CESi alternance

ÉCOLE SUPÉRIEURE DES MÉTIERS

LE CESI :
ENSEIGNEMENT
SUPERIEUR ET
FORMATION
PROFESSIONNELLE

CESi alternance

ÉCOLE SUPÉRIEURE DES MÉTIERS

Cryptography
I. Intro

LE CESI : ENSEIGNEMENT SUPERIEUR ET FORMATION PROFESSIONNELLE

CESi alternance

ÉCOLE SUPÉRIEURE DES MÉTIERS

Cryptography: from Greek κρυπτός kryptós, "**hidden, secret**"; and γράφειν graphein, "**writing**", or -λογία -logia, "study", respectively is the practice and study of techniques for **secure communication** in the presence of **third parties** (called adversaries)

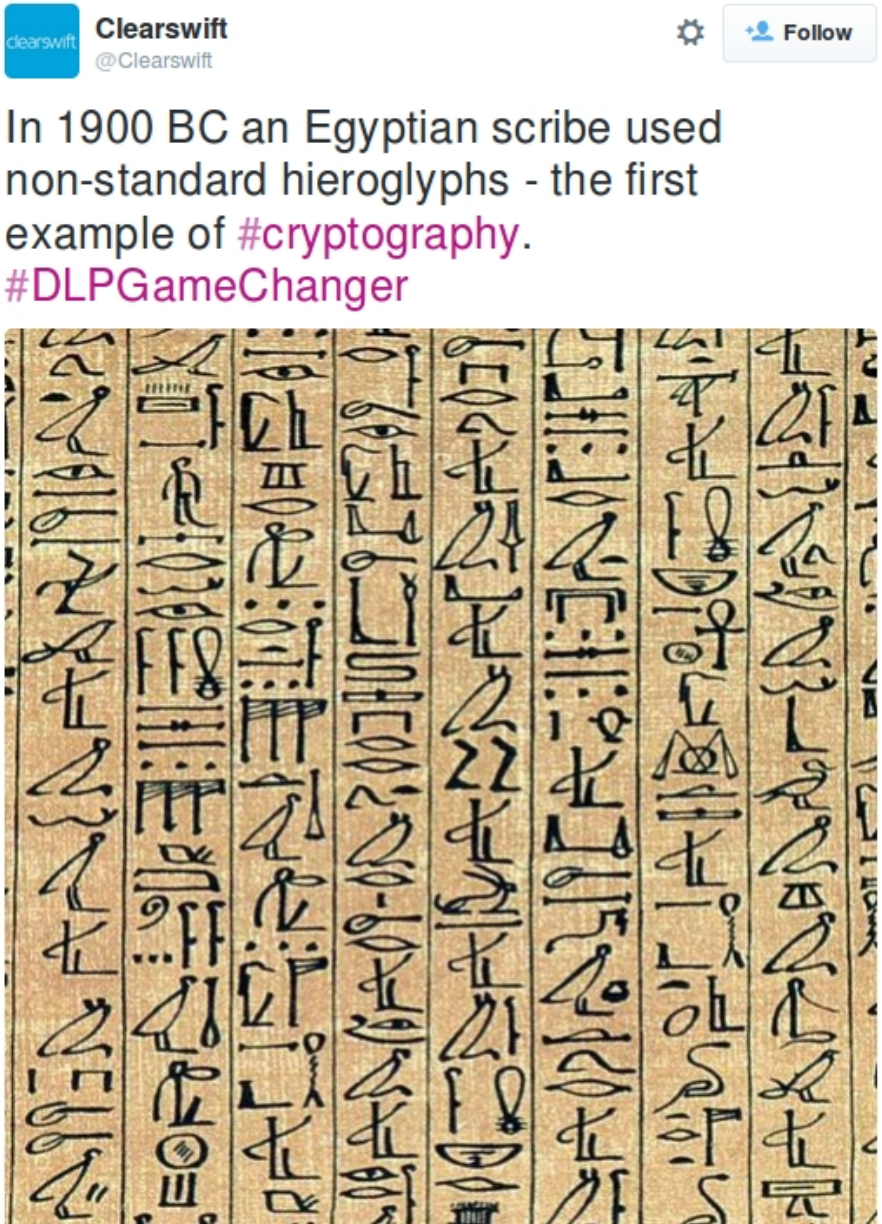
4000 BC

Authentication system

CESi alternance
ÉCOLE SUPÉRIEURE DES MÉTIERS

1900 BC

First known example of cryptography



500 BC

Atbash cipher

substitution cypher for Hebrew alphabet

```
Plain:  אבגדהוזחטיכלמנסעפצקרשת
Cipher: תשרקצפעסנמלכיטחזוהדגבא
```

110 BC

Caesar cipher

The secrecy of the message depends on the secrecy encryption key, rather than the secrecy of the system.

CESi alternance
ÉCOLE SUPÉRIEURE DES MÉTIERS

1883 “La Cryptographie Militaire”

Kerckhoffs’s principle

The **secrecy** of your **message** should always depend on the **secrecy** of the **key**, and not on the **secrecy** of the **encryption system**.

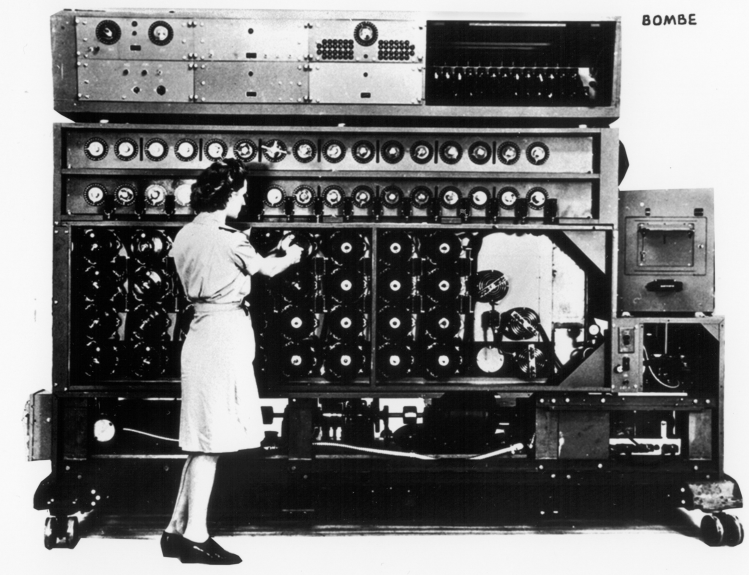
20th century

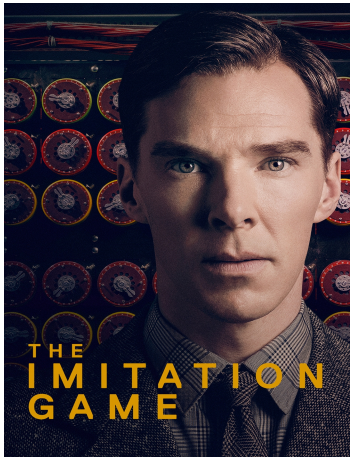
Enigma

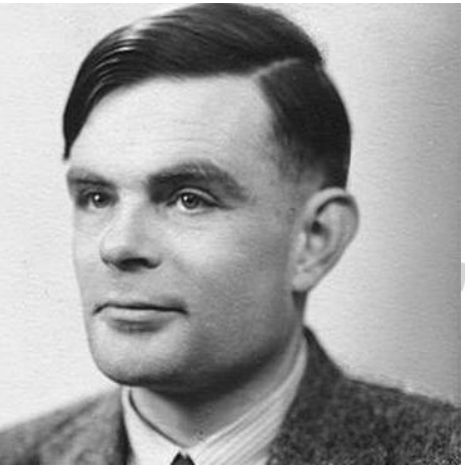
26x26x26x60=1054560

CESi alternance
ÉCOLE SUPÉRIEURE DES MÉTIERS

Fight Machine to Machine







CESi alternance
ÉCOLE SUPÉRIEURE DES MÉTIERS

1970 Modern Cryptography

1970 Lucifer Cypher
1976 Deffie-Hellman


1976 DES (Date Encryption Standard)
1977 RSA (Rivest Shamir Adleman)



1979 Shamir Secret Sharing
1991 PGP (Pretty Good Privacy)

1997 DES Broken
1998 AES (Advanced Encryption System)
1999 Triple-DES (Walter Tuchman)

$$C = E_{DES}^{k3}\left(D_{DES}^{k2}\left(E_{DES}^{k1}(M)\right)\right)$$

CESi alternance
ÉCOLE SUPÉRIEURE DES MÉTIERS

Until 1996 in France....

CESi alternance
ÉCOLE SUPÉRIEURE DES MÉTIERS

Used massively by states...

NATIONAL SECURITY AGENCY
UNITED STATES OF AMERICA

CESi alternance
ÉCOLE SUPÉRIEURE DES MÉTIERS

... or not

CESi alternance
ÉCOLE SUPÉRIEURE DES MÉTIERS

Sometimes shits appends...

During the 1960s, a computer error in Nebraska unwittingly sets off a perilous chain of events leading to a Cold War crisis. The computer sends an order to a squadron piloted by Col. Jack Grady (George Clooney) to drop a bomb on Moscow.

CESi alternance
ÉCOLE SUPÉRIEURE DES MÉTIERS

Only **ONE** rule...

PROTECT YOUR CIPHER KEYS

For **TWO** goals

1- PROTECT COMMUNICATIONS

2- AUTHENTICATE COMMUNICATIONS

Base bricks

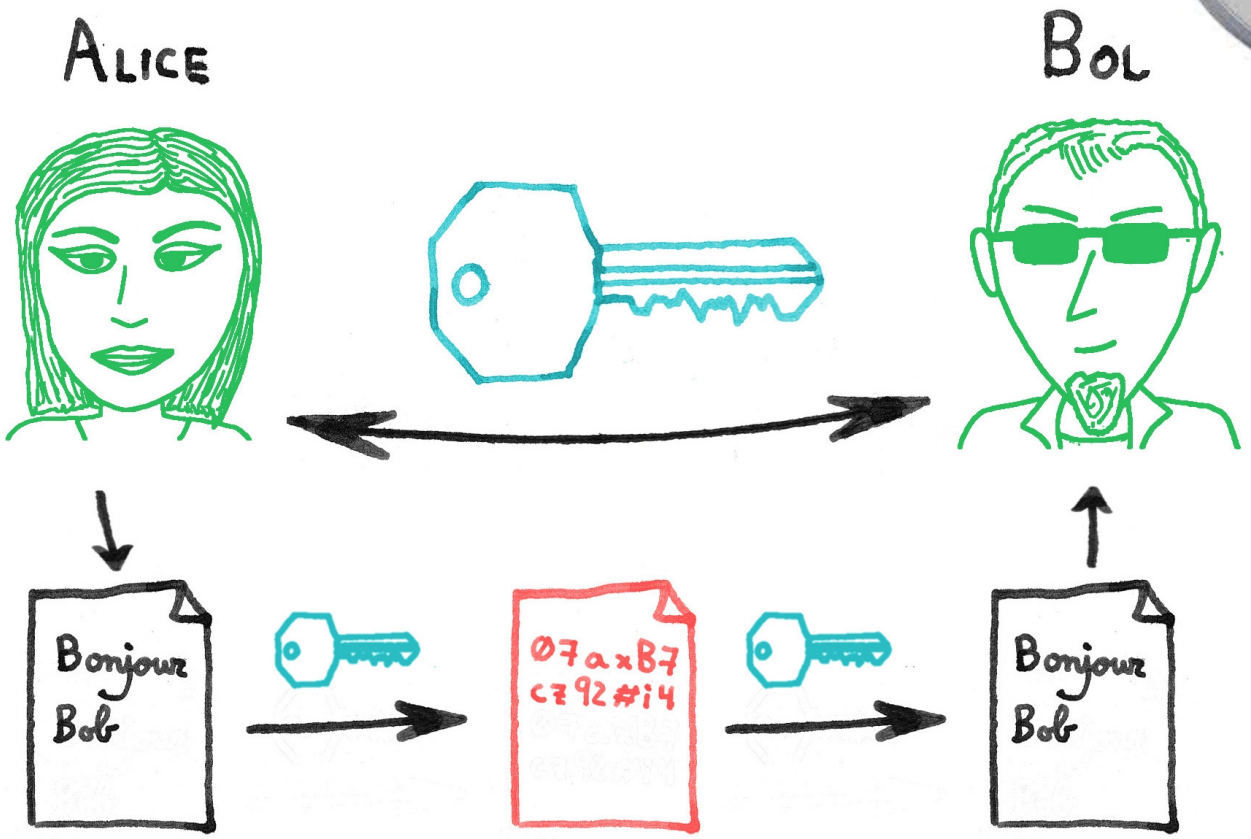
Cryptography
II. Basics

CESi alternance
ÉCOLE SUPÉRIEURE DES MÉTIERS

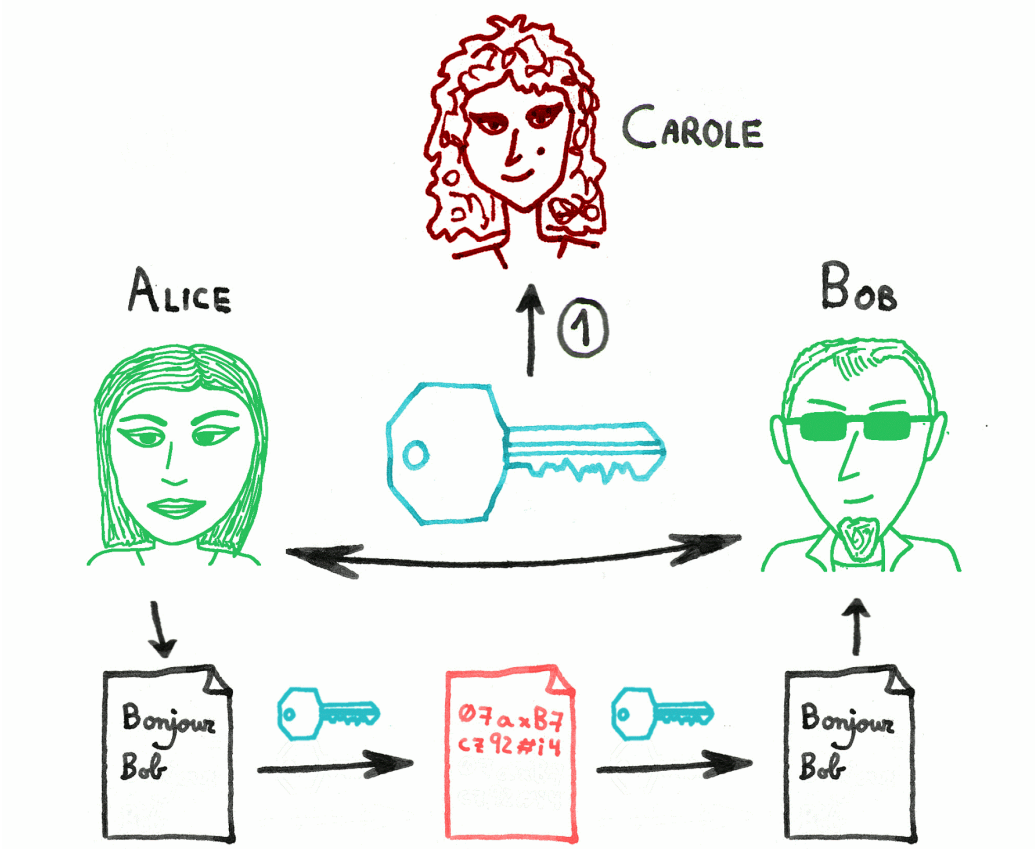
Symmetric Cryptography

The universe itself only existed for 14 billion (1.4e10) years.
It would take ~6.7e40 times longer than the age of the universe to exhaust half of the keyspace of a AES-256 key.

