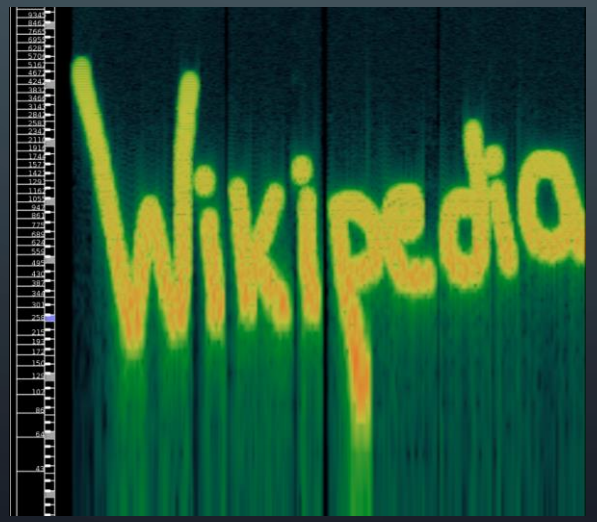
Steganography is not as per say a cryptography method. Steganography is a technique that intend to hide information within another information or a physical object.

Nabuchodonosor (Babylon King) was known to shave head of a slave. Write the message on the slave's head. Wait for the hair to grow. Send the slave to his general. The general would then shave the head again and read the King's instruction for war.

4.3 STEGANOGRAPHY

Steganography has been heavily used by spies through the ages and is still used nowadays.

It's possible to hide information within sound, images, video, binaries, documents, etc.



Encoded image within a sound and seen through a spectrogram.

4.3 STEGANOGRAPHY

cat.jpg

hidden-cat.jpg

4.3 STEGANOGRAPHY

```
$> cat hidden-cat.jpg >> cat.jpg
```

```
ExifTool Version Number         : 12.40
File Name                       : cat.jpg
Directory                       : .
File Size                       : 135 KiB
File Modification Date/Time     : 2022:08:22 09:45:36+02:00
File Access Date/Time           : 2022:08:22 09:47:21+02:00
File Inode Change Date/Time     : 2022:08:22 09:47:21+02:00
File Permissions                : -rw-r--r--
File Type                       : JPEG
File Type Extension             : jpg
MIME Type                       : image/jpeg
JFIF Version                    : 1.01
Resolution Unit                 : inches
X Resolution                    : 240
Y Resolution                    : 240
Image Width                     : 800
Image Height                    : 751
Encoding Process                : Baseline DCT, Huffman coding
Bits Per Sample                 : 8
Color Components                : 3
Y Cb Cr Sub Sampling            : YCbCr4:4:4 (1 1)
Image Size                      : 800×751
Megapixels                      : 0.601
```

```
ExifTool Version Number         : 12.40
File Name                       : cat.jpg
Directory                       : .
File Size                       : 281 KiB
File Modification Date/Time     : 2022:08:22 09:48:26+02:00
File Access Date/Time           : 2022:08:22 09:48:26+02:00
File Inode Change Date/Time     : 2022:08:22 09:48:26+02:00
File Permissions                : -rw-r--r--
File Type                       : JPEG
File Type Extension             : jpg
MIME Type                       : image/jpeg
JFIF Version                    : 1.01
Resolution Unit                 : inches
X Resolution                    : 240
Y Resolution                    : 240
Image Width                     : 800
Image Height                    : 751
Encoding Process                : Baseline DCT, Huffman coding
Bits Per Sample                 : 8
Color Components                : 3
Y Cb Cr Sub Sampling            : YCbCr4:4:4 (1 1)
Image Size                      : 800×751
Megapixels                      : 0.601
```

4.3 STEGANOGRAPHY

To retrieve the image within the image it's possible to use the tools

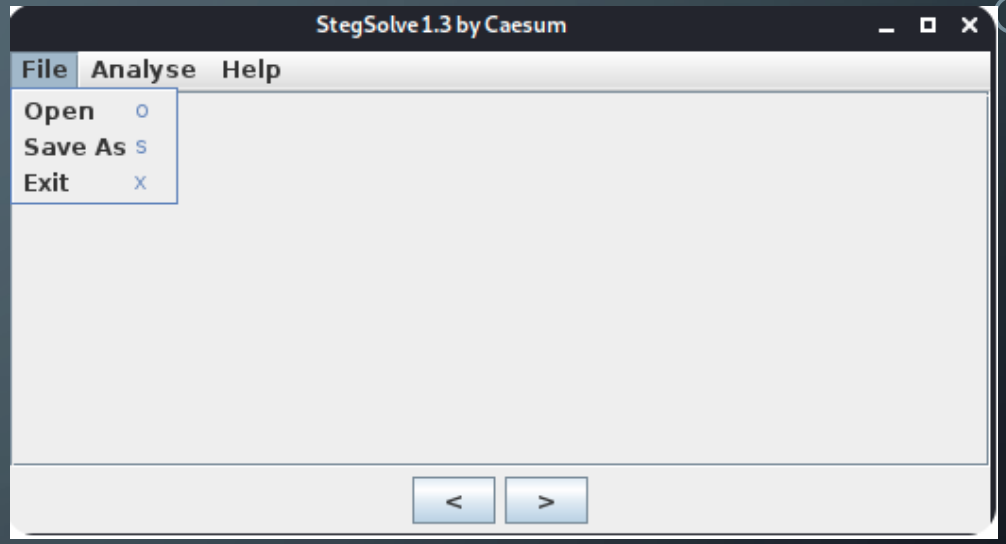
- foremost
- stegsolve

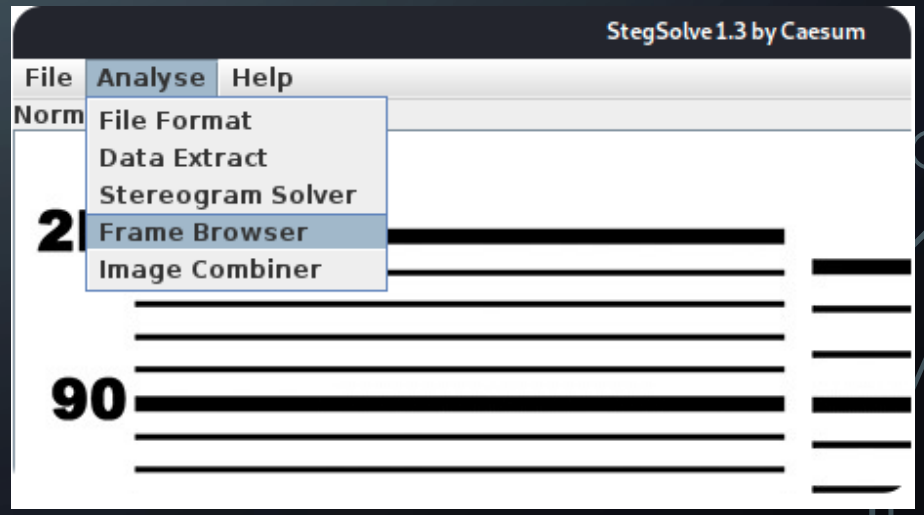
4.3 STEGANOGRAPHY

```
user@kali $> foremost -t jpg -i cat-photo-id.jpg -v
Foremost version 1.5.7 by Jesse Kornblum, Kris Kendall, and Nick Mikus
Audit File

Invocation: foremost -t jpg -i cat-photo-id.jpg -v
Output directory: /home/user/Documents/SANS CTF/FM02/output
Configuration file: /etc/foremost.conf
Processing: cat-photo-id.jpg
|------------------------------------------------------------------
File: cat-photo-id.jpg
Start: Mon Nov 15 20:29:46 2021
Length: 281 KB (287750 bytes)

Num      Name (bs=512)         Size      File Offset     Comment
```





DEMO

4.4 SUBSTITUTION & POLY SUBSTITUTION

4.4 CIPHER

A *cipher* is a method used to scramble or obfuscate characters to hide their value.