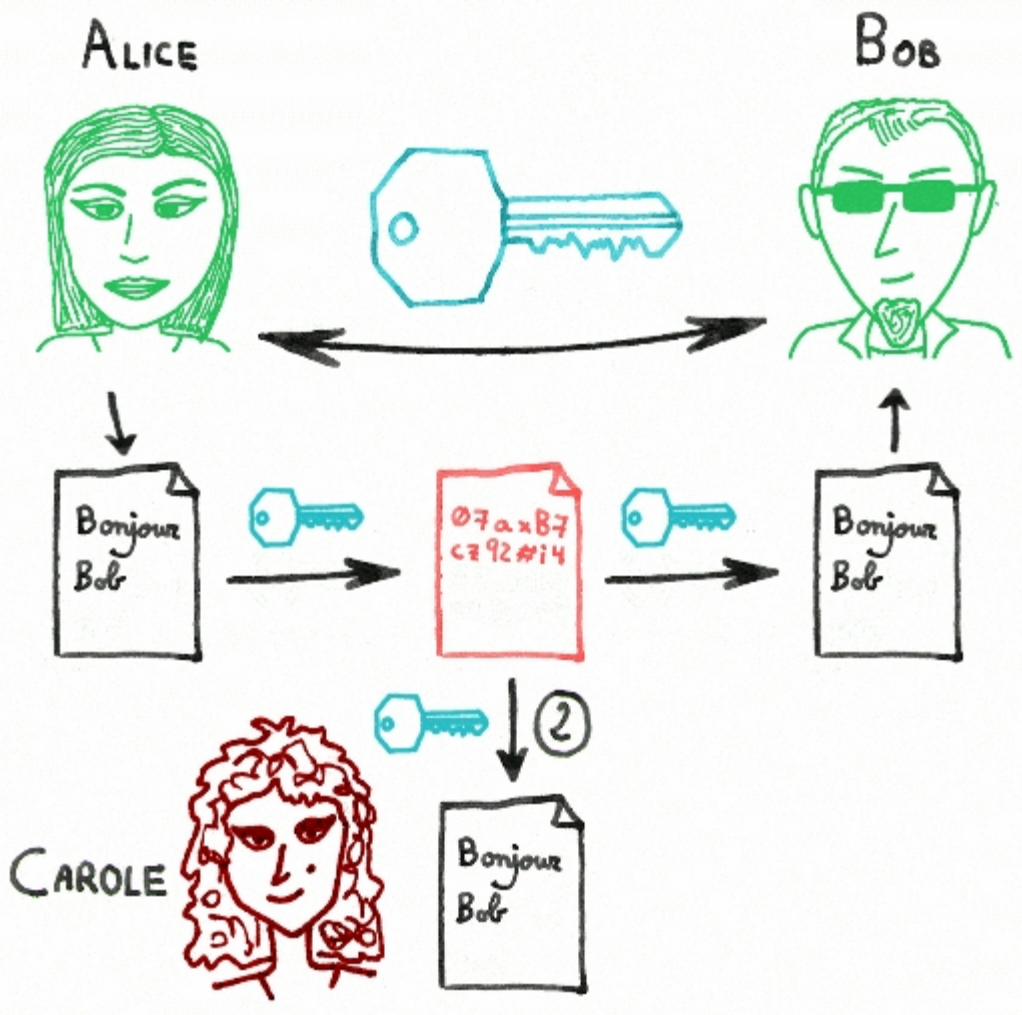
Symmetric Cryptography



Symmetric Cryptography **#PROBLEM**



Symmetric Cryptography **#PROBLEM**



AES-256 ENCRYPTION

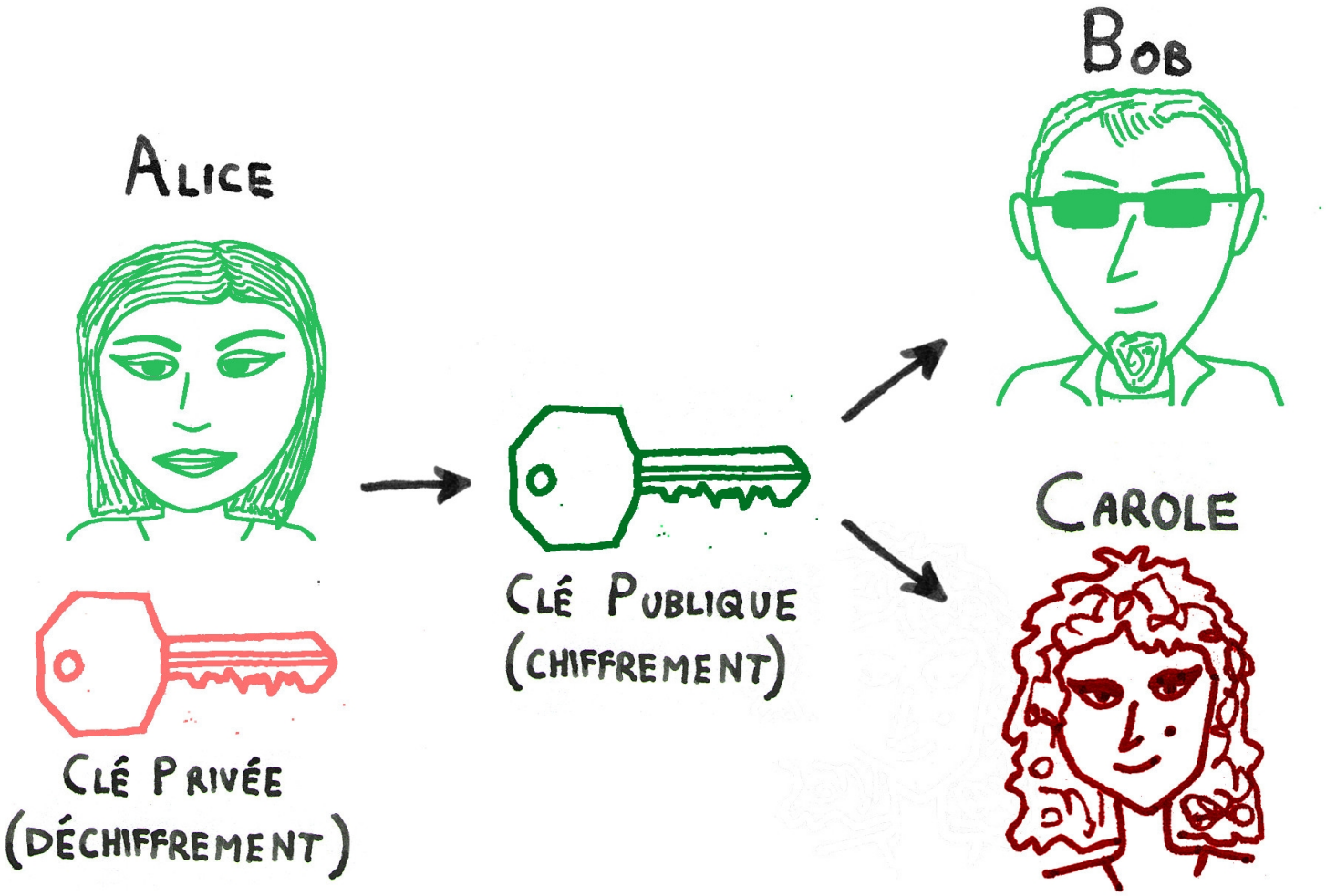
CESi alternance
ÉCOLE SUPÉRIEURE DES MÉTIERS

Asymmetric Cryptography

Keys are likes nuts... you must have two!

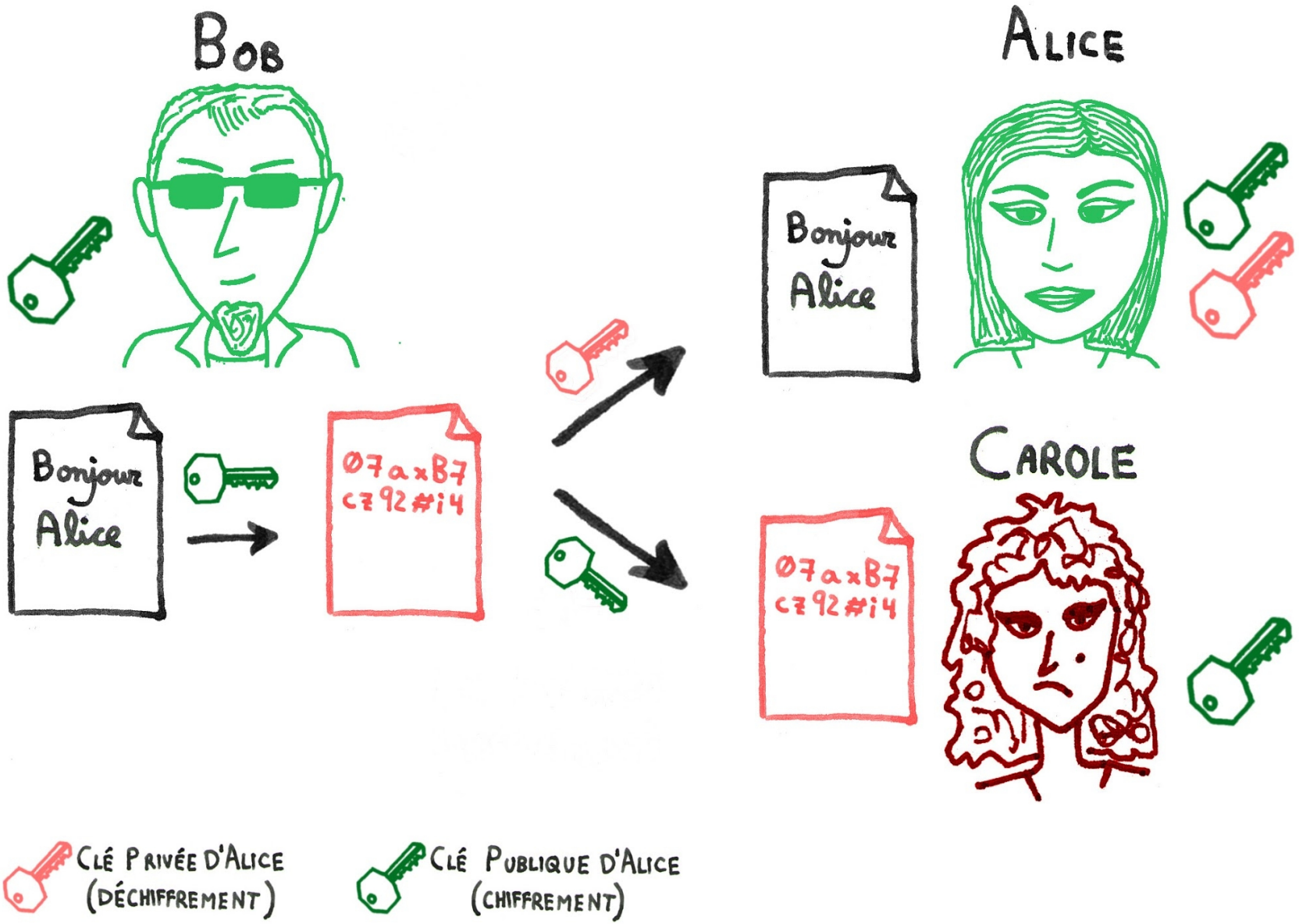
CESi alternance
ÉCOLE SUPÉRIEURE DES MÉTIERS

Asymmetric Cryptography



CESi alternance
ÉCOLE SUPÉRIEURE DES MÉTIERS

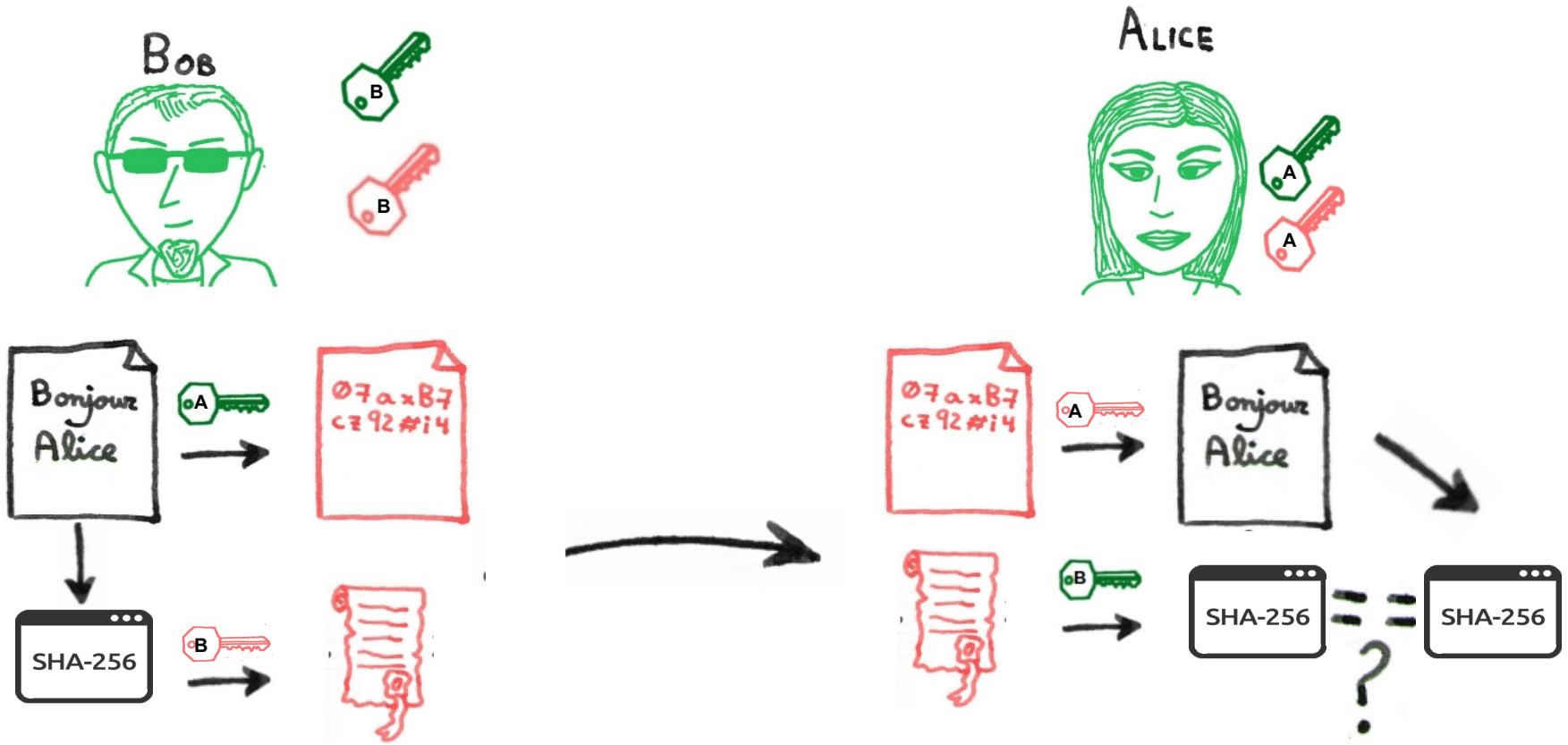
Asymmetric Cryptography



Asymmetric Cryptography

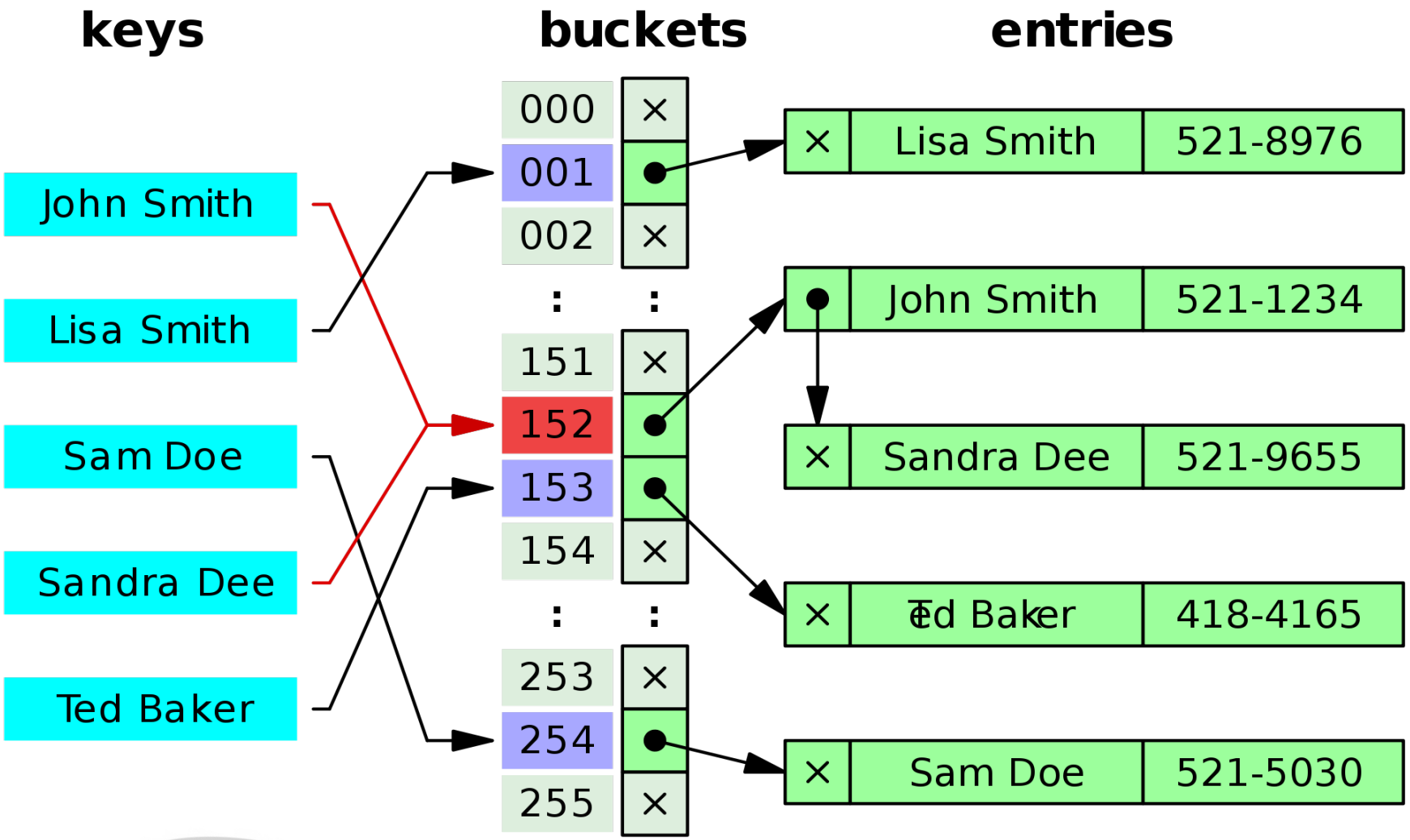
PK Ciphers are useless without an authentication system...