Ciphering is the process of using a cipher to do that type of scrambling to a message.

4.4 SUBSTITUTION

A *substitution cipher* is a type of coding or cipheering system that changes one character or symbol into another.

Character substitution can be a relatively easy method of encrypting information. One of the oldest known substitution cipher is called the C*aesar cipher*.

It was used by Julius Caesar. The system involves simply shifting all letters a certain number of spaces in the alphabet.

4.4 CAESAR CIPHER

Let's apply it concretely.

Caesar cipher +3 = Replace letters by the third letter to the right of the original letter.

```
ABCDEFGHIJKLMNOPQRSTUVWXYZ
DEFGHIJKLMNOPQRSTUVWXYZABC
```

I LOVE SECURITY => L ORYH VHFXULWB

4.4 CAESAR CIPHER

In order to decrypt the message you simply perform the opposite operation.

The Caesar cipher is a very simple example of substitution cipher.

Today this cipher is far too easy to be used as any cryptologist could break these ciphers or any similar substitution, in a matter of seconds.

Nevertheless the substitution operation method is the foundation of many modern encryption algorithms. They just perform far more sophisticated substitutions.

4.4 POLY SUBSTITUTION

One problem with the substitution cipher is that it gives a low number of trial before being broken and it does not change the frequency of word or letter in the text.

In 1586, Blaise de Vigenère invented the *Vigenere cipher*, a poly substitution cipher.

4.4 VIGENERE CIPHER

Vigenere idea is simple.

Instead of shiffting letter by a certain amount, we will shift the letter based on a cipher table. The key of this cipher will be a word that both party will have agreed upon.

4.4 VIGENERE CIPHER

	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z
A	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z
B	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A
C	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B
D	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C
E	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D
F	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E
G	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F
H	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G
I	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H
J	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I
K	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J
L	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K
M	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L
N	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M
O	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N
P	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O
Q	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P
R	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q
S	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R
T	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S
U	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T
V	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U
W	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V
X	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W
Y	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X
Z	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y

Vigenère cipher table

Using the Vigenère table, let's encrypt "SECRET MESSAGE" with the keyword "APPLE"

4.4 VIGENERE CIPHER

	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z
A	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z
B	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A
C	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B
D	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C
E	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D
F	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E
G	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F
H	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G
I	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H
J	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I
K	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J
L	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K
M	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L
N	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M
O	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N
P	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O
Q	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P
R	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q
S	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R
T	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S
U	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T
V	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U
W	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V
X	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W
Y	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X
Z	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y

S E C R E T M E S S A G E

A P P L E A P P L E A P P

S T R C I T B T D E A V T

4.4 VIGENERE CIPHER

To decrypt the message you simply perform the opposite action.

4.4 ATTACKS ON SUBSTITUTION & POLY SUBSTITUTION

Around 800, *Ibn Ishaq al-Kindi*, mathematician, philosopher, physician, chemist, astronomer... Write the first cryptanalysis treaty !

He invented nothing else than the concept of *frequency analysis*.

This fantastic discovery will be used to decrypt messages until... World War II

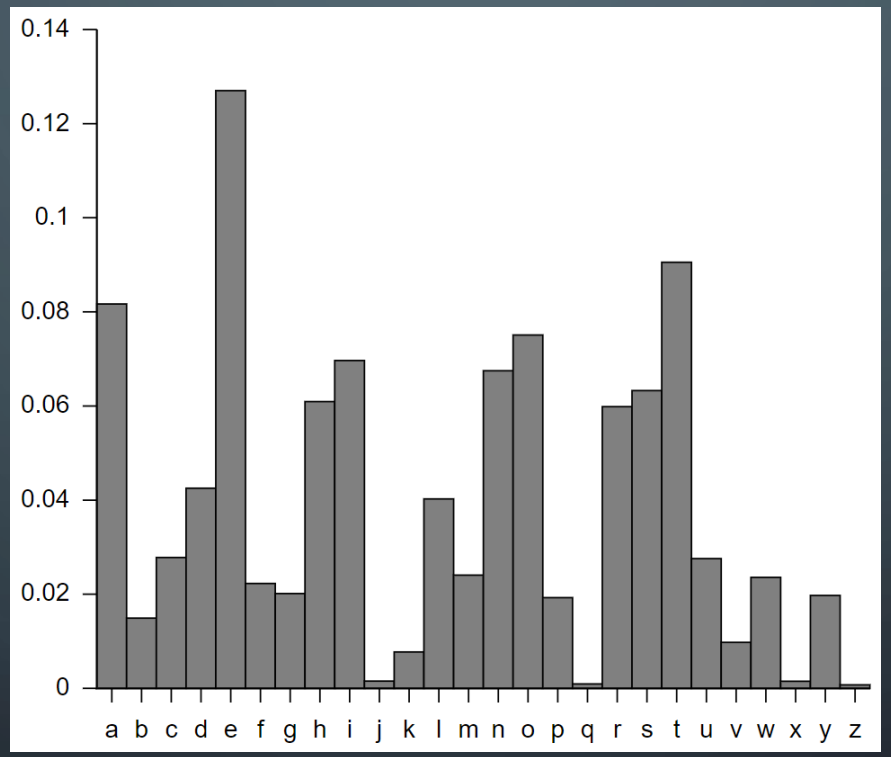
4.4 FREQUENCY ANALYSIS

Frequency analysis is the study of frequency of letters or groups of letter in a ciphertext.

This concept is based on the fact that, in any given stretch of written language certain letters and combinations of letters occur with varying frequencies.

Even better than that! Each language has its own letter frequency.

4.4 FREQUENCY ANALYSIS



The letter repartition in the English language.

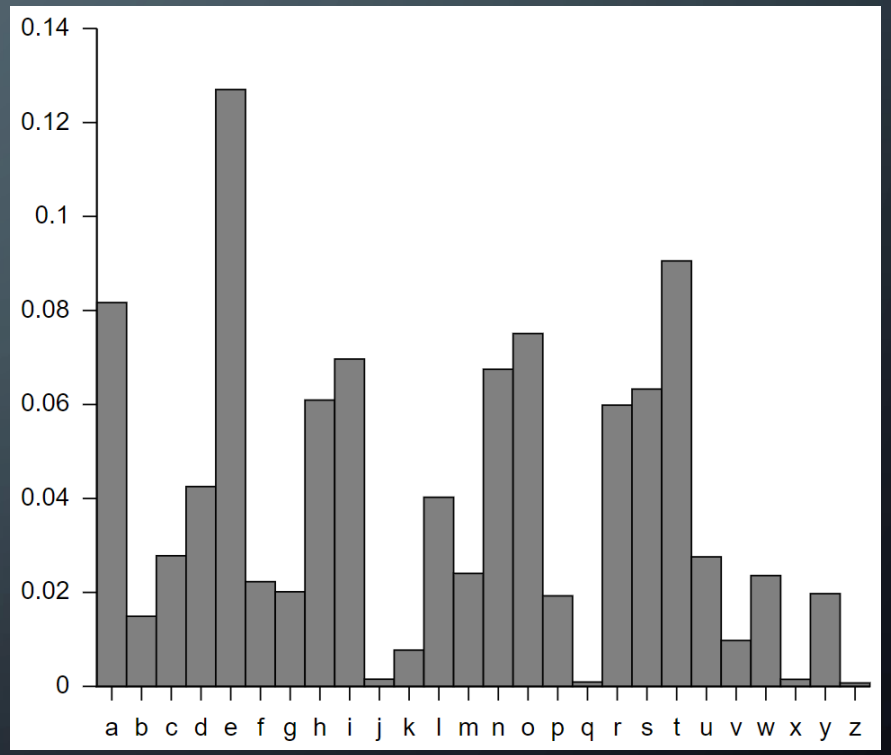
4.4 FREQUENCY ANALYSIS

JG ZPV EPO'U GBJM, ZPV'SF OPU FWFO USZJOH. J'MM TBZ JU BHBJO. JG ZPV EPO'U GBJM, ZPV'SF OPU FWFO USZJOH. NZ XJGF UPME NF UIJT HSFBU FYQSFTTJPO. UP HFU TPNFUIJOH ZPV OFWFS IBE, ZPV IBWF UP EP TPNFUIJOH ZPV OFWFS EJE. MFT CSPXO'T B NPUJWBUJPOBM TQFBLFS. IF NBEF BO BOBMPHZ BCPVU UIJT. IF TBZT, "JNBHJOF ZPV'SF PO ZPVS EFBUICFE, BOE TUBOEJOH BSPVOE ZPVS EFBUICFE BSF UIF HIPTUT SFQSFTFOUJOH ZPVS VOGVMGJMMFE QPUFOUJBM, UIF HIPTU PG UIF JEFBT ZPV OFWFS BDUFE PO, UIF HIPTU PG UIF UBMFOUT ZPV EJEO'U VTF. BOE UIFZ'SF TUBOEJOH BSPVOE ZPVS CFE, BOHSZ, EJTBQQPJOUFE, BOE VQTFU. UIFZ TBZ, 'XF DBNF UP ZPV CFDBVTF ZPV DPVME IBWF CSPVHIU VT UP MJGF,' UIFZ TBZ. 'BOE OPX XF IBWF UP HP UP UIF HSBWF UPHFUIFS.'"

F=67	E=29
P=52	T=28
U=51	Z=28
B=43	V=27
O=41	S=26
J=30	H=20

4.4 FREQUENCY ANALYSIS

F=67	E=29
P=52	T=28
U=51	Z=28
B=43	V=27
O=41	S=26
J=30	H=20



We know that in English, the most represented letter is the "e".

As it is a statistical approach it's possible that the most represented letter in our text is not "e" but "o" for example.

What we can be nearly sure is that the "e" will be one of the most represented letter, maybe the first, maybe the second.

4.4 FREQUENCY ANALYSIS

Let's try and do F = e, P = o and U = t :

JG ZoV EoO’t GBJM, ZoV’Se Oot eWeO tSZJOH. J’MM TBZ Jt BHBJO. JG ZoV EoO’t GBJM, ZoV’Se Oot eWeO tSZJOH. NZ XJGe toME Ne tIJT HSeBt eYQSeTTJoO. to Het ToNetIJOH ZoV OeWeS IBE, ZoV IBWe to Eo ToNetIJOH ZoV OeWeS EJE. MeT CSoXO’T B NotJWBtJoOBM TQeBLeS. Ie NBEe BO BOBMoHZ BCoVt tIJT. Ie TBZT, “JNBHJOe ZoV’Se oO ZoVS EeBtICeE, BOE TtBOEJOH BSoVOE ZoVS EeBtICeE BSe tLe HIoTtT SeQSeTeOtJOH ZoVS VOGVMGJMMeE QoteOtJBM, tLe HIoTt oG tLe JEeBT ZoV OeWeS BDteE oO, tLe HIoTt oG tLe tBMeOtT ZoV EJEO’t VTe. BOE tLeZ’Se TtBOEJOH BSoVOE ZoVS CeE, BOHSZ, EJTBQQoJOteE, BOE VQTet. tLeZ TBZ, ‘Xe DBNe to ZoV CeDBVTe ZoV DoVME IBWe CSoVHIt VT to MJGe,’ tLeZ TBZ. ‘BOE OoX Xe IBWe to Ho to tLe HSBWe toHetLeS.'”

EoO’t = don't ? / to Ho to = to go to ? / tIe = the ? / tleZ = they ?

4.4 FREQUENCY ANALYSIS

EoO’t = don't ? / to Ho to = to go to ? / tLe = the ? / tLeZ = they ?

Let's try with E = d, O=n, H=g, I=h and Z=y

JG yoV don’t GBJM, yoV’Se not eWen tSyJng. J’MM TBy Jt BgBJn. JG yoV don’t GBJM, yoV’Se not eWen tSyJng. Ny XJGe toMd Ne thJT gSeBt eYQSeTTJon. to get ToNethJng yoV neWeS hBd, yoV hBWe to do ToNethJng yoV neWeS dJd. MeT CSoXn’T B NotJWBtJonBM TQeBLeS. he NBde Bn BnBMogy BCoVt thJT. he TByT, “JNBgJne yoV’Se on yoVS deBthCed, Bnd TtBndJng BSoVnd yoVS deBthCed BSe the ghoTtT SeQSeTentJng yoVS VnGVMGJMMed QotentJBM, the ghoTt oG the JdeBT yoV neWeS BDted on, the ghoTt oG the tBMentT yoV dJdn’t VTe. Bnd they’Se TtBndJng BSoVnd yoVS Ced, BngSy, dJTBQQoJnted, Bnd VQTet. they TBy, ‘Xe DBNe to yoV CeDBVTe yoV DoVMd hBWe CSoVght VT to MJGe,’ they TBy. ‘Bnd noX Xe hBWe to go to the gSBWe togetheS.'”

yoV = you / togetheS = together /yoV'Se = you're

4.4 FREQUENCY ANALYSIS

Then we replace V = u, S = r and so on and so on...

Each cycle making the reading and replacement easier.

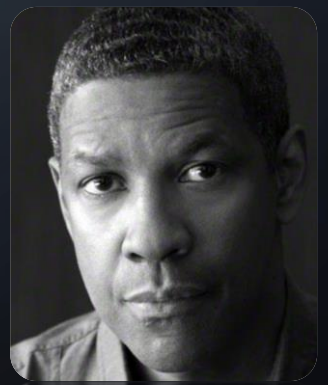
We discover the following text...