Asymmetric Cryptography



CESi alternance
ÉCOLE SUPÉRIEURE DES MÉTIERS

Hash functions

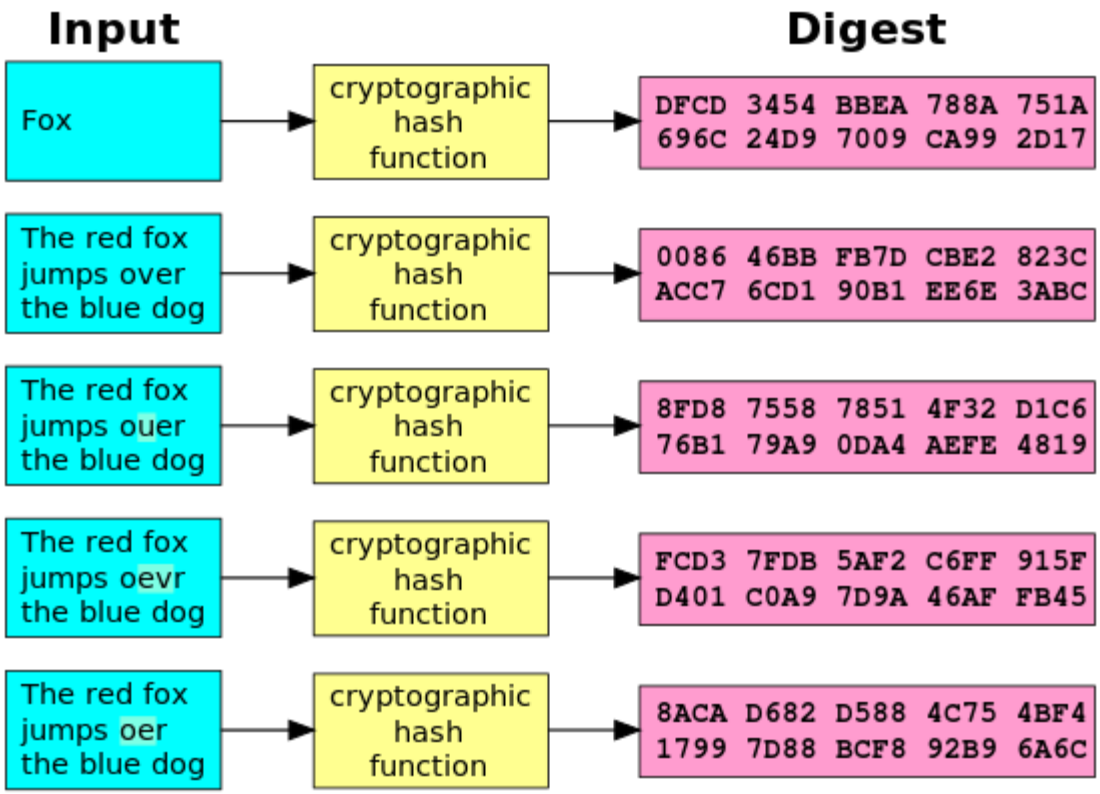


CESi alternance
ÉCOLE SUPÉRIEURE DES MÉTIERS

Cryptographic Hash functions

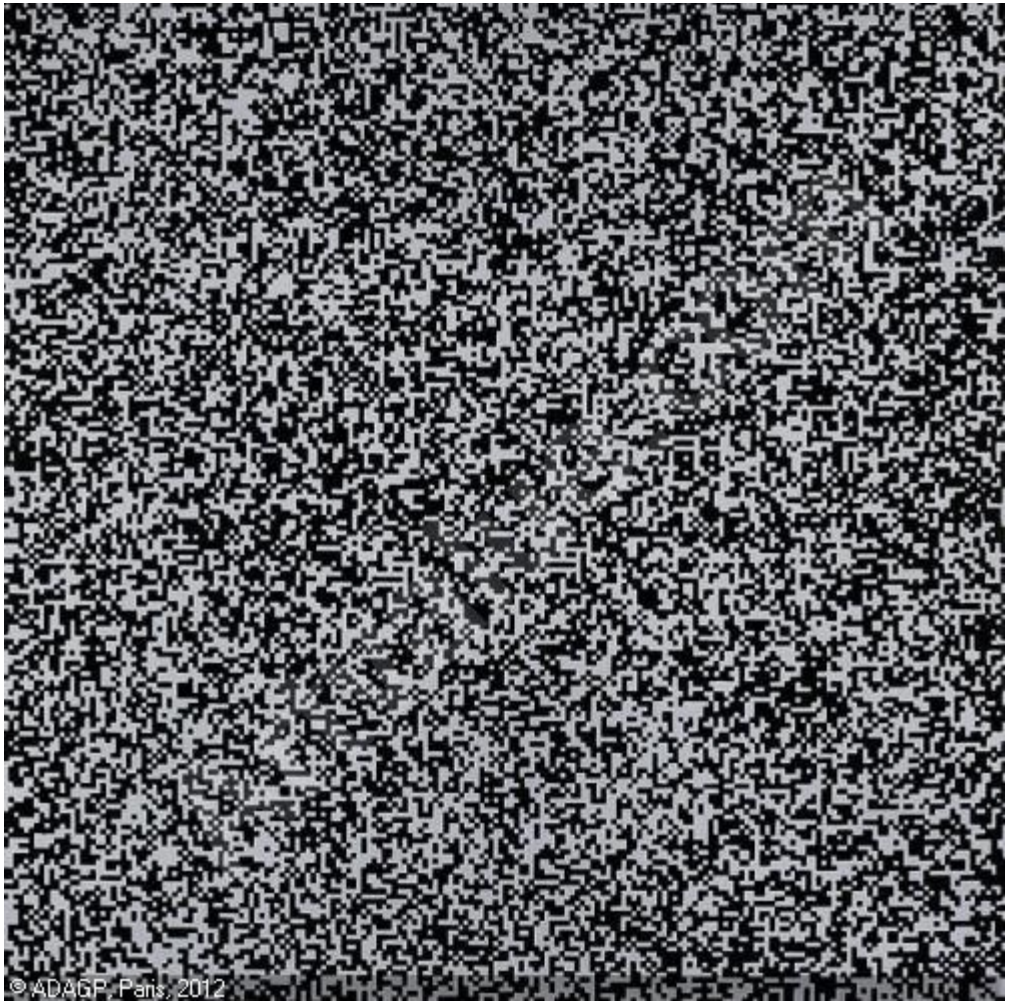
CESi alternance
ÉCOLE SUPÉRIEURE DES MÉTIERS