4.4 FREQUENCY ANALYSIS

If you don't fail, you're not even trying. I'll say it again. If you don't fail, you're not even trying. My wife told me this great expression. To get something you never had, you have to do something you never did. Les Brown's, a motivational speaker. He made an analogy about this. He says, "Imagine you're on your deathbed, and standing around your deathbed are the ghosts representing your unfulfilled potential, the ghost of the ideas you never acted on, the ghost of the talents you didn't use. And they're standing around your bed, angry, disappointed, and upset. They say, 'We came to you because you could have brought us to life', they say. 'And now we have to go to the grave together.'"

- Denzel Washington

"Fall forward" - University of Pennsylvania – 2010



Does perfect encryption exist ?

Can we encrypt a text in a way that it cannot be cracked ?

Well ...

YES !

… but with extremely difficult conditions to met !

4.4 ONE-TIME PAD

Such encryption technique is named *one-time pad*.

The conditions to met are the following:

1. The key MUST be as long as the text
2. The key MUST be random (real random not pseudo-random)
3. The key MUST never be reused
4. The key MUST remain completely secret by the communicating parties


4.5 SYMMETRIC

4.5 SYMMETRIC KEY ALGORITHM

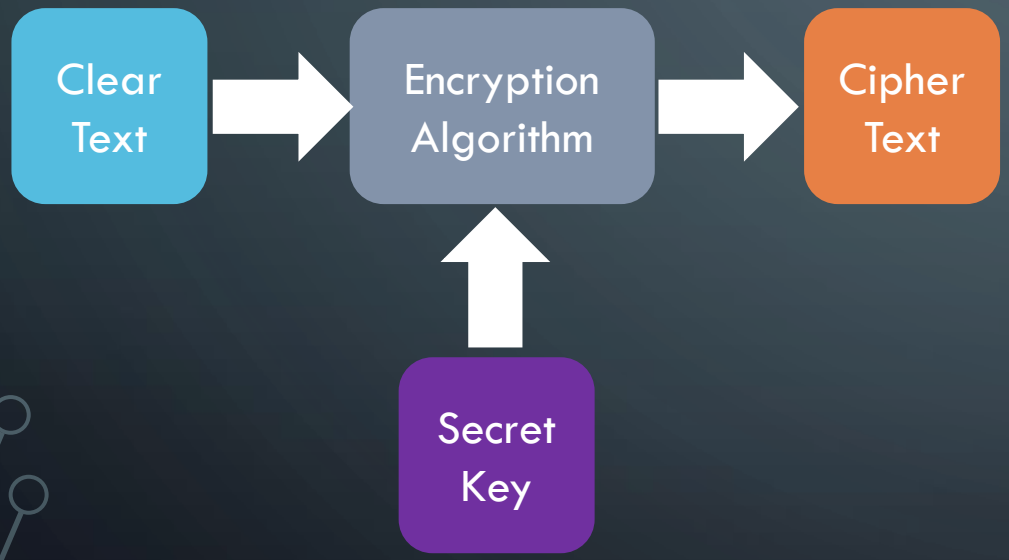
Symmetric key algorithm rely on a shared secret encryption key that is distributed to all members who participate in the communication. This key is used to both encrypt and decrypt messages.

When large-sized keys are used, symmetric encryption is very difficult to break!

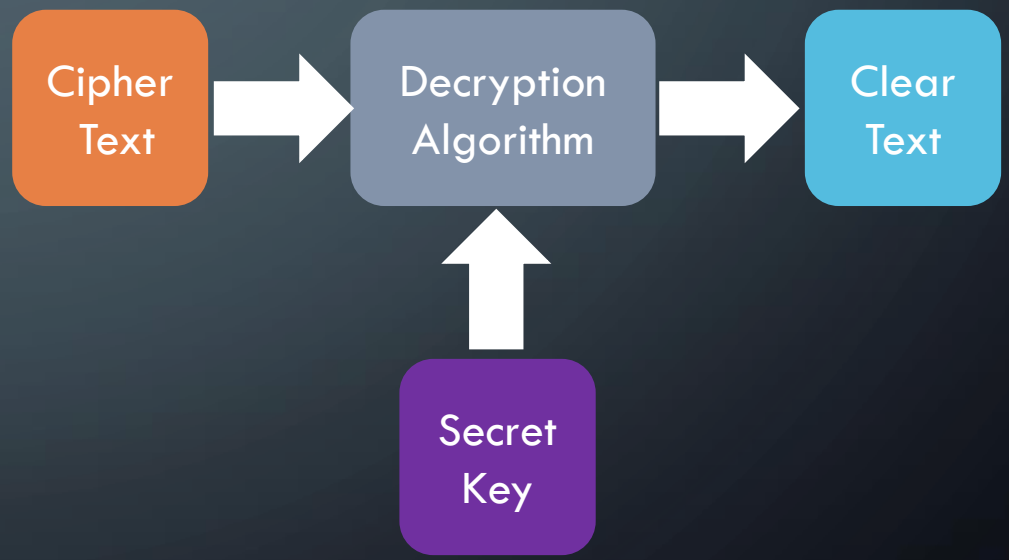
Symmetric encryption is primarily used to perform bulk encryption because it's fast !

4.5 SYMMETRIC KEY ALGORITHM

Symmetric Encryption



Symmetric Decryption



4.5 SYMMETRIC STRENGTH

The major strength of symmetric key cryptography is the great speed at which it can operate. It's really fast, often 1.000 to 10.000 times faster than assymetric algorithms.

Additionaly, due to the mathematical nature of symmetric key cryptography, it's possible to create dedicated hardware for encryption. Which makes it even faster! (15GB/s on an i7-12700k)

4.5 SYMMETRIC WEAKNESSES

Key distribution

- Parties must have a secure method of exchanging the secret key before establishing communications. An offline key distribution method must often be used. Out-of-band.

No implementation of nonrepudiation

- Because everyone use the same key, there is no way to prove the origin of the message.

No scalability

- It is extremely difficult for large groups to communicate using symmetric key cryptography. You have as many key as you have person to communicate with.

Key regeneration

- Each time a participant leaves the group, all keys known by the participant must be discarded.

4.5 SYMMETRIC KEY ALGORITHM

Here is a list of some very well known symmetric key algorithm:

To use	To Avoid
• AES • Twofish • Serpent • Camellia	• DES • 3DES • Blowfish

Nothing stops you to *combine* symmetric key algorithms to get an even stronger encryption mechanism !

```
AES( Twofish( Serpent( MySecretMessage) ) )
```

4.5 AES

Why is AES so good ?

Because it's 100% BELGIAN Invented @KU Leuven!

Because by mathematical design AES is build to withstand differential and linear cryptanalyses (that means no frequency analysis).

The only way to break it is through mathematics.

That's no good news. Because it's mathematically extremely difficult to solve quadratic equation system that has lots of complex unknowns and it's exactly what AES is creating, a massive quadratic equation system.

The best known mathematic theorical attack on AES-256 requires 2^254.4 operations = 3.81e76

The estimated number of atoms in the universe is 10e80. Not so bad...

4.6 ASYMMETRIC

4.6 ASYMMETRIC

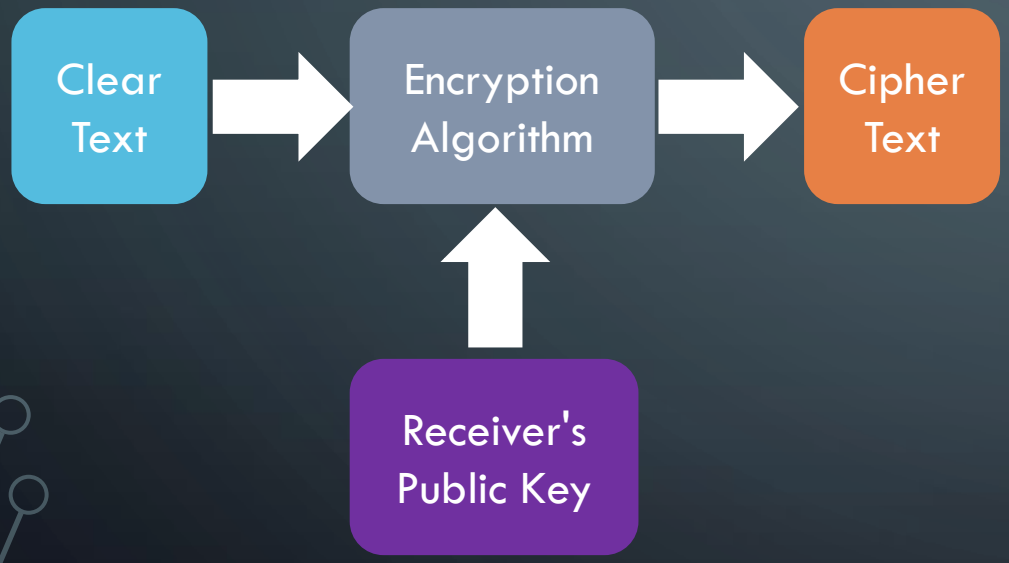
Asymmetric key algorithm, also known as public key algorithm, provide a solution to the weakness of symmetric key encryption.

In these system, each user has **two** keys. A public key that you can share with absolutely anyone. A private key which only you possess.

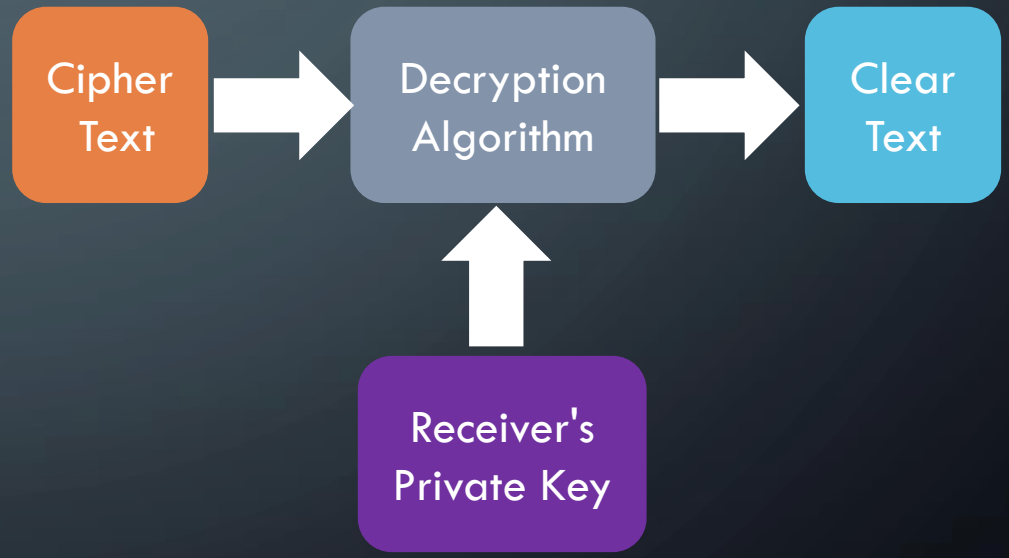
But the specificity is the following: Anybody can encrypt a message with your public key but only your private key can decrypt it (and the opposite!).

4.6 ASYMMETRIC

Symmetric Encryption



Symmetric Decryption



4.6 ASYMMETRIC STRENGTH

Scalability

- The addition of a new user only requires the generation of one public-private key pair.

User management

- Asymmetric cryptosystems provide a key revocation mechanism that allows a key to be canceled, effectively removing a user from the system.

Key management

- Key regeneration is only required when a user's private key is compromised.

Integrity, Authentication and nonrepudiation

- If the private key is not compromised, a message signed by that user can be shown to be acccurate and from a specific source and cannot be later repudiated.

Key distribution

- It's simple! You just make your public key available to anyone you want to communicate with.

No preexisting link required

- Two persons can begin communicating securely from the start of their communication session. No need to transmit a secret key. In-band.

4.6 ASYMMETRIC STRENGTH

Scalability in numbers:

Number of participants	# of symmetric key required	# of assymetric key required
2	1	4
3	3	6
4	6	8
5	10	10
10	45	20
100	4.950	200
1.000	499.500	2.000
10.000	49.995.000	20.000

Symmetric = n*(n-1)/2

Asymmetric = n*2

4.6 ASYMMETRIC STRENGTH

Here is a list of some very well known symmetric key algorithm:

To use	To Avoid
• ED25519 • Diffie-Hellman (2048 bits) • RSA (2048 bits)	• Small size keys below or equal to 1024 bits

4.7 ASYMMETRIC

The mathematical concept behind asymmetric encryption is that it's mathematicaly extremely difficult to solve

$$N = P \times Q$$

With N being a prime number, finding P and Q is extremely difficult when N is big (more than 100 digits).

RSA-2048 is using a prime number of 617 digits.

4.6 SYMMETRIC VS ASYMMETRIC

Symmetric

- Single shared key
- Out-of-band exchange
- Not scalable
- Fast
- Bulk encryption
- Confidentiality, Integrity

Asymmetric

- Key pair set
- In-band exchange
- Scalable
- Slow
- Small blocks of data, signatures, certificate
- Confidentiality, integrity, authentication, nonrepudiation

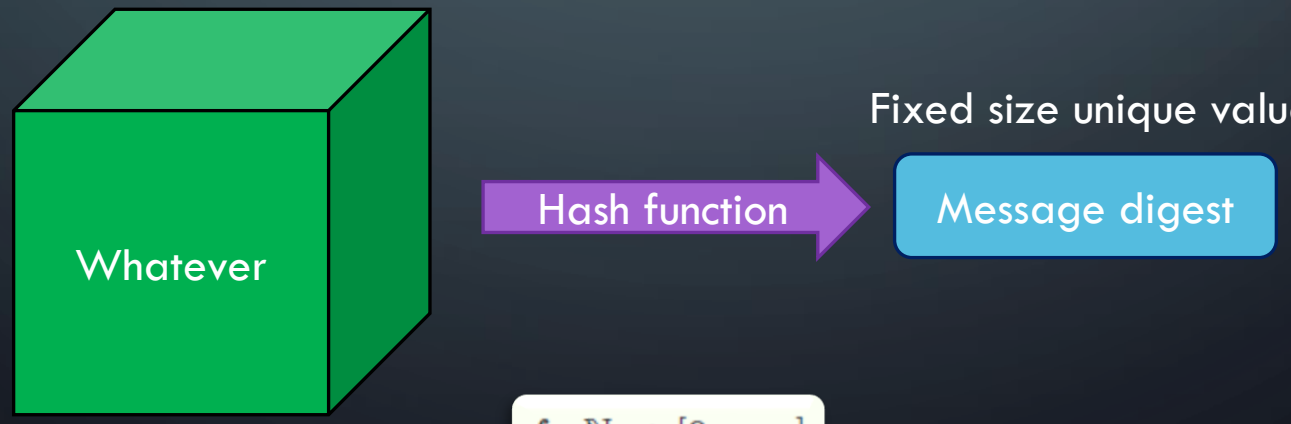

IF YOU SECURE EVERYTHING WITH A
KEY, HOW ARE YOU GOING TO PROTECT THE KEY?
WITH ANOTHER KEY


4.7 HASHING

4.7 HASHING

Hash functions have a very simple purpose: they take a long message and generate a unique output value derived from the message content. The result of this operation is named *message digest*.