Cryptographic Hash functions



CESi alternance
ÉCOLE SUPÉRIEURE DES MÉTIERS

Cryptographic Hash functions

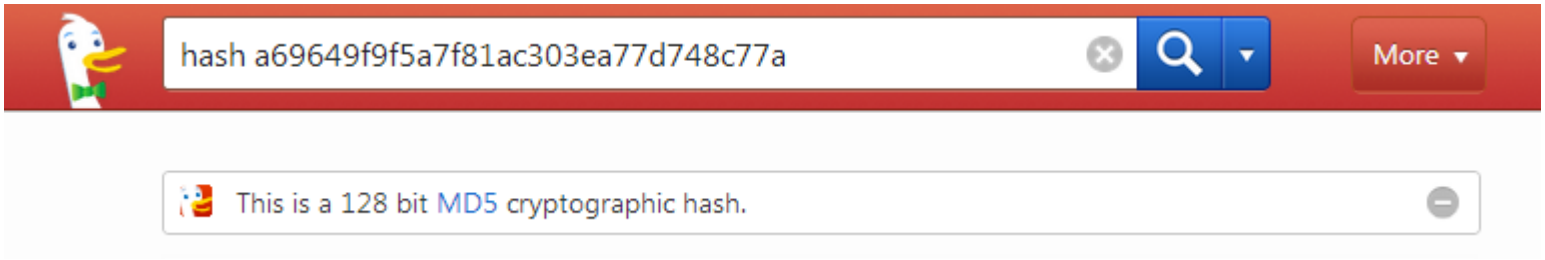


CESi alternance
ÉCOLE SUPÉRIEURE DES MÉTIERS

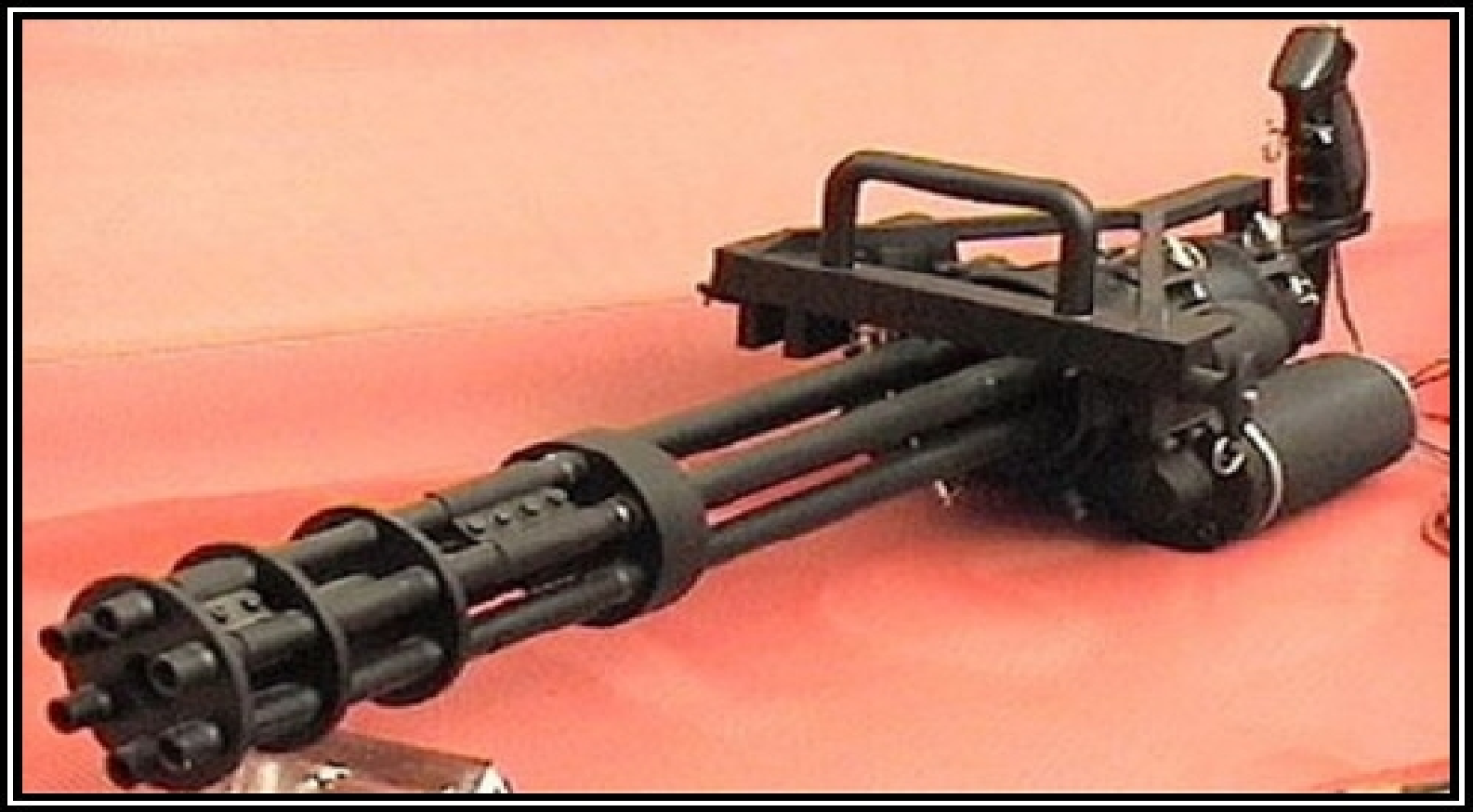
Cryptographic Hash functions

CESi alternance
ÉCOLE SUPÉRIEURE DES MÉTIERS

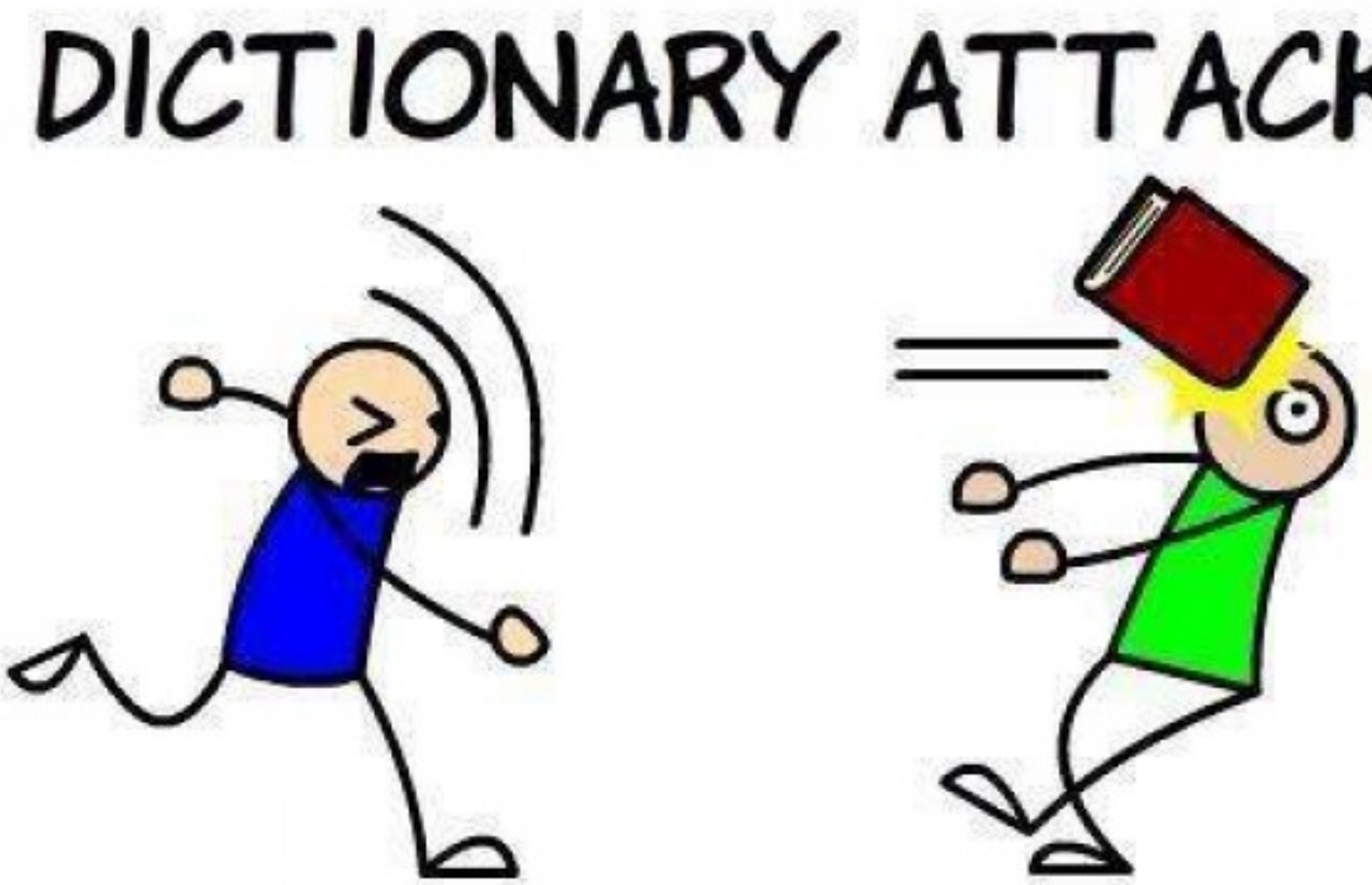
Cryptographic Hash functions



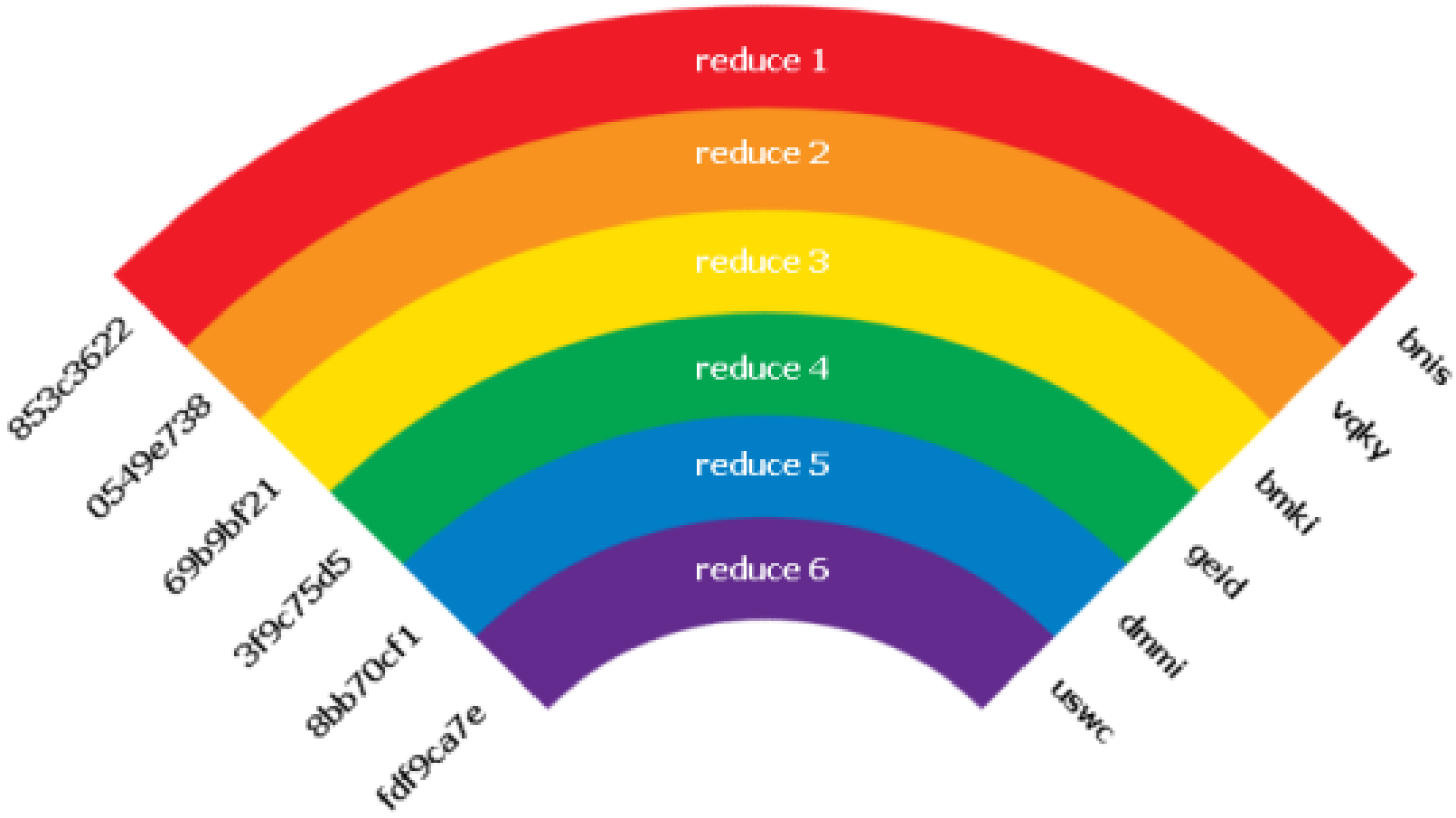
Cryptographic Hash functions



Cryptographic Hash functions



Cryptographic Hash functions



CESi alternance
ÉCOLE SUPÉRIEURE DES MÉTIERS

Cryptographic Hash functions

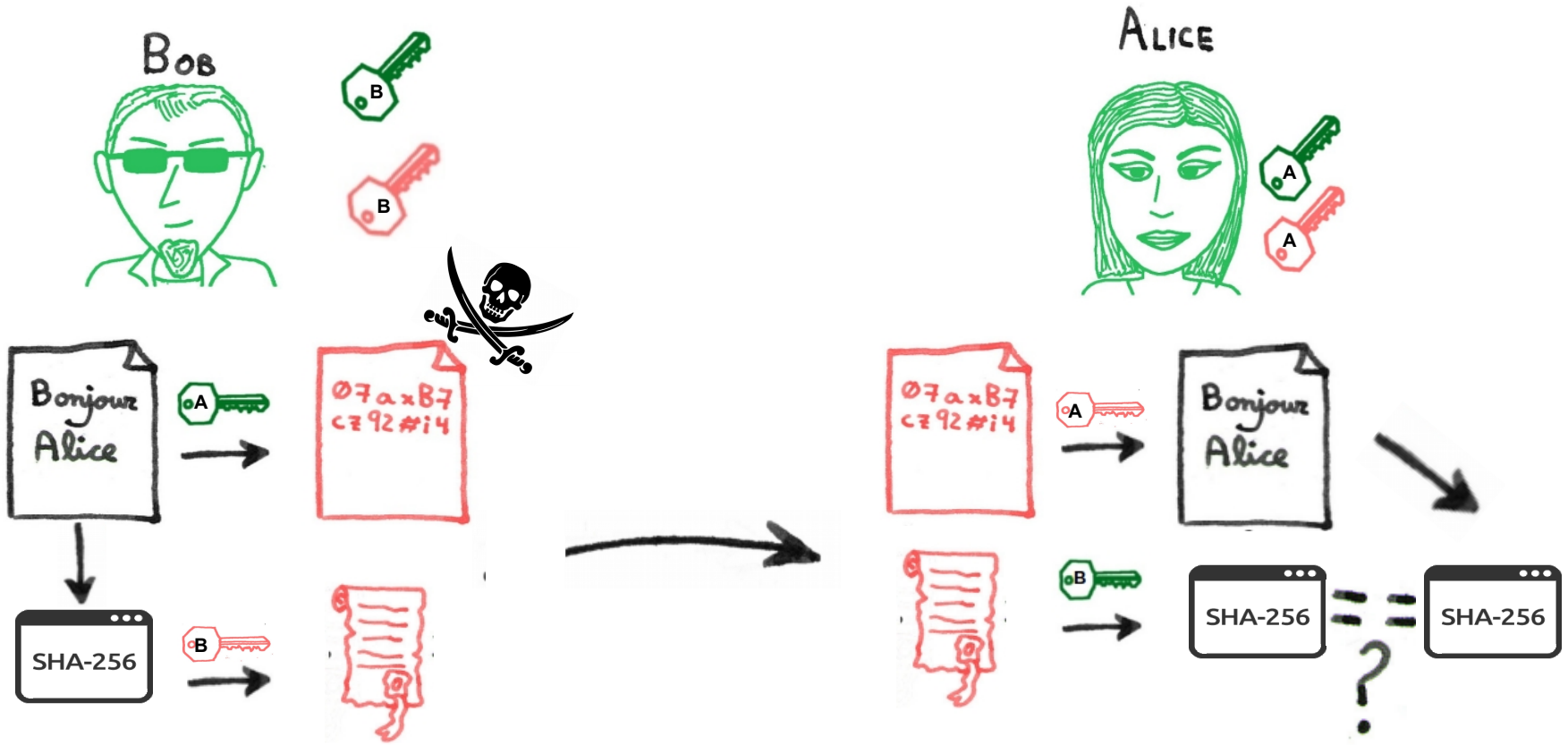
1992 - **MD5** - 128 bits 

1995 (NSA) - **SHA-1** - 160 bits 

2001 (NSA) - **SHA-2** - 224,256,384 or 512 bits

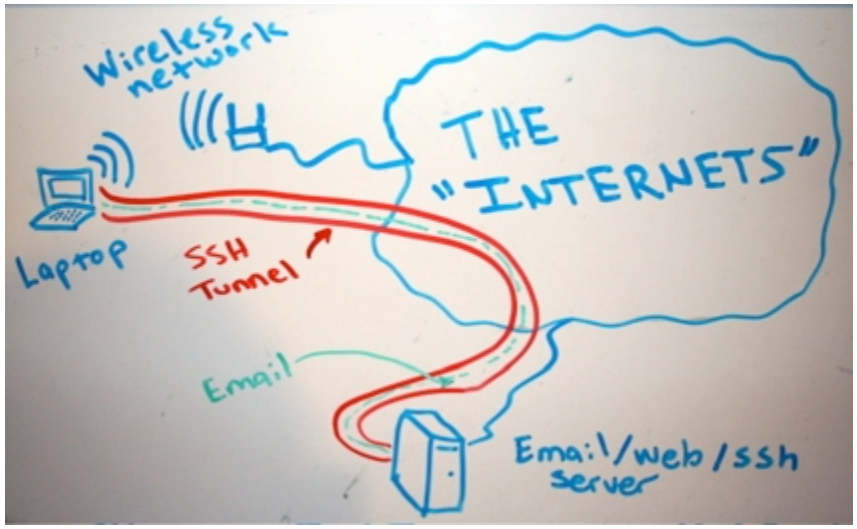
2006 - **SHA-3** - arbitrary

Asymmetric Cryptography



CESi alternance
ÉCOLE SUPÉRIEURE DES MÉTIERS

III. Secured communications



SSL (Secured Socket Layer) History

1994 - SSL 1.O designed but no developed

1995 - SSL 2.0 release

1996 - SSL 3.0 release

2011 - SSL 2.0 

2014 - Poodle attack breaks SSL 3.0 

2015 - SSL 3.0 

CESi alternance
ÉCOLE SUPÉRIEURE DES MÉTIERS

TLS (transport Layer Security)

1999 TLS 1.0 upgrade of SSLv3

2006 – TLS 1.1

2006 – TLS 1.2 - MD5-SHA1 replaced by SHA-256

2011 – SSL backward compatibility removed

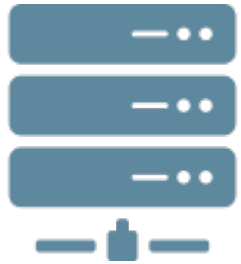
2014 – TLS 1.3

TLS (transport Layer Security)

Salut, on lance une session SSL ?

OK, voici mon certificat de sécurité.

Vérification du certificat

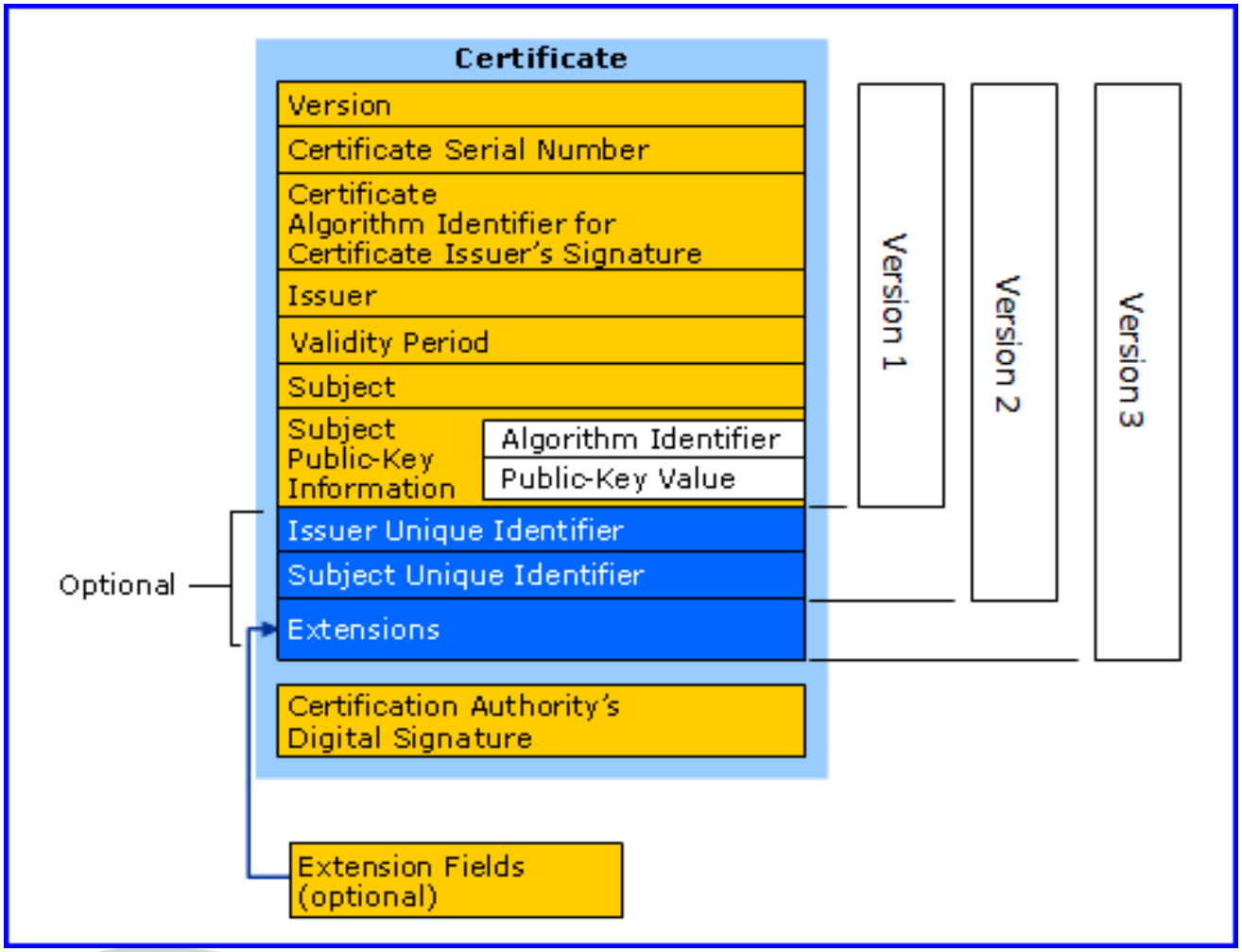


Très bien, voici la clé de notre session.

Communication via tunnel sécurisé

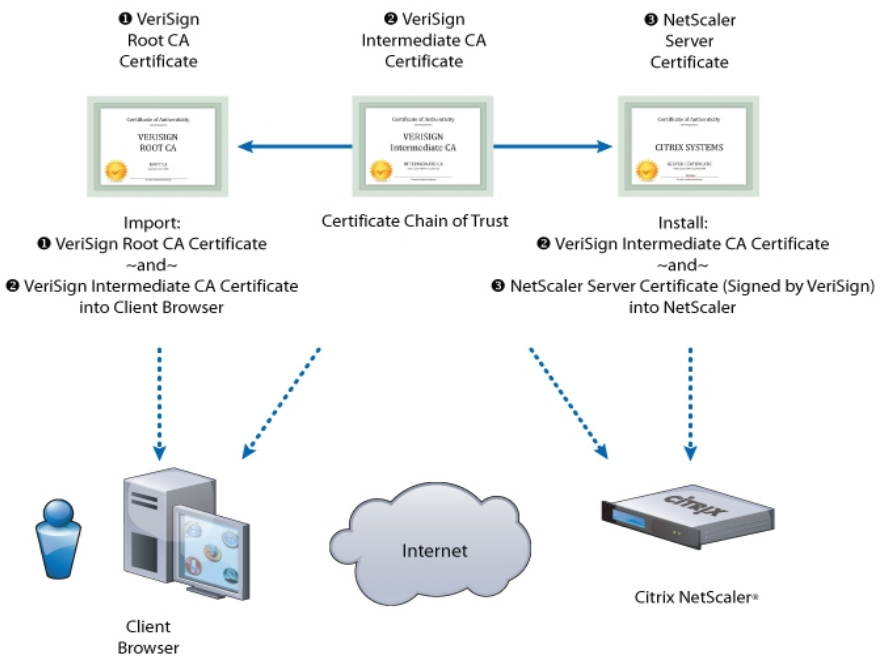
CESi alternance
ÉCOLE SUPÉRIEURE DES MÉTIERS

TLS Need Certificates...