The smallest difference in the message will generate a different message digest.



$$f : \mathbb{N} \rightarrow [0 \,..\, m]$$

4.7 HASHING

There are five basic requirements for a cryptographic hash function:

- Input of any length size
- Fixed length output
- Easy to compute
- Hash is ONE way
- Collision free

4.7 HASHING

Hash is ONE way: It is *extremely* difficult to determine the input when provided with the message digest.

Collision free: It is *extremely* hard to find two messages that produce the same hash value.

4.7 HASHING

Famously known hashing functions:

To use	To Avoid
• SHA-256/512 • Whirlpool	• SHA-1 • MD5

4.7 HASHING USAGE

Hashing is used when you download a file to ensure that the file you have download is really the file you are expecting.

Hashing is used for *Digital Signatures* which is the foundation of nonrepudiation of the whole internet and the Public Key Infrastructure.

4.7 ATTACKS ON HASH WITH

4.8 DIGITAL SIGNATURE

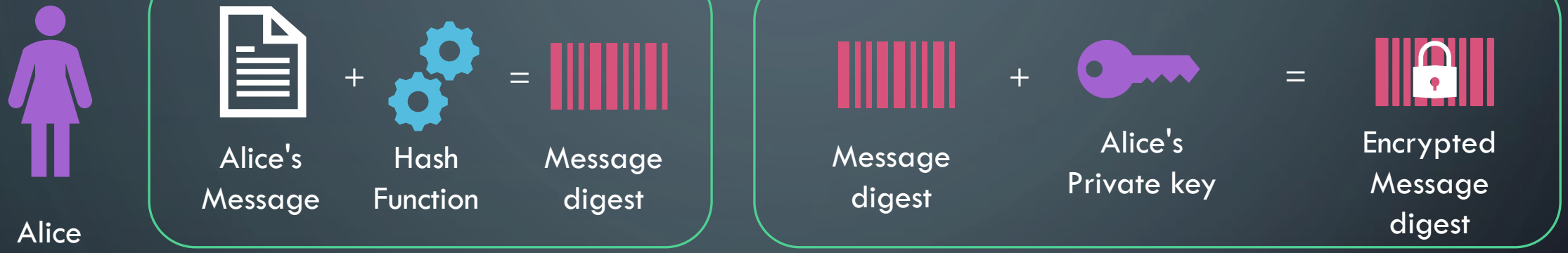
4.8 DIGITAL SIGNATURE

Digital signature rely on the combination of two major concepts we have seen in this chapter: *public key cryptography* and *hashing* functions.

1. A digitally signed message assure the recipient that the message truly come from the claimed sender. (Nonrepudiation)
2. A digitally signed message assure the recipient that the message was not altered while in transit between the sender and recipient. (Integrity)

How does digital signature works?

4.8 DIGITAL SIGNATURE



1- Create a Message Digest

2- Encrypt the message digest with private key

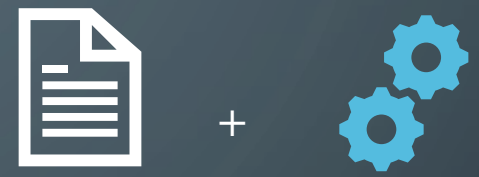
3- Send message **AND** the Encrypted message digest to Bob

4.8 DIGITAL SIGNATURE

Bob

Encryped Message digest | Alice's Public key | Message digest

1- Bob decrypts message digest



Alice's Message | Hash Function | Message Digest

2- Bob compute hash of Alice's message

Message digest | Message digest

Alice really sent me a message! \o/

3- Compare decrypted message digest with computed message digest

4.8 DIGITAL SIGNATURE

Digital signature are used for more than Alice and Bob exchanging messages.

Software vendors often used digital signature technology to authenticate code distributions that you download from the internet, such as applets and software patches.

Digital signature DOES NOT provide any privacy. It only ensures integrity, authentication and nonrepudiation! NOT confidentiality.

4.9 PUBLIC KEY INFRASTRUCTURE

4.9 PUBLIC KEY INFRASTRUCTURE

The major strength of public key infrastructure is its ability to facilitate communication between parties previously unknown to each other.

This ability is due to a fundamental concept: Trust Relationship

The trust relationship is a combination of asymmetric, symmetric, hash and digital certificates!

We will focus on the role of certificate authorities, digital certificate and certificate lifecycle.

4.9 CERTIFICATE AUTHORITIES

Certificate authorities (CAs) are the glue that binds the public key infrastructure together.

They are neutral organizations that offer notarization (agissent comme un notaire) for digital certificates.

To obtain a digital certificate you must prove your identity to the CA.

You can see this mechanism as in real life! You do not prove your own identity. It's your identity card provided by your country that prove your identity.

Because the ID card is extremely difficult to forge and you trust the emitting country. You conclude that the person is who she claims to be.

4.9 CERTIFICATE AUTHORITIES

A Certification Authoriy is as good as the trust you place in it!

It's all based on trust. I fyou don't trust the CA, then you shouldn't put any trust in their certificate.

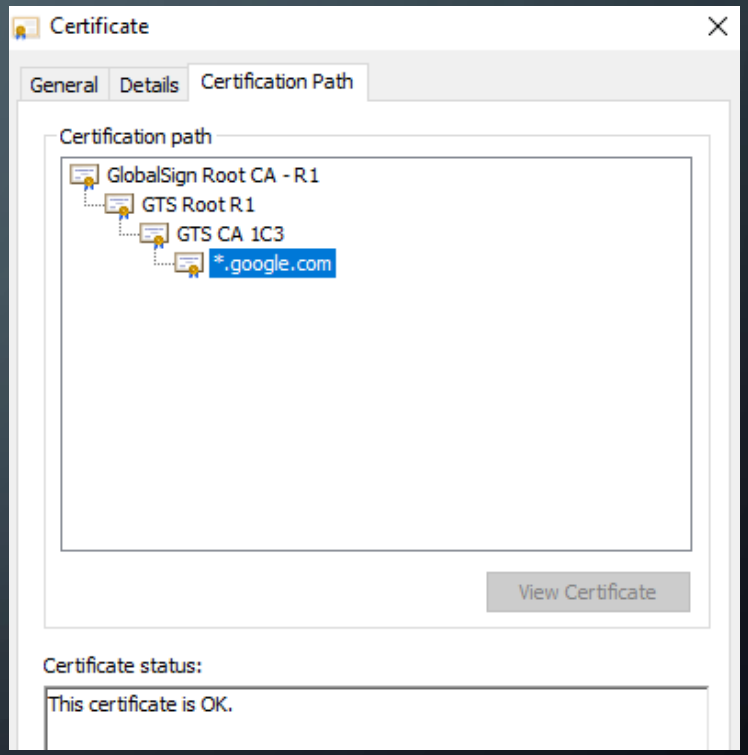
In your web browser, developers already include the major CA certificate so that users do not have this burden to take care of.

Certificate authorities are subject to the most thorough IT audit to ensure safety of everyone the whole PKI.

4.9 CERTIFICATE AUTHORITIES

Certificate authorities are carefully protecting their own private keys offline. This is the CA Root certificates.

The root certificate is only used to generate an intermediate certificate that serves as the online CAs to issue certificates on a routine basis.



4.9 DIGITAL CERTIFICATE

Digital certificate provide the assurance the the people or company they are communicating with truly are who they claim to be.

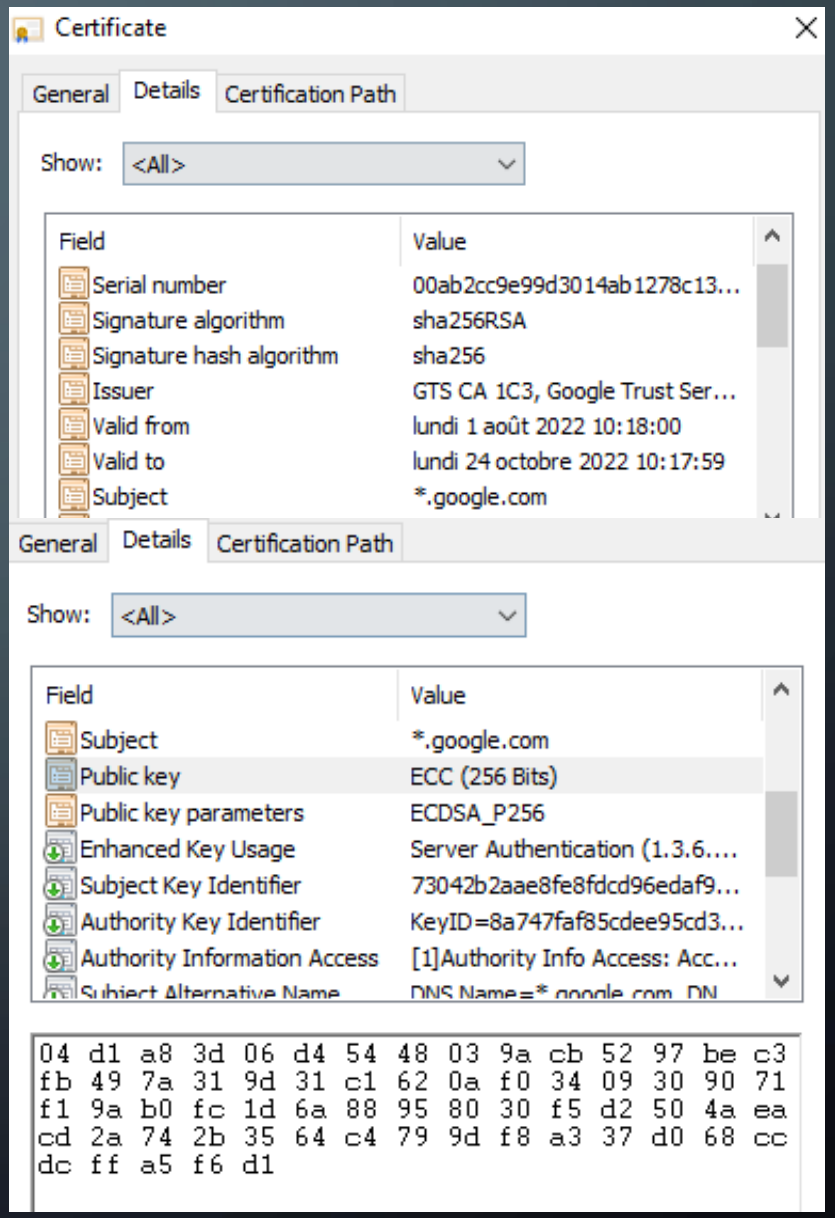
They are nothing else than individual or company public keys validated by a CA.

Digital Certificate contain specific identifying information and is defined by an international standard: X.509

4.9 DIGITAL CERTIFICATE

X.509 gives us following information:

- Serial Number
- Signature algorithm
- Issuer Name
- Validity Period
- Subject = Owner
- The Public Key



4.9 DIGITAL CERTIFICATE

The subject of a certificate may include a wildcard in the certificate name.

That would indicate that the certificate is valid for subdomains as well.

A certificate with subject: `*.vinci.be`

would be valid for all the following domain:

```
vinci.be
www.vinci.be
mail.vinci.be
secure.vinci.be
```

But it would *NOT* cover second-level subdomain:

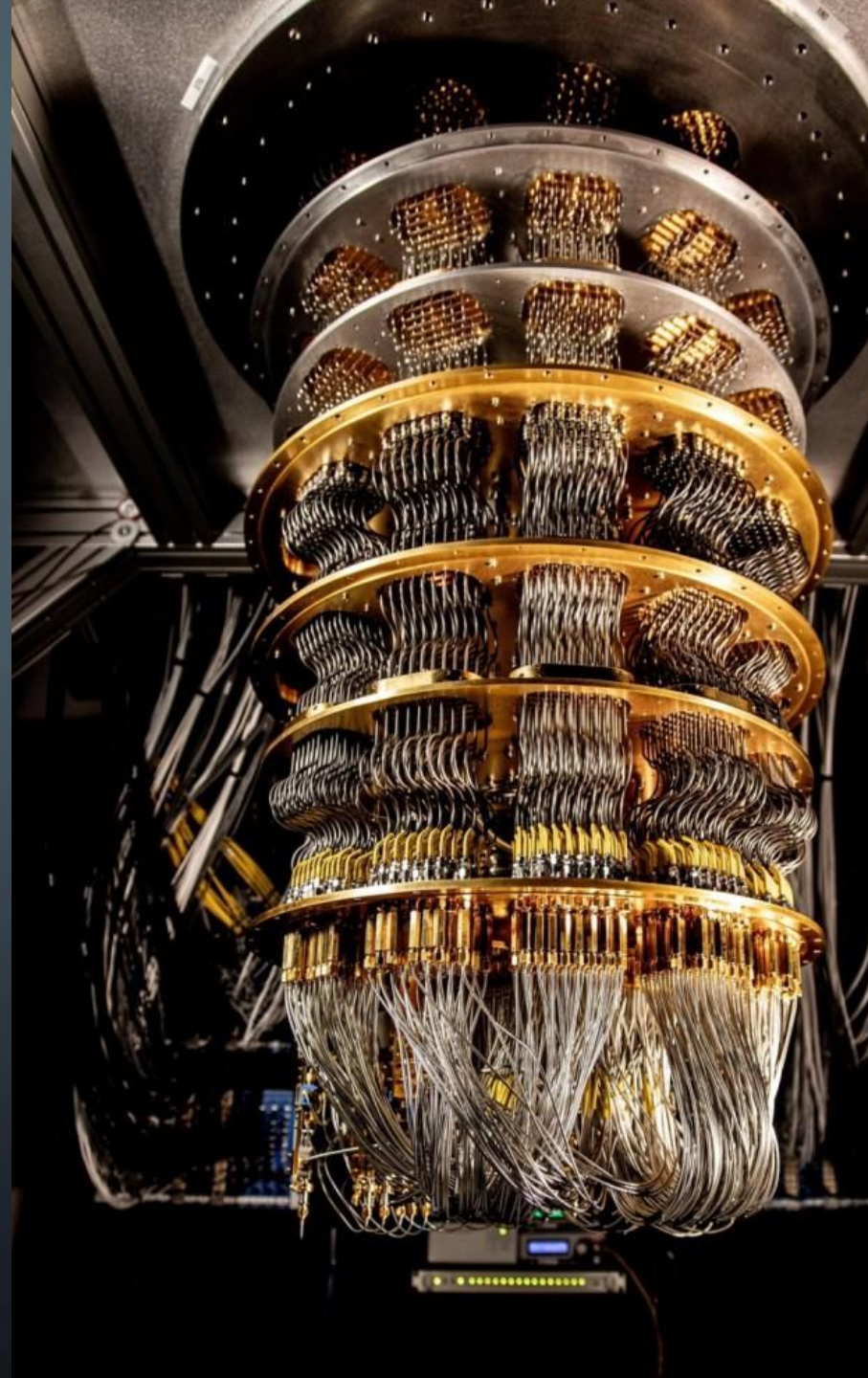
```
super.secure.vinci.be
```


YOU GET A CERTIFICATE,
YOU GET A CERTIFICATE
EVERYONE GET A CERTIFICATE

4.10 POST-QUANTUM

4.10 THE FUTURE IS CLOSE

- Theory is already available since mid-80s
- IBM, Google, NASA have already built quantum computers
- A lot of revolutions are foreseen: new medications, cancer treatment, AI, breakthrough in mathematics and physics
- The power of such computer is measured in "qubits".



4.10 POST-QUANTUM & SECURITY

- Imagine a world where encrypted, secret files are suddenly cracked-open: This is known as the ***quantum apocalypse***.
- What is the real issue ?
  - Widely used today's security algorythm will be broken. RSA for example.
  - Most at risk algorythm are **asymmetric algorythms**
  - Symmetric cryptography is at risk with too short passwords
  - Suddenly a computer will no longer take billions or millions of years to crack security but a matter of hours or minutes.

4.10 POST-QUANTUM & SECURITY ISSUE

- A 20 millions qubits computer could break RSA-2048 in 8 hours...
- … today the most powerfull quantum computer is 433 qubits...
- … but IBM planned to achieve a 4.000 qubits computer by 2025

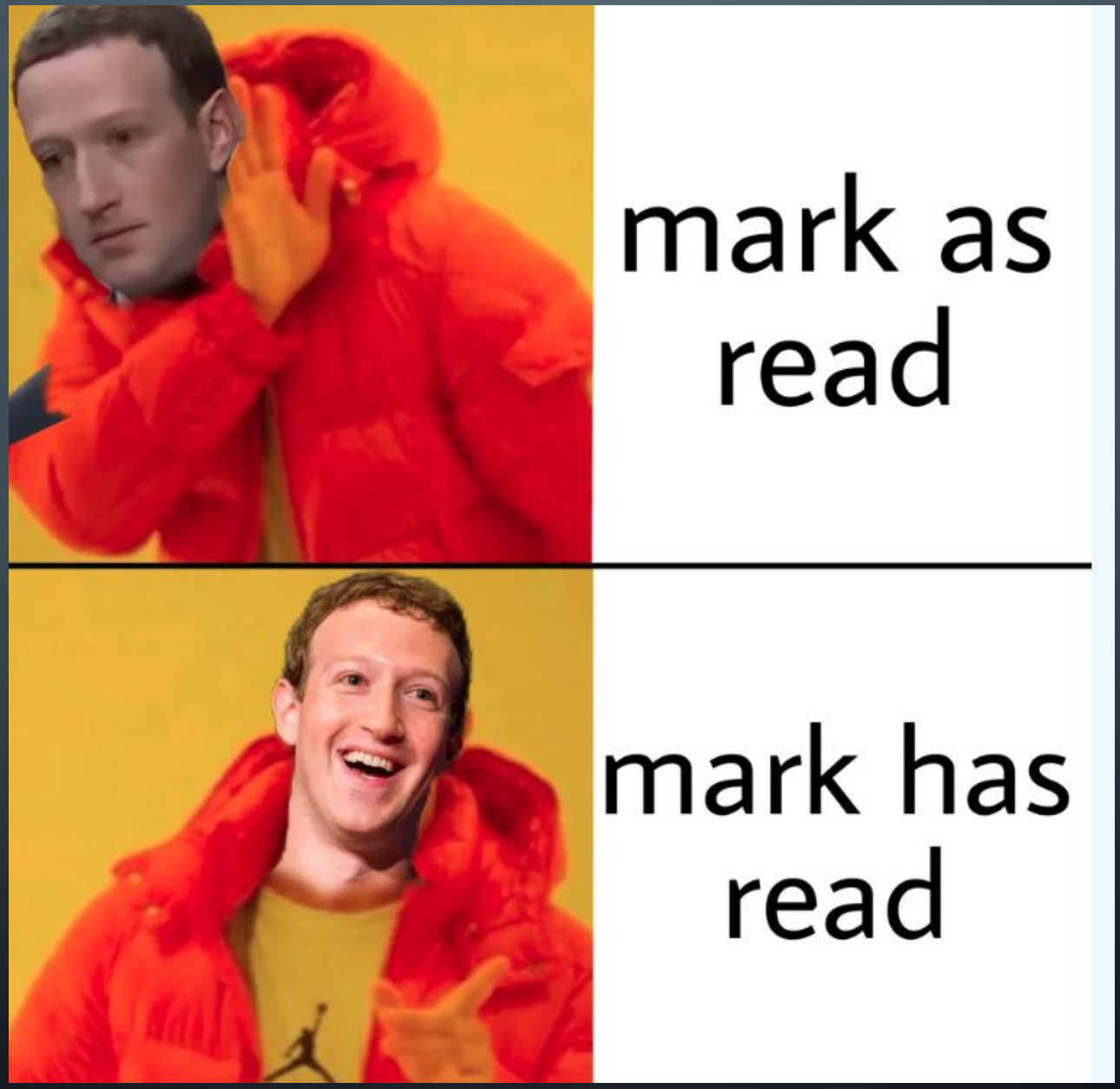
4.10 IT'S NOT MAGICAL

- Quantum computer are not all powerull. Resistant algorythm to quantum computer already exists. Some have been validated and more are currently being reviewd by scientific community.

- In August 2023, Chrome v116 is embedding a Post-Quantum encryption mechanism named: X25519Kyber768.

4.10 IT'S IMPORTANT TO ACT NOW

- The ennemy is: "Harvest now, decrypt later".
- Today it's not possible to break encryption but it's not a problem to store all this information and wait to be able to break it in the future.
- Long-term secret and private information must be kept secure for a long-time.
  - Health information, defense secret, critical services, insurance contract gov. communications, etc.
- If not protected today, in 10 or 20 years these informations will be accessible to unauthorized company and/or government.


mark as read
mark has read