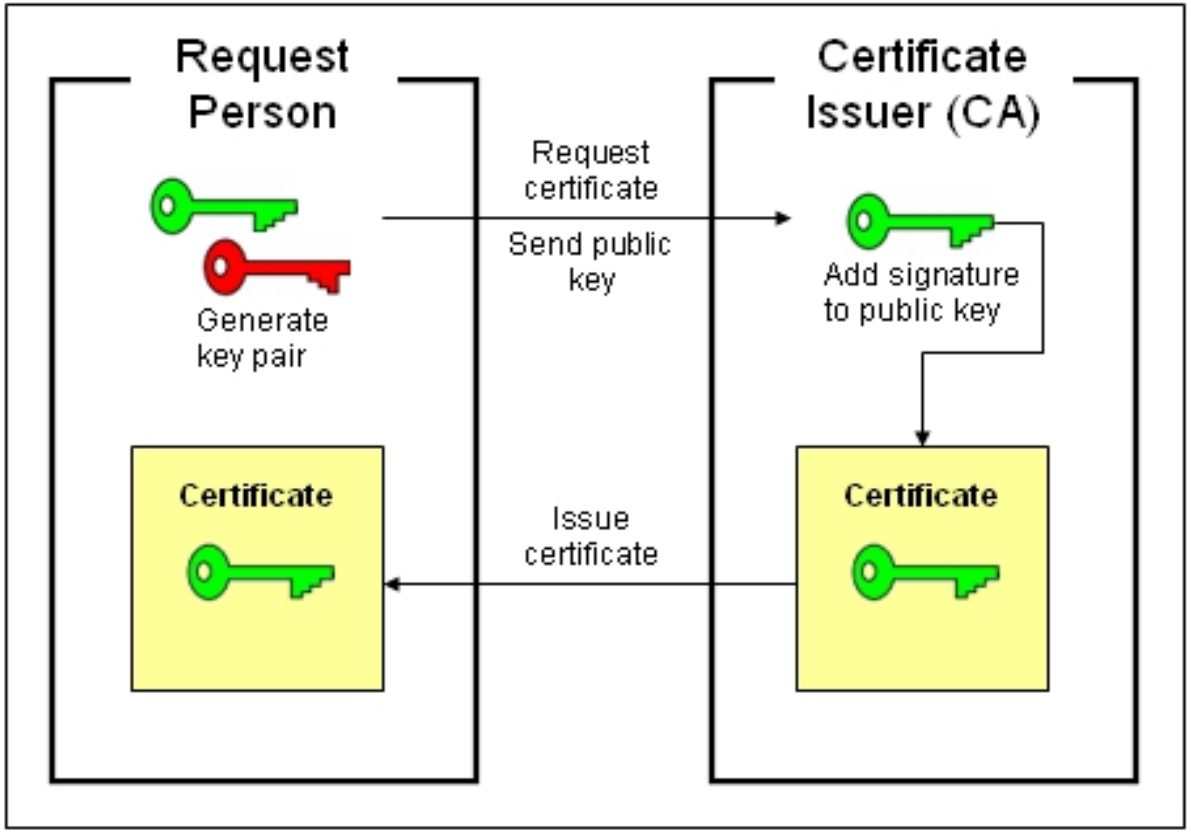
CESi alternance
ÉCOLE SUPÉRIEURE DES MÉTIERS

TLS Need Certificates... trusted



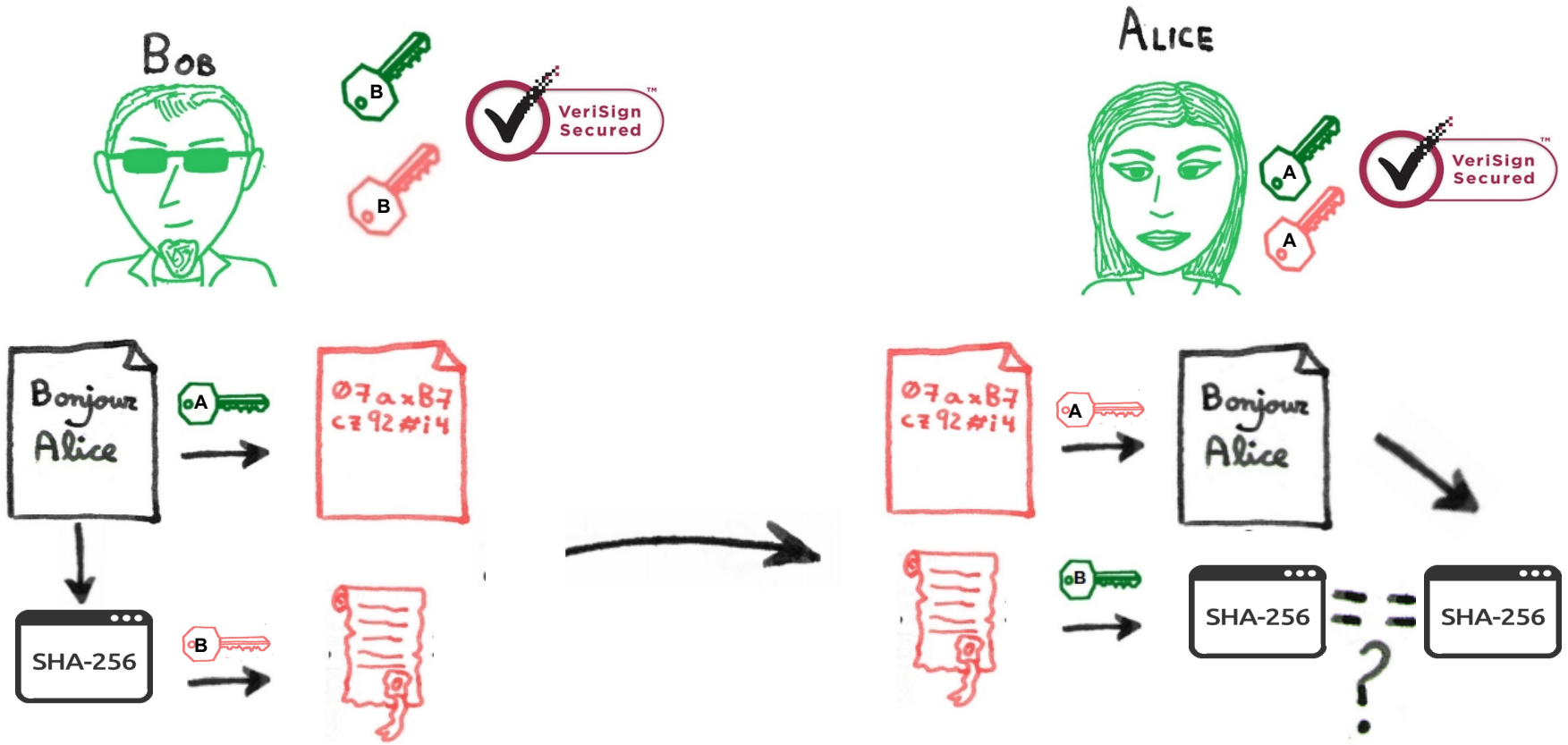
CESi alternance
ÉCOLE SUPÉRIEURE DES MÉTIERS

TLS Need Certificates... trusted



CESi alternance
ÉCOLE SUPÉRIEURE DES MÉTIERS

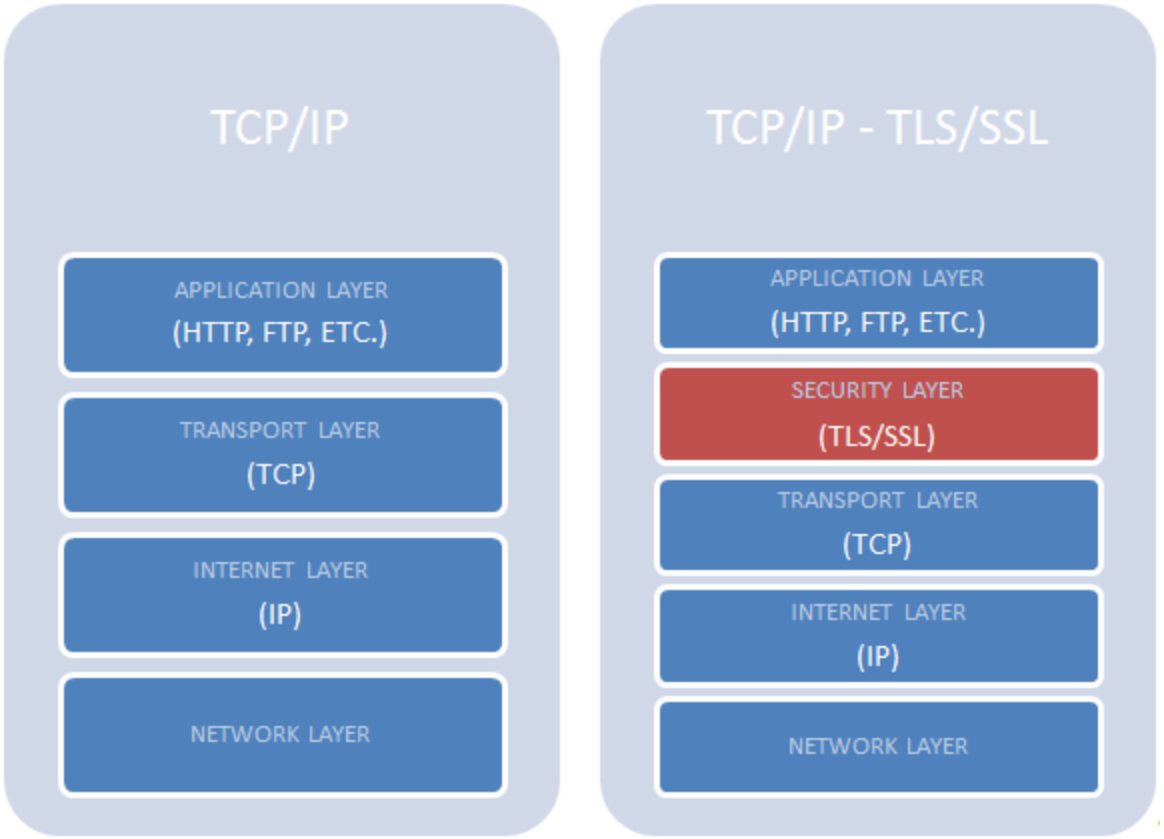
Asymmetric Cryptography



CESi alternance
ÉCOLE SUPÉRIEURE DES MÉTIERS

What is HTTPS ?

HTTP over TLS ;-)



CESi alternance
ÉCOLE SUPÉRIEURE DES MÉTIERS

How used HTTPS is?

30.1% of the Internet have a

secure implementation of HTTPS

CESi alternance
ÉCOLE SUPÉRIEURE DES MÉTIERS

How Insecure internet is? **www.ssllabs.com**

QUALYS® SSL LABS

Home Projects Qualys.com Contact

You are here: Home > Projects > SSL Server Test > centralbank.go.ke

SSL Report: centralbank.go.ke (197.248.5.8)

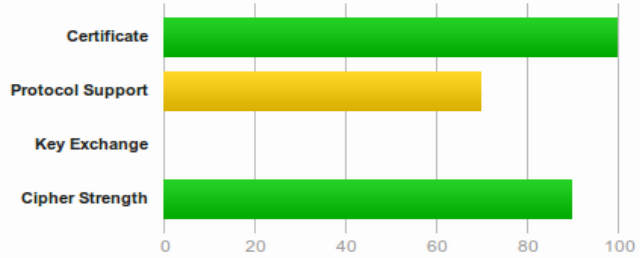
Assessed on: Sun, 15 Nov 2015 17:39:46 UTC | Clear cache

Scan Another »

Summary

Overall Rating

F



Visit our documentation page for more information, configuration guides, and books. Known issues are documented here.

This server supports anonymous (insecure) suites (see below for details). Grade set to F.

This server is vulnerable to the POODLE attack. If possible, disable SSL 3 to mitigate. Grade capped to C. MORE INFO »

This server supports weak Diffie-Hellman (DH) key exchange parameters. Grade capped to B. MORE INFO »

Intermediate certificate has a weak signature. Upgrade to SHA2 as soon as possible to avoid browser warnings. MORE INFO »

This server accepts RC4 cipher, but only with older protocol versions. Grade capped to B. MORE INFO »

The server does not support Forward Secrecy with the reference browsers. MORE INFO »

This server supports TLS_FALLBACK_SCSV to prevent protocol downgrade attacks.

TLS is not the only one...

CESi alternance
ÉCOLE SUPÉRIEURE DES MÉTIERS

SSH (Secure SHell)

Provide confidentiality and integrity of data over an unsecured network, such as the Internet

CESi alternance
ÉCOLE SUPÉRIEURE DES MÉTIERS

SSH (Secure SHell)

1995 – V1

1998 – unauthorized insertion of content into encrypted SSH stream

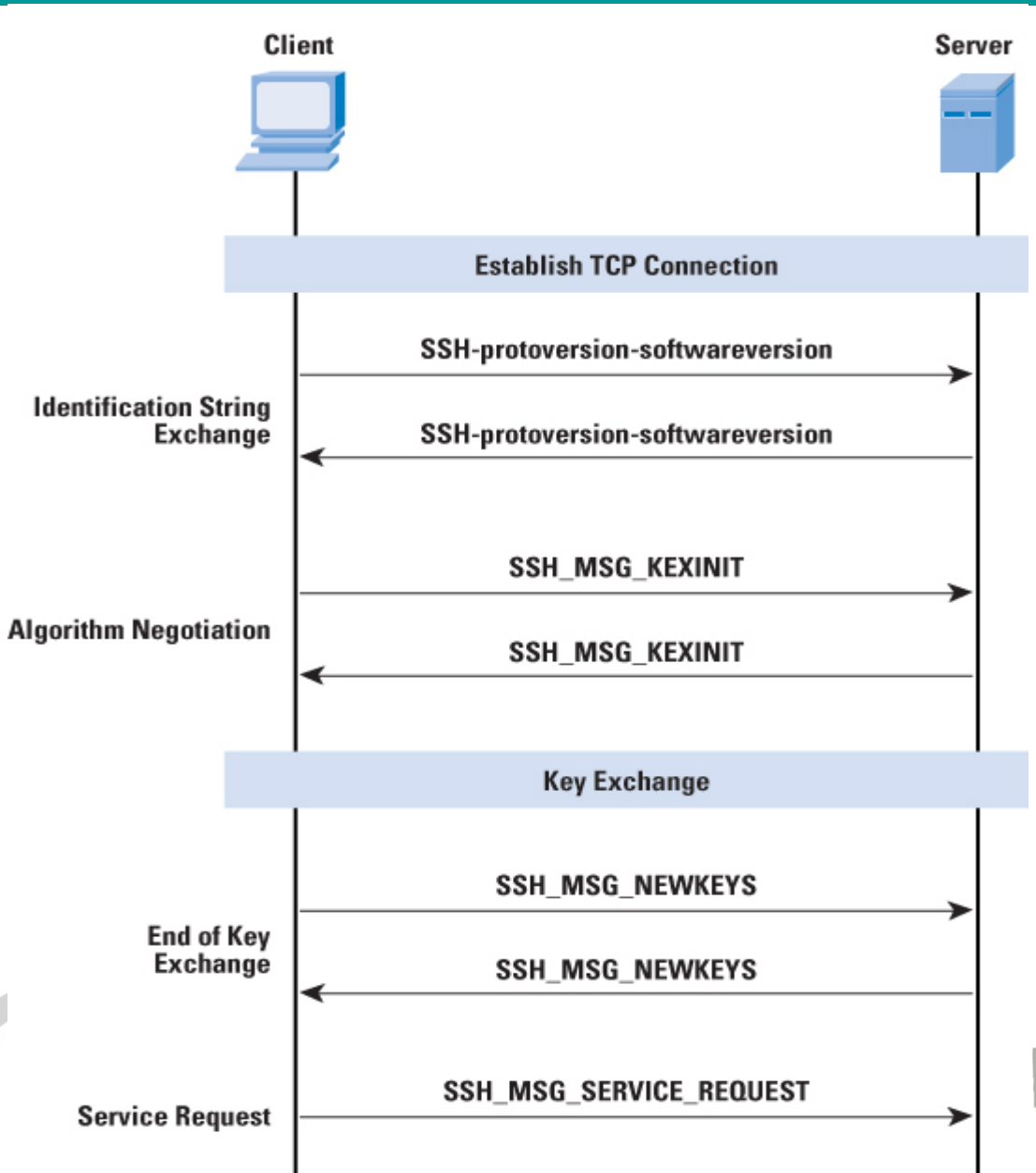
2006 – V2 RFC approved

2007 – SSHv1 considered as obsolete

2008 – Theatrical vulnerability discovered

2014 – Snowden suggest that the NSA may able to decrypt some SSH traffic.

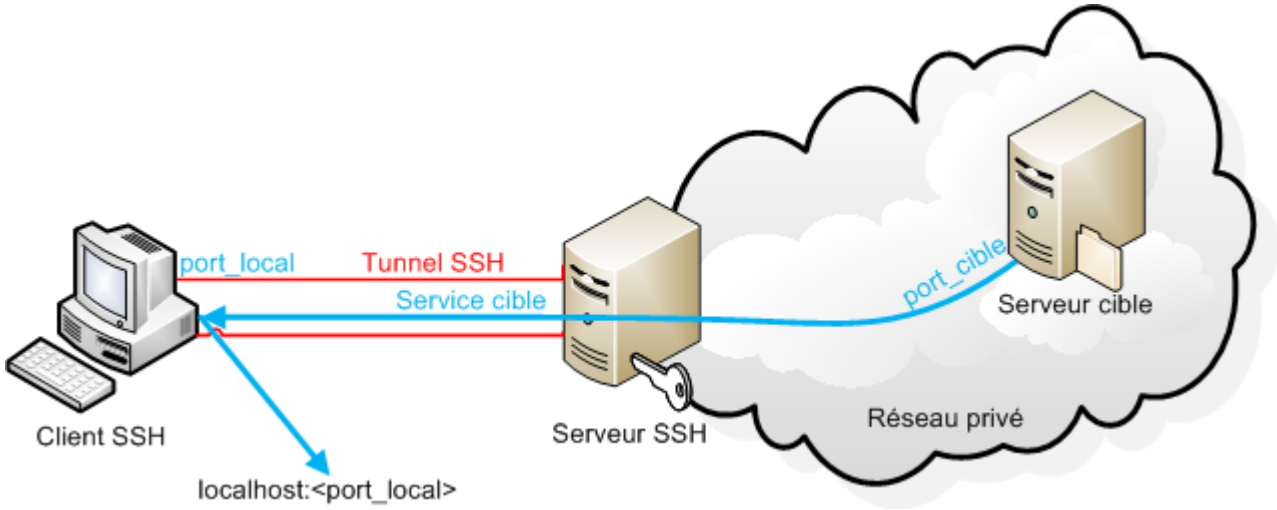
SSH (Secure SHell)



Tunneling

SSH (Secure SHell)

Expose only bastion servers



CESi alternance
ÉCOLE SUPÉRIEURE DES MÉTIERS

Crypto → Keys storage

CESi alternance
ÉCOLE SUPÉRIEURE DES MÉTIERS

Crypto → Keys storage

Bush “We don't torture, we baptize”

Crypto → Keys storage

Store keys in a secured key server

Crypto → Keys storage

The... classic (old school)

Classic - HSM – Works... but does not scale

→ Data center centric
→ Used by Banks & institutional companies
→ Proprietary techno

Crypto → Keys storage

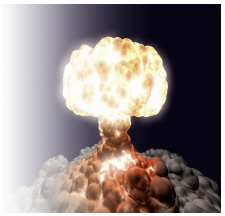
The... most complete

→ Unified API
→ Access management & logs
→ Integrated in many OPS tools
→ OpenSource

Crypto → Keys storage

The... challenger

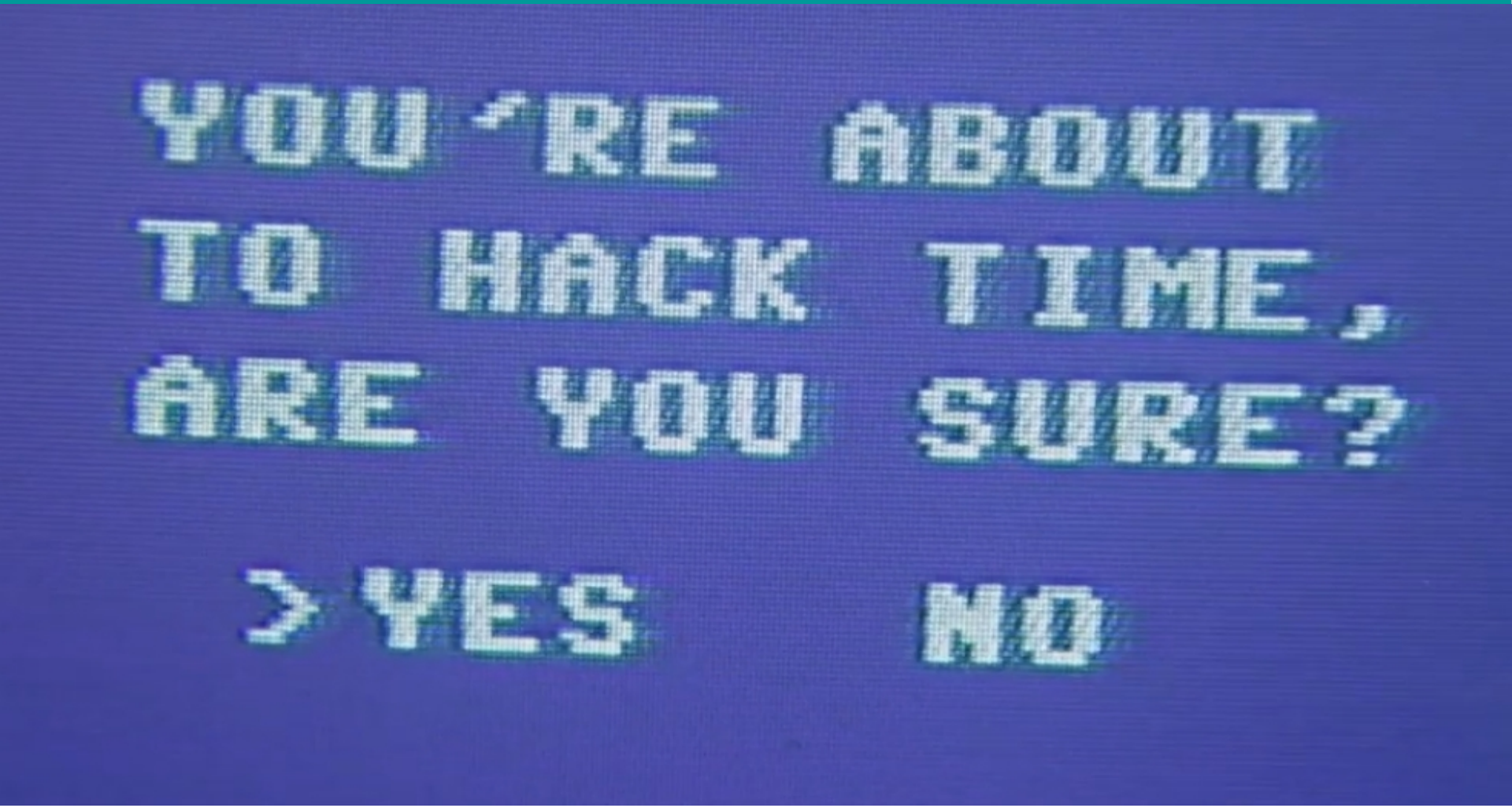
→ SSH centric
→ Low level
→ Use a Shamir's Sharing Secret
→ Made in Breizh
→ OpenSource



OSS (OpenSecretServer)

CESi alternance
ÉCOLE SUPÉRIEURE DES MÉTIERS

And now ?



CESi alternance
ÉCOLE SUPÉRIEURE DES MÉTIERS

CESi alternance

ÉCOLE SUPÉRIEURE DES MÉTIERS

LE CESI :
ENSEIGNEMENT
SUPERIEUR ET
FORMATION
PROFESSIONNELLE

CESi alternance
ÉCOLE SUPÉRIEURE DES MÉTIERS

Cryptography
I. Intro

LE CESI : ENSEIGNEMENT SUPERIEUR ET FORMATION PROFESSIONNELLE

CESi alternance
ÉCOLE SUPÉRIEURE DES MÉTIERS

Cryptography: from Greek κρυπτός kryptós, "**hidden, secret**"; and γράφειν graphein, "**writing**", or -λογία -logia, "study", respectively is the practice and study of techniques for **secure communication** in the presence of **third parties** (called adversaries)

LE CESI : ENSEIGNEMENT SUPERIEUR ET FORMATION PROFESSIONNELLE

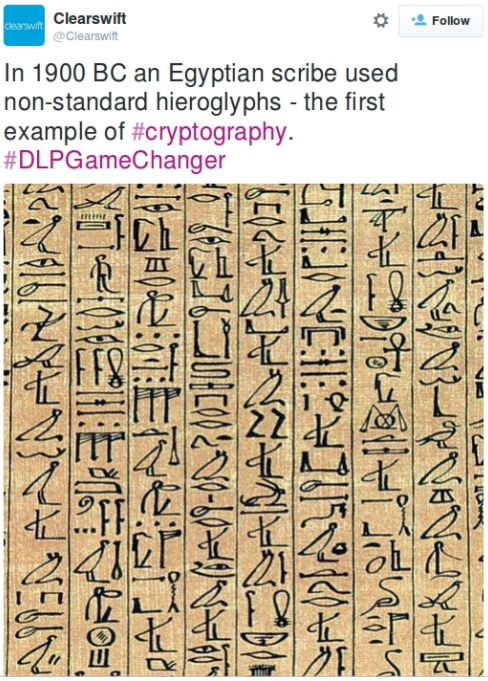
4000 BC

Authentication system

CESi alternance
ÉCOLE SUPÉRIEURE DES MÉTIERS

1900 BC

First known example of cryptography



500 BC

Atbash cipher

substitution cypher for Hebrew alphabet

```
Plain:  אבגדהוזחטיכלמנסעפצקרשת
Cipher: תשרקצפעסנמלכיטחזוהדגבא
```


CESi alternance
ÉCOLE SUPÉRIEURE DES MÉTIERS

110 BC

Caesar cipher

The secrecy of the message depends on the secrecy encryption key, rather than the secrecy of the system.

CESi alternance
ÉCOLE SUPÉRIEURE DES MÉTIERS

1883 “La Cryptographie Militaire”

Kerckhoffs’s principle

The **secrecy** of your **message** should always depend on the **secrecy** of the **key**, and not on the **secrecy** of the **encryption system**.

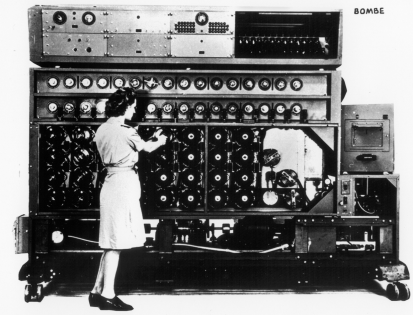
20th century

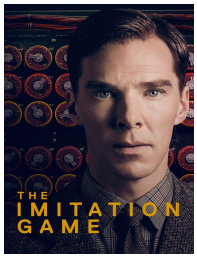
Enigma

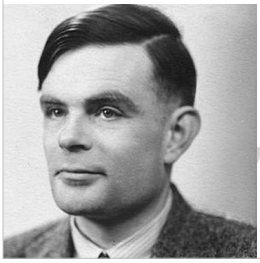
26x26x26x60=1054560

CESi alternance
ÉCOLE SUPÉRIEURE DES MÉTIERS

Fight Machine to Machine







CESi
alternance
ÉCOLE SUPÉRIEURE DES MÉTIERS

1970 Modern Cryptography

1970 Lucifer Cypher
1976 Deffie-Hellman  
1976 DES (Date Encryption Standard)
1977 RSA (Rivest Shamir Adleman)   
1979 Shamir Secret Sharing
1991 PGP (Pretty Good Privacy)
1997 DES Broken 
1998 AES (Advanced Encryption System)
1999 Triple-DES (Walter Tuchman)

$$C = E_{DES}^{k3}\left(D_{DES}^{k2}\left(E_{DES}^{k1}(M)\right)\right)$$

CESi alternance
ÉCOLE SUPÉRIEURE DES MÉTIERS

Until 1996 in France....

CESi alternance
ÉCOLE SUPÉRIEURE DES MÉTIERS

Used massively by states...

CESi alternance
ÉCOLE SUPÉRIEURE DES MÉTIERS

... or not

CESi alternance
ÉCOLE SUPÉRIEURE DES MÉTIERS

Sometimes shits appends...

During the 1960s, a computer error in Nebraska unwittingly sets off a perilous chain of events leading to a Cold War crisis. The computer sends an order to a squadron piloted by Col. Jack Grady (George Clooney) to drop a bomb on Moscow.

CESi alternance
ÉCOLE SUPÉRIEURE DES MÉTIERS

Only **ONE** rule...

PROTECT YOUR CIPHER KEYS

CESi alternance
ÉCOLE SUPÉRIEURE DES MÉTIERS

For **TWO** goals

1- PROTECT COMMUNICATIONS

2- AUTHENTICATE COMMUNICATIONS

CESi alternance
ÉCOLE SUPÉRIEURE DES MÉTIERS

Cryptography
II. Basics

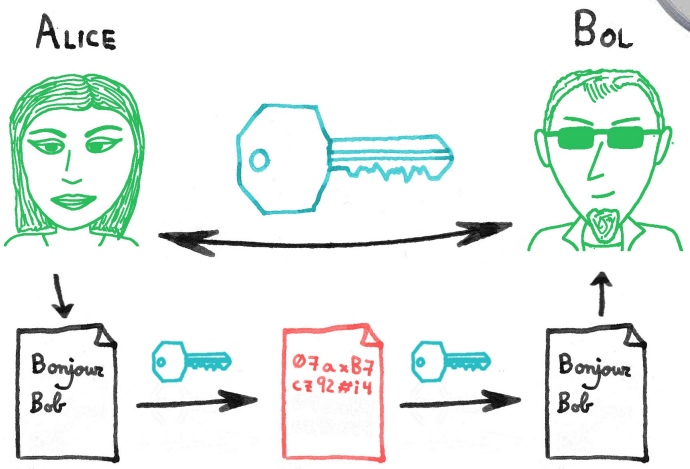
CESi alternance
ÉCOLE SUPÉRIEURE DES MÉTIERS

Symmetric Cryptography

The universe itself only existed for 14 billion (1.4e10) years.
It would take ~6.7e40 times longer than the age of the universe to exhaust half of the keyspace of a AES-256 key.

CESi alternance
ÉCOLE SUPÉRIEURE DES MÉTIERS

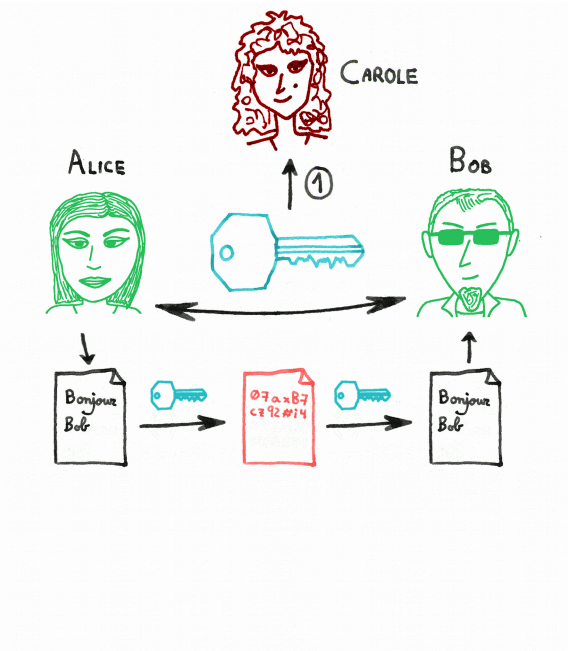
Symmetric Cryptography



AES-256 ENCRYPTION

CESI alternance
ÉCOLE SUPÉRIEURE DES MÉTIERS

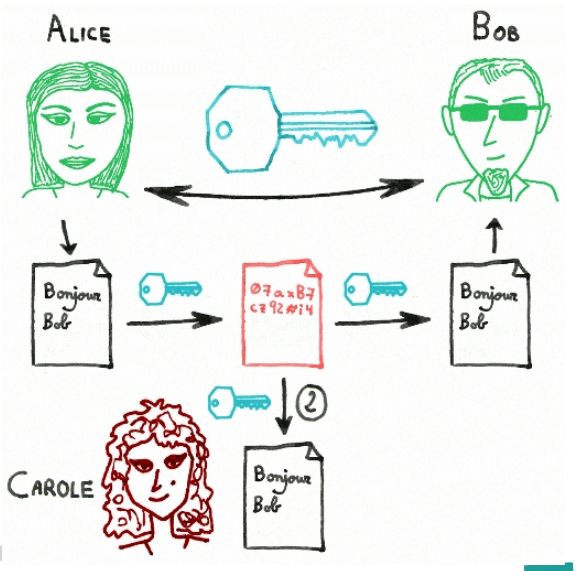
Symmetric Cryptography **#PROBLEM**



AES-256 ENCRYPTION

CESI alternance
ÉCOLE SUPÉRIEURE DES MÉTIERS

Symmetric Cryptography **#PROBLEM**



AES-256 ENCRYPTION

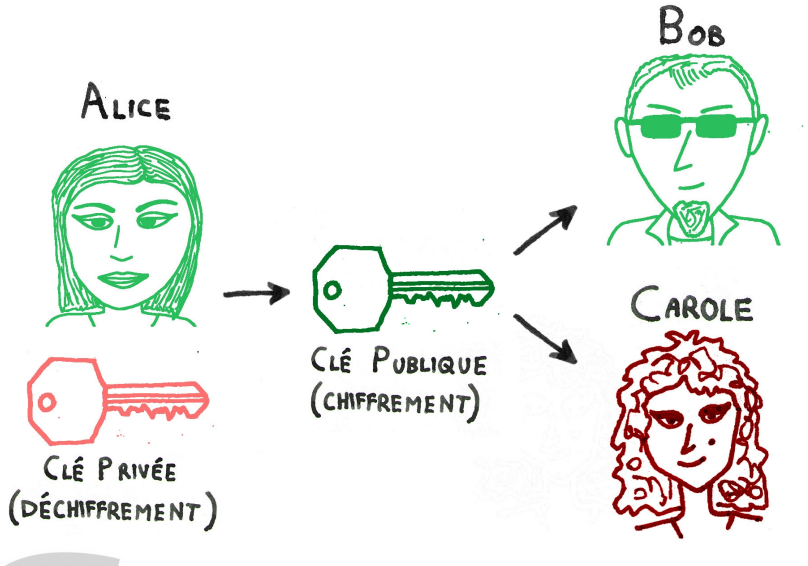
CESI alternance
ÉCOLE SUPÉRIEURE DES MÉTIERS

Asymmetric Cryptography

Keys are likes nuts... you must have two!

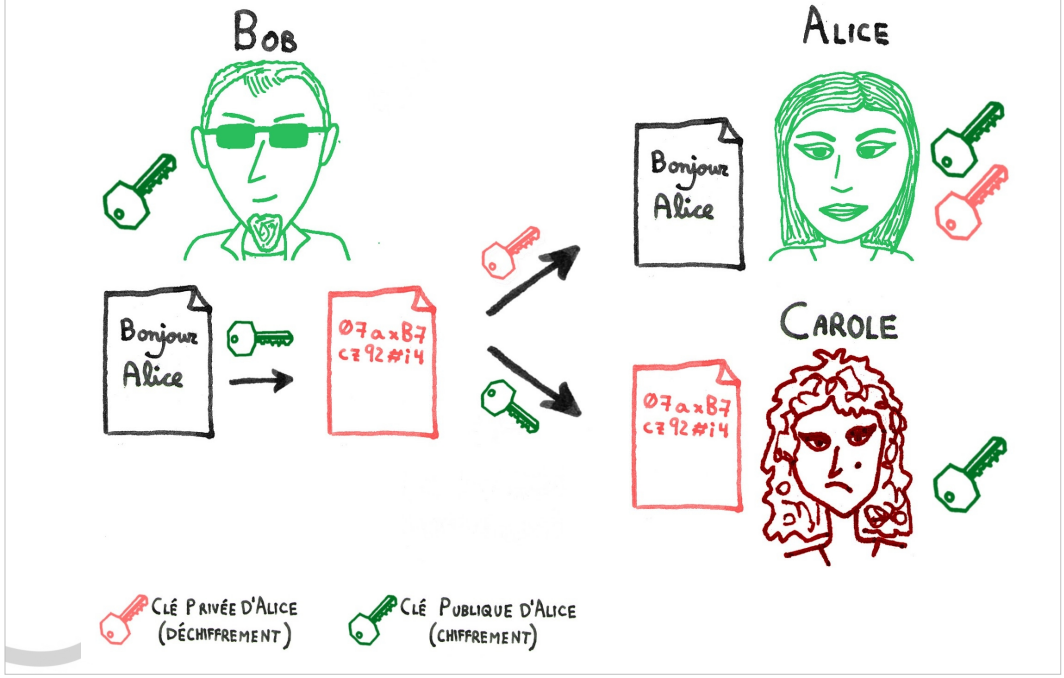
CESi alternance
ÉCOLE SUPÉRIEURE DES MÉTIERS

Asymmetric Cryptography



CESI alternance
ÉCOLE SUPÉRIEURE DES MÉTIERS

Asymmetric Cryptography

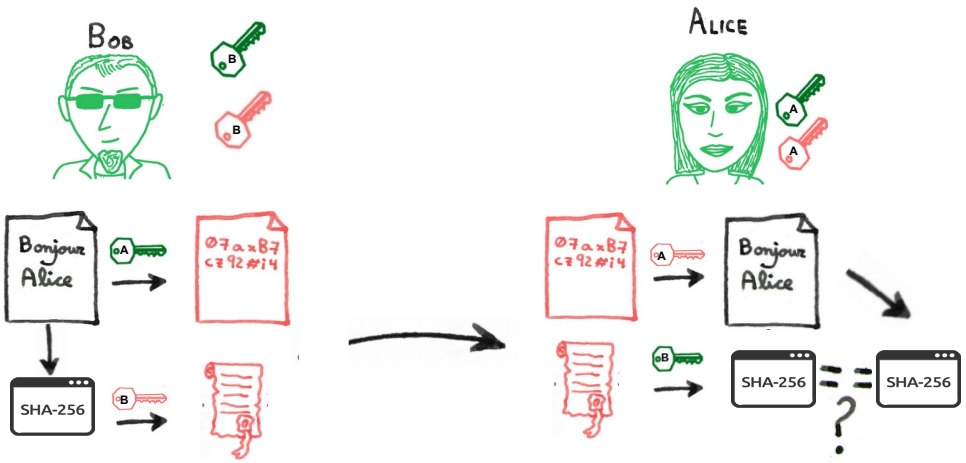


Asymmetric Cryptography

PK Ciphers are useless without an authentication system...

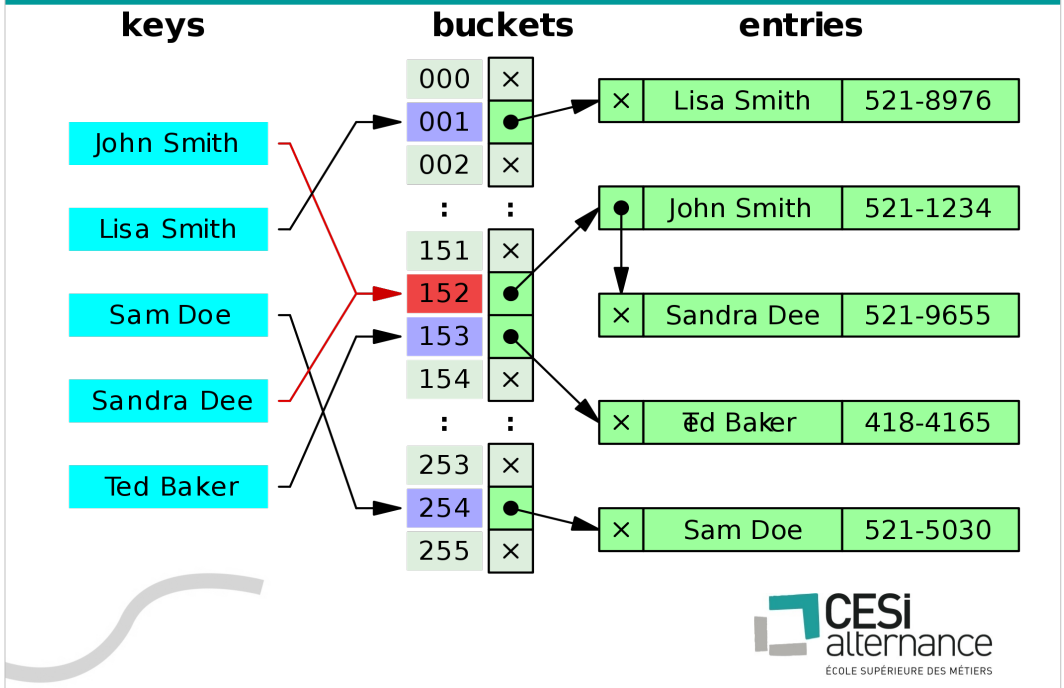
CESi alternance
ÉCOLE SUPÉRIEURE DES MÉTIERS

Asymmetric Cryptography



CESi alternance
ÉCOLE SUPÉRIEURE DES MÉTIERS

Hash functions

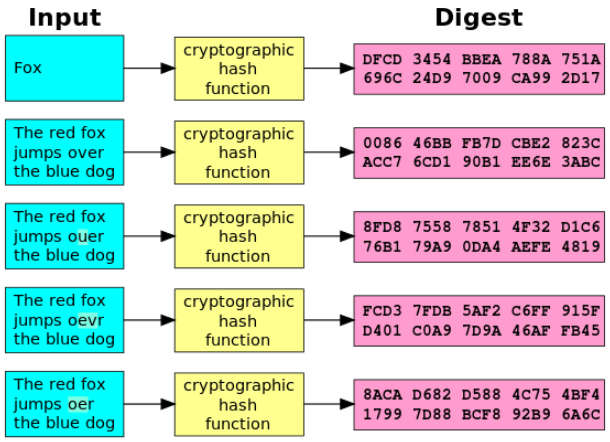


CESi alternance
ÉCOLE SUPÉRIEURE DES MÉTIERS

Cryptographic Hash functions

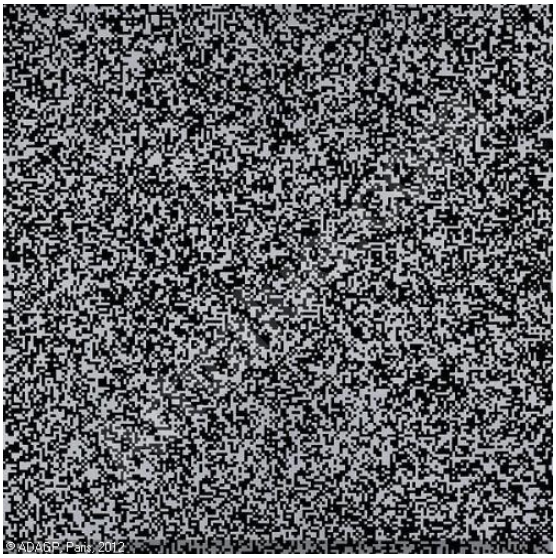
CESi alternance
ÉCOLE SUPÉRIEURE DES MÉTIERS

Cryptographic Hash functions



CESi alternance
ÉCOLE SUPÉRIEURE DES MÉTIERS

Cryptographic Hash functions

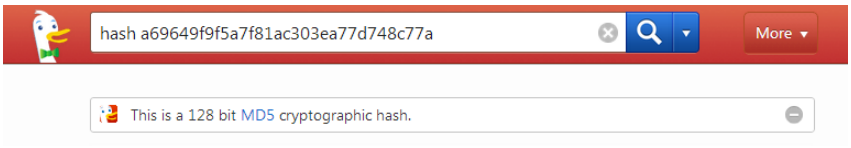


CESi alternance
ÉCOLE SUPÉRIEURE DES MÉTIERS

Cryptographic Hash functions

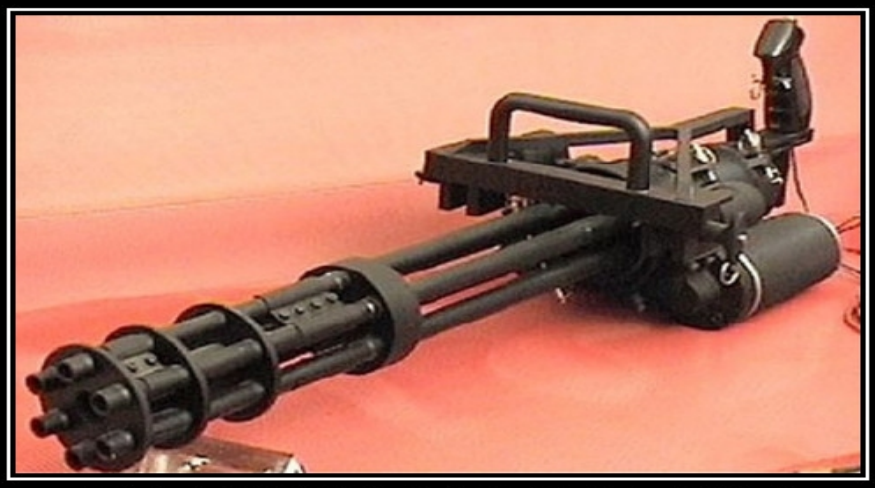
CESi alternance
ÉCOLE SUPÉRIEURE DES MÉTIERS

Cryptographic Hash functions



CESi alternance
ÉCOLE SUPÉRIEURE DES MÉTIERS

Cryptographic Hash functions

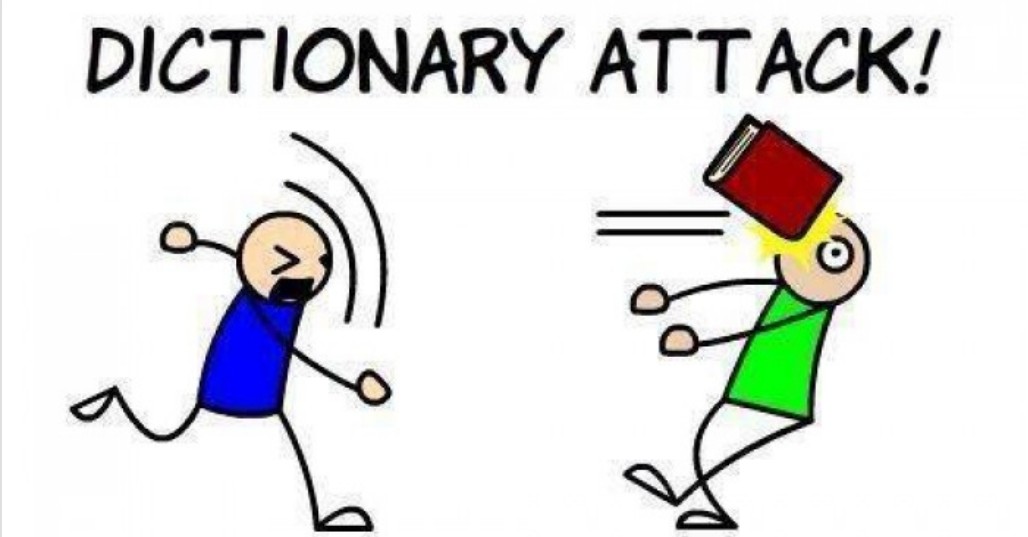


BRUTE FORCE

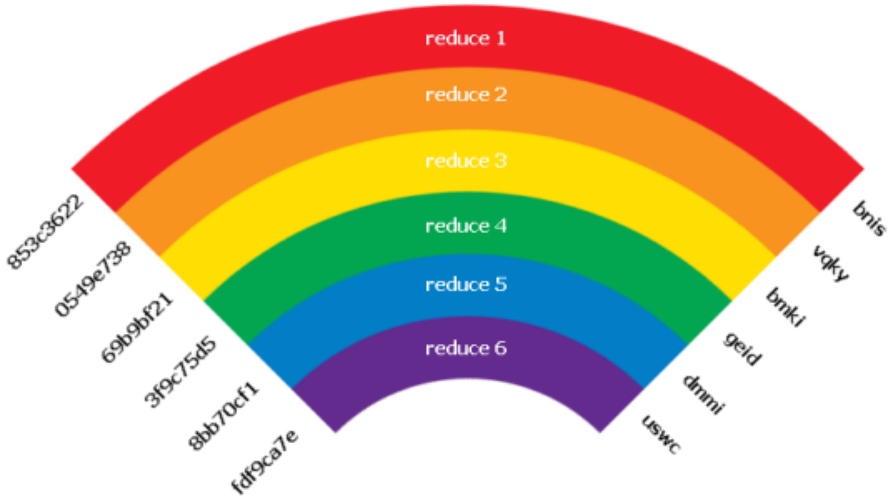
If it doesn't work, you're just not using enough.

fakeposters.com

Cryptographic Hash functions



Cryptographic Hash functions



CESi alternance
ÉCOLE SUPÉRIEURE DES MÉTIERS

Cryptographic Hash functions

1992 - **MD5** - 128 bits 

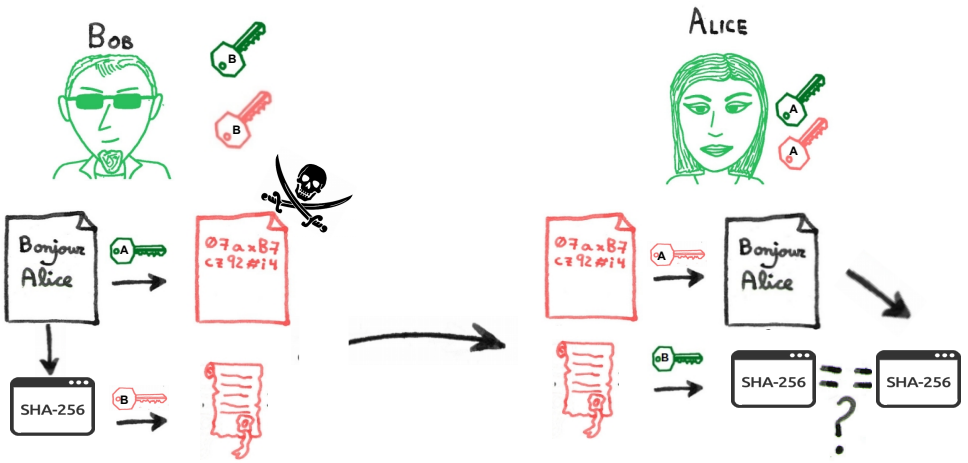
1995 (NSA) - **SHA-1** - 160 bits 

2001 (NSA) - **SHA-2** - 224,256,384 or 512 bits

2006 - **SHA-3** - arbitrary

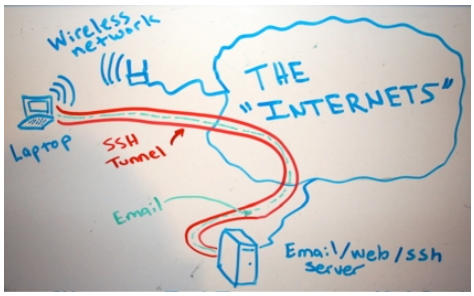
CESi alternance
ÉCOLE SUPÉRIEURE DES MÉTIERS

Asymmetric Cryptography



CESi alternance
ÉCOLE SUPÉRIEURE DES MÉTIERS

III. Secured communications



CESI alternance
ÉCOLE SUPÉRIEURE DES MÉTIERS

SSL (Secured Socket Layer) History

1994 - SSL 1.O designed but no developed

1995 - SSL 2.0 release

1996 - SSL 3.0 release

2011 - SSL 2.0 BANNED

2014 - Poodle attack breaks SSL 3.0

2015 - SSL 3.0 BANNED

CESi alternance
ÉCOLE SUPÉRIEURE DES MÉTIERS

TLS (transport Layer Security)

1999 TLS 1.0 upgrade of SSLv3

2006 – TLS 1.1

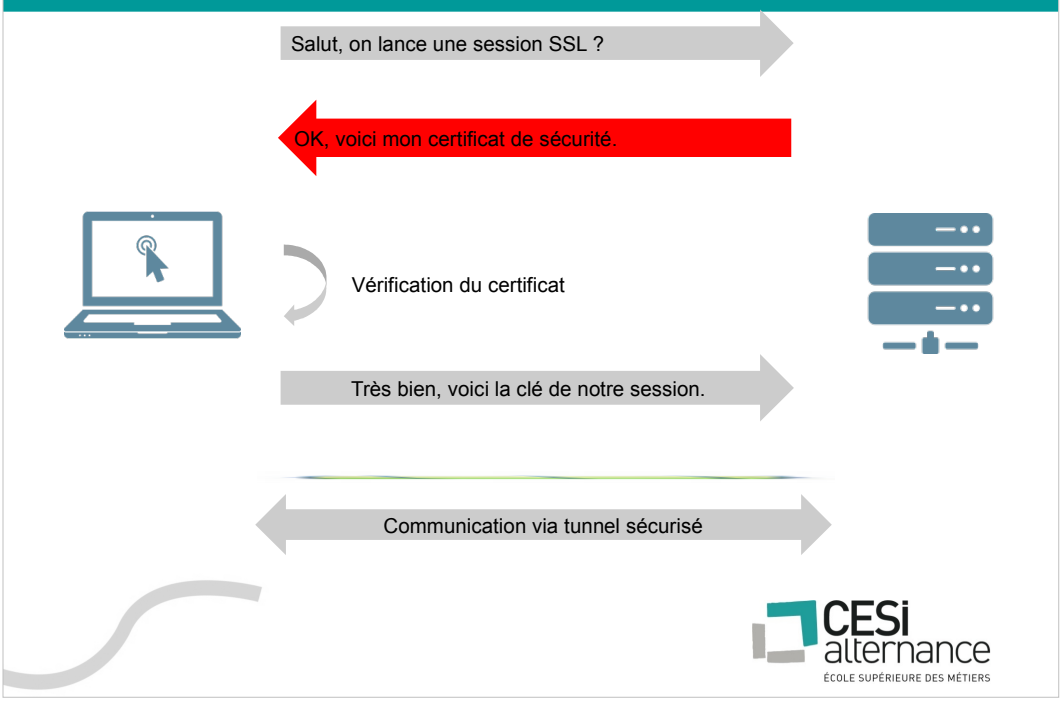
2006 – TLS 1.2 - MD5-SHA1 replaced by SHA-256

2011 – SSL backward compatibility removed

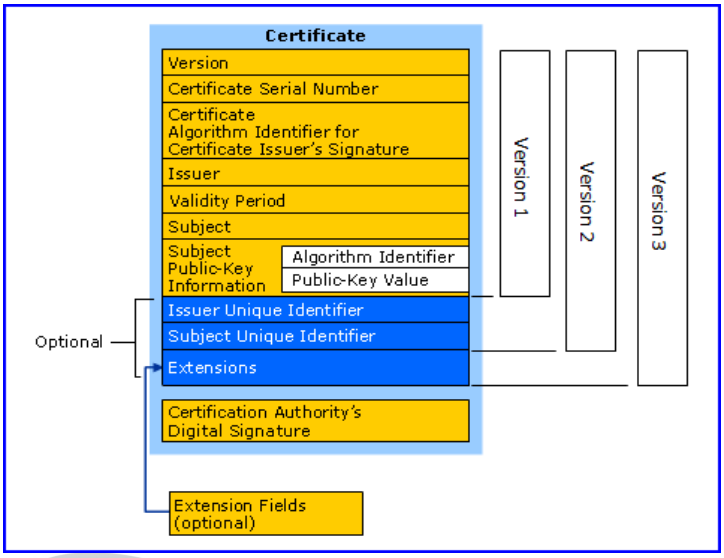
2014 – TLS 1.3 

CESi alternance
ÉCOLE SUPÉRIEURE DES MÉTIERS

TLS (transport Layer Security)

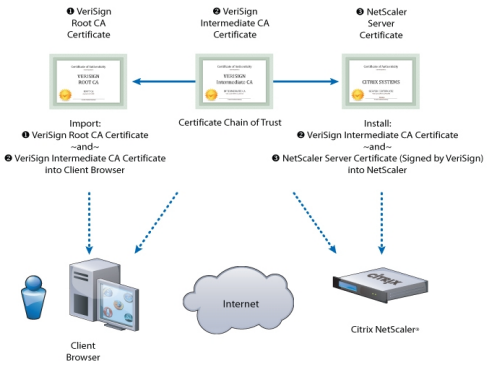


TLS Need Certificates...



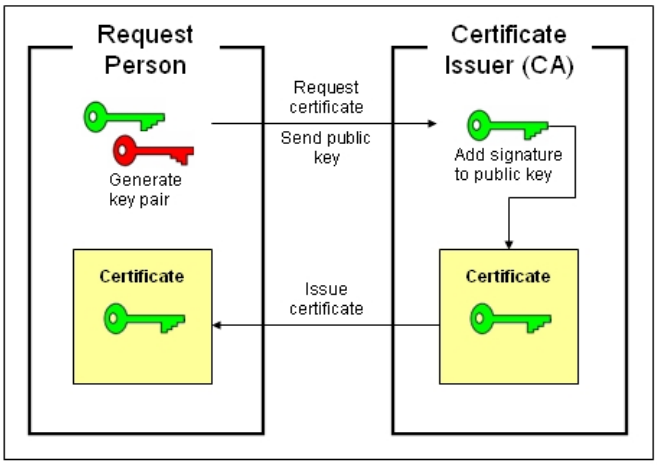
CESi alternance
ÉCOLE SUPÉRIEURE DES MÉTIERS

TLS Need Certificates... trusted



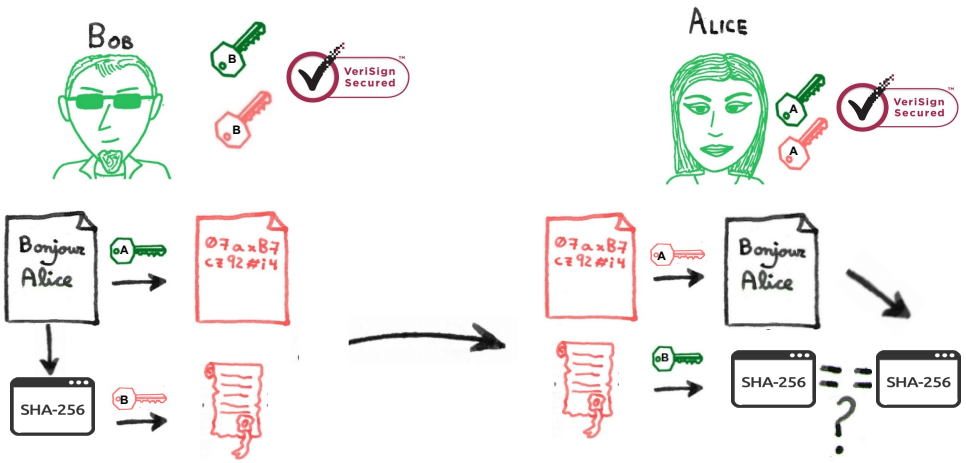
CESi alternance
ÉCOLE SUPÉRIEURE DES MÉTIERS

TLS Need Certificates... trusted



CESi alternance
ÉCOLE SUPÉRIEURE DES MÉTIERS

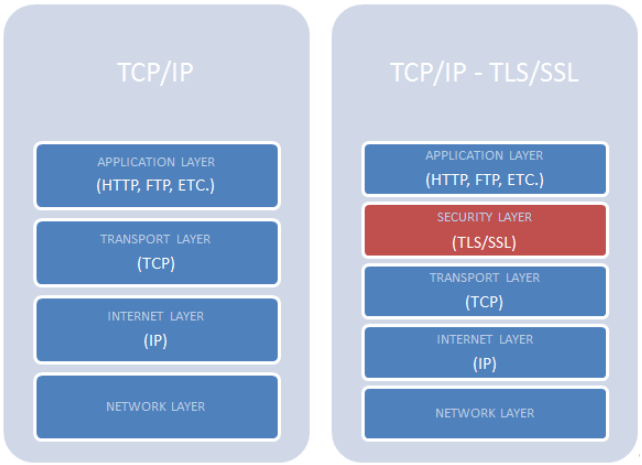
Asymmetric Cryptography



CESi alternance
ÉCOLE SUPÉRIEURE DES MÉTIERS

What is HTTPS ?

HTTP over TLS ;-)



CESi alternance
ÉCOLE SUPÉRIEURE DES MÉTIERS

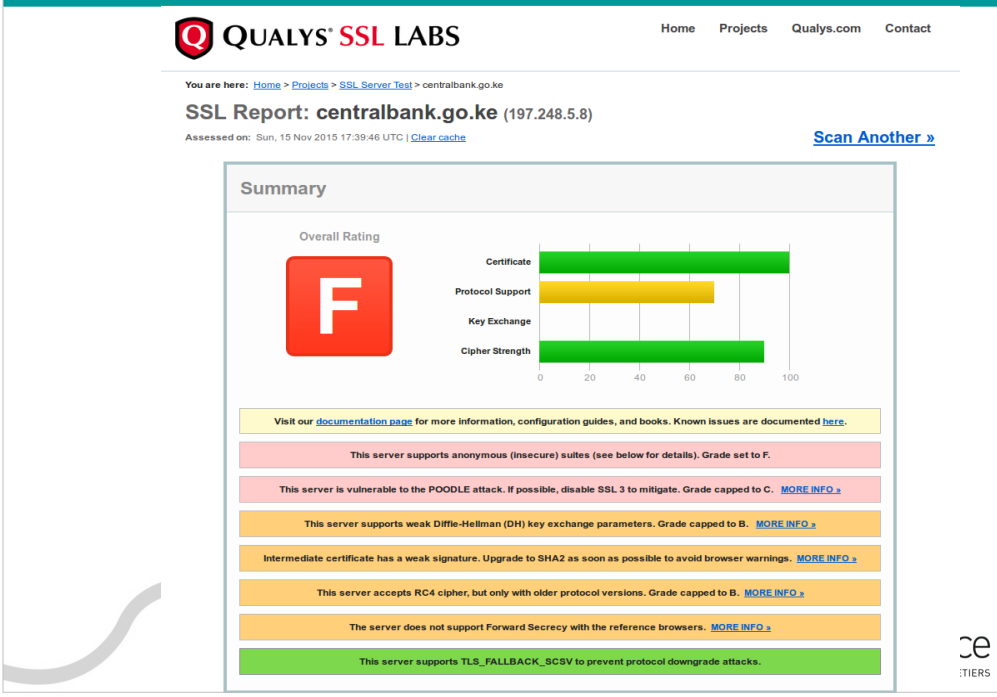
How used HTTPS is?

30.1% of the Internet have a

secure implementation of HTTPS

CESi alternance
ÉCOLE SUPÉRIEURE DES MÉTIERS

How Insecure internet is? **www.ssllabs.com**



TLS is not the only one...

CESi alternance
ÉCOLE SUPÉRIEURE DES MÉTIERS

SSH (Secure SHell)

Provide confidentiality and integrity of data over an unsecured network, such as the Internet

CESi alternance
ÉCOLE SUPÉRIEURE DES MÉTIERS

SSH (Secure SHell)

1995 – V1

1998 – unauthorized insertion of content into encrypted SSH stream

2006 – V2 RFC approved

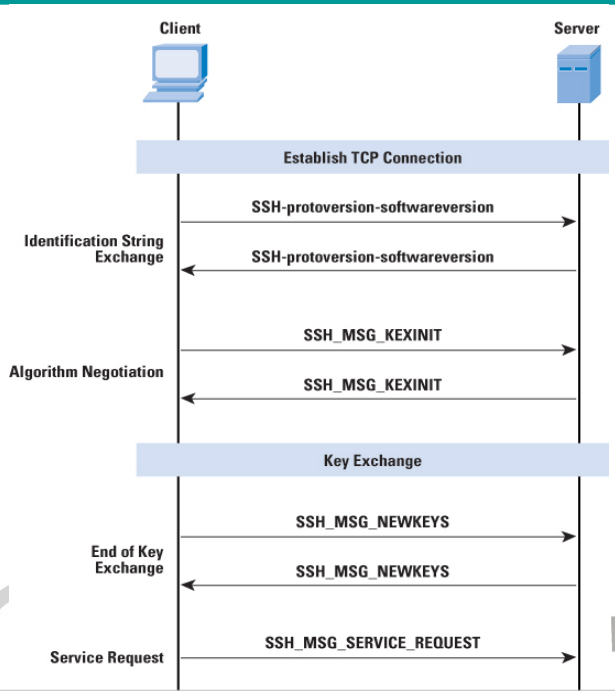
2007 – SSHv1 considered as obsolete

2008 – Theatrical vulnerability discovered

2014 – Snowden suggest that the NSA may able to decrypt some SSH traffic.

CESI alternance
ÉCOLE SUPÉRIEURE DES MÉTIERS

SSH (Secure SHell)

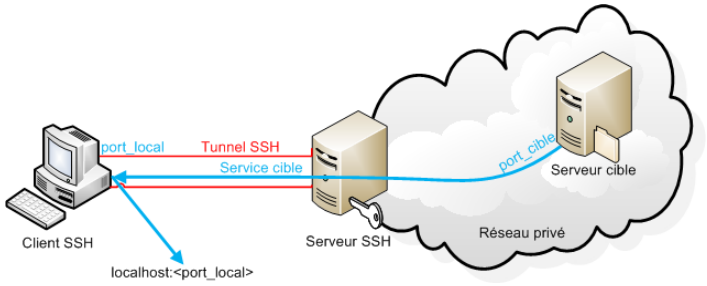


CESi alternance
ÉCOLE SUPÉRIEURE DES MÉTIERS

Tunneling

SSH (Secure SHell)

Expose only bastion servers



CESi alternance
ÉCOLE SUPÉRIEURE DES MÉTIERS

Crypto → Keys storage

CESi alternance
ÉCOLE SUPÉRIEURE DES MÉTIERS

Crypto → Keys storage

Bush “We don't torture, we baptize”

CESi alternance
ÉCOLE SUPÉRIEURE DES MÉTIERS

Crypto → Keys storage

Store keys in a secured key server

CESi alternance
ÉCOLE SUPÉRIEURE DES MÉTIERS

Crypto → Keys storage

The... classic (old school)

Classic - HSM – Works... but does not scale

→ Data center centric
→ Used by Banks & institutional companies
→ Proprietary techno

CESi alternance
ÉCOLE SUPÉRIEURE DES MÉTIERS

Crypto → Keys storage

The... most complete

→ Unified API
→ Access management & logs
→ Integrated in many OPS tools
→ OpenSource

CESi alternance
ÉCOLE SUPÉRIEURE DES MÉTIERS

Crypto → Keys storage

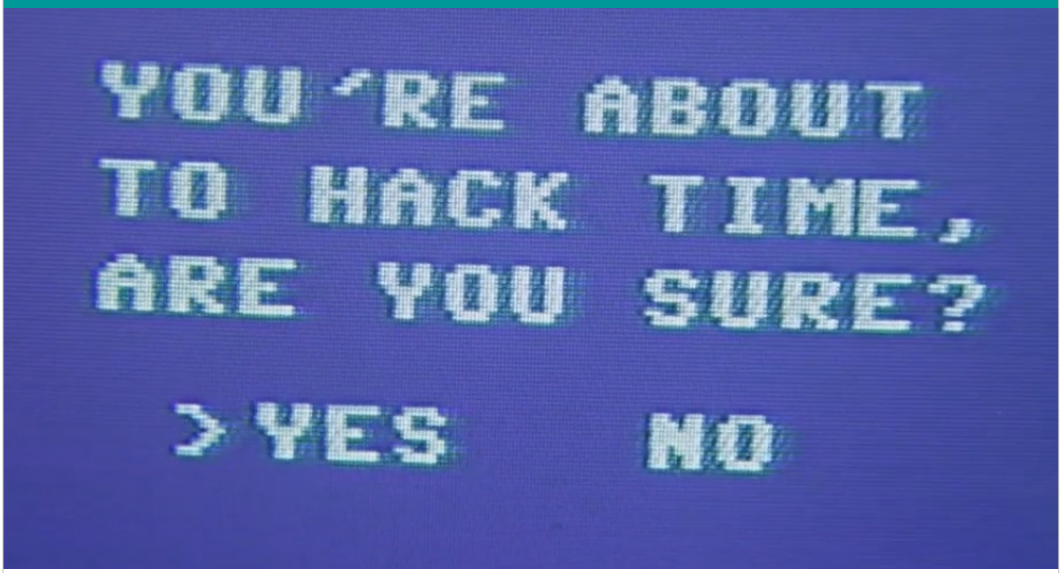
The... challenger

→ SSH centric
→ Low level
→ Use a Shamir's Sharing Secret
→ Made in Breizh
→ OpenSource

OSS (OpenSecretServer)

CESi alternance
ÉCOLE SUPÉRIEURE DES MÉTIERS

And now ?



CESi alternance
ÉCOLE SUPÉRIEURE DES MÉTIERS