

Sécurité

Sécurité des Systèmes d'Information
Concepts, Organisation, Outils et Tendances



Cryptologie et Applications

Sécurité des Systèmes d'Information
Concepts, Organisation, Outils et Tendances



Outline

- I. Introduction et définitions
- II. Chiffrement Symétrique
- III. Chiffrement Asymétrique
- IV. Fonction à sens unique
- V. PKI
- VI. Sécurité de l'Internet





Introduction et définition

- **Historique**
- Définitions et concepts
- Type de chiffrement
- Méthodes de chiffrement

La cryptologie

❑ Cryptographie

« Science permettant de créer des systèmes de chiffrement »

❑ Système de Chiffrement- Définition

« Opération de chiffrement qui transforme un texte en clair en un texte chiffré, appelé cryptogramme, au moyen d'une clé (qu'on dénomme la clé de chiffrement) »

❑ Cryptanalyse - Définition

« Science complémentaire qui consiste à déterminer certaines propriétés d'un système cryptographique dans le but de reconstituer le texte en clair, souvent en l'absence des paramètres qui sont nécessaires pour le déchiffrement »



Cryptologie – les origines

Secret: **111**

Système de chiffrement : +

Clé: **58**

User A



$$111 + 58$$

cryptogramme: **169**



User B



$$169 - 58 = 111$$

Cryptologie – les origines



Chiffrement
Hébraïque: Atbash
500 av JC
Méthode: Décalage alphabet

En clair	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
Chiffré	z	y	x	w	v	u	t	s	r	q	p	o	n	m	l	k	j	i	h	g	f	e	d	c	b	a

Chiffrement:
Substitution
mono alphabétique



Ancien testament ou la tanakh



Chiffrement Spartiate
400 av JC
Méthode: Utilisation d'un rondin de bois pour déchiffrer



Chiffrement:
introduction du principe de clé



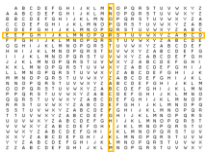
Chiffrement de César
2 av JC
Méthode: Décalage alphabet (3 positions)

En Clair	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
Chiffré	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

Chiffrement:
Substitution
mono alphabétique



Chiffrement de Blaise de Vigenere (pour Henri VIII)
1500
Méthode: Décalage alphabet (27 positions)



Chiffrement:
Substitution
polyalphabétique



Cryptologie – les origines



Chiffrement de Blaise de Vigenere (pour Henri VIII)

1500

Méthode: Décalage alphabet (27 positions)



Chiffrement:

Substitution polyalphabétique

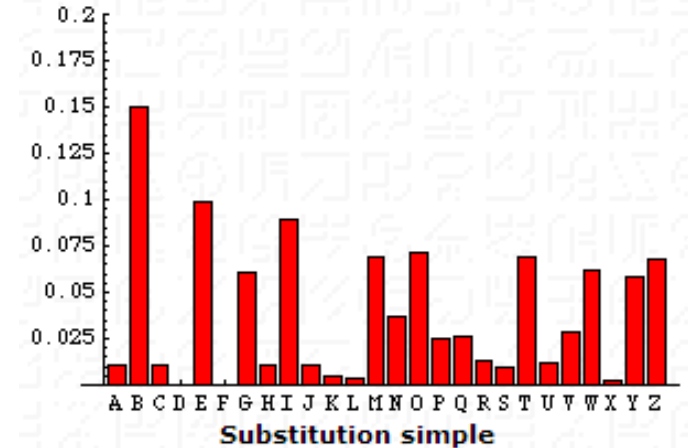


A	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z
B	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A
C	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B
D	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C
E	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D
F	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T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

Message=NOUS...

Clé=ETESTLA

Chiffre=RHYKG PSSFQ WLAAW LIMED



Cryptologie – les origines



Chiffrement
Hébraïque: Atbash
500 av JC
Méthode: Décalage alphabet

En clair: 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
Chiffre: z y x w v u t s r q p o n m l k j i h g f e d c b a

Chiffrement:
Substitution
mono alphabétique



Ancien testament ou la tanakh



Chiffrement Spartiate
400 av JC
Méthode: Utilisation d'un rondin de bois pour déchiffrer



Chiffrement:
introduction du principe de clé



Chiffrement de César
2 av JC
Méthode: Décalage alphabet (3 positions)

En clair: 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
Chiffre: 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

Chiffrement:
Substitution
mono alphabétique



Chiffrement de Blaise de Vigenere (pour Henri VIII)
1500
Méthode: Décalage alphabet (27 positions)

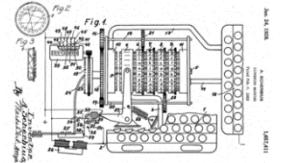
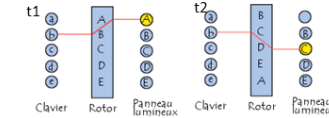


Chiffrement:
Substitution
polyalphabétique



The Enigma Machine
1939
Méthode: Machine électromécanique

Exemple avec 1 ROTOR



Chiffrement:
Substitution **polyalphabétique**





Introduction et définition

- Historique
- **Définitions et concepts**
- Type de chiffrement
- Méthodes de chiffrement

Cryptologie – les concepts

□ L'algorithme

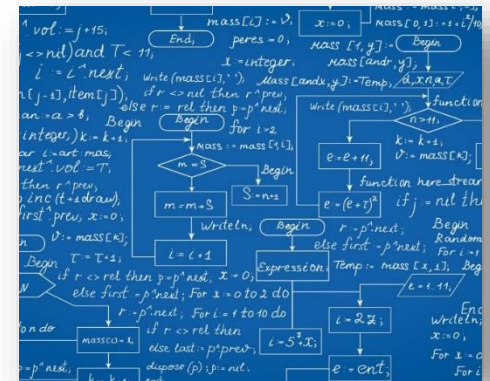
Ensemble des règles décrivant comment un message est chiffré et déchiffré.

- La plupart des algorithmes de chiffrement ne sont pas secrets.
- La partie secrète (de la plupart des algorithmes de chiffrement) est la clé

□ La clé

Clé ou cryptovariable peut être vue comme une valeur comprenant une grande séquence de bits aléatoires.

- Plus l'espace des possibles de la clé est grande
- Plus les valeurs des clés ont un caractère aléatoire
- plus la difficulté est grande pour un attaquant de trouver le secret



Cryptologie – les concepts

- Puissance d'un algorithme de chiffrement
 - Dépend de:
 - La méthode de chiffrement
 - La taille de la clé
 - Les vecteurs d'initialisation
 - La faculté de tous ces éléments à travailler ensemble

 - Est liée à
 - À La puissance
 - Aux ressources
 - Nécessaires pour casser le système de chiffrement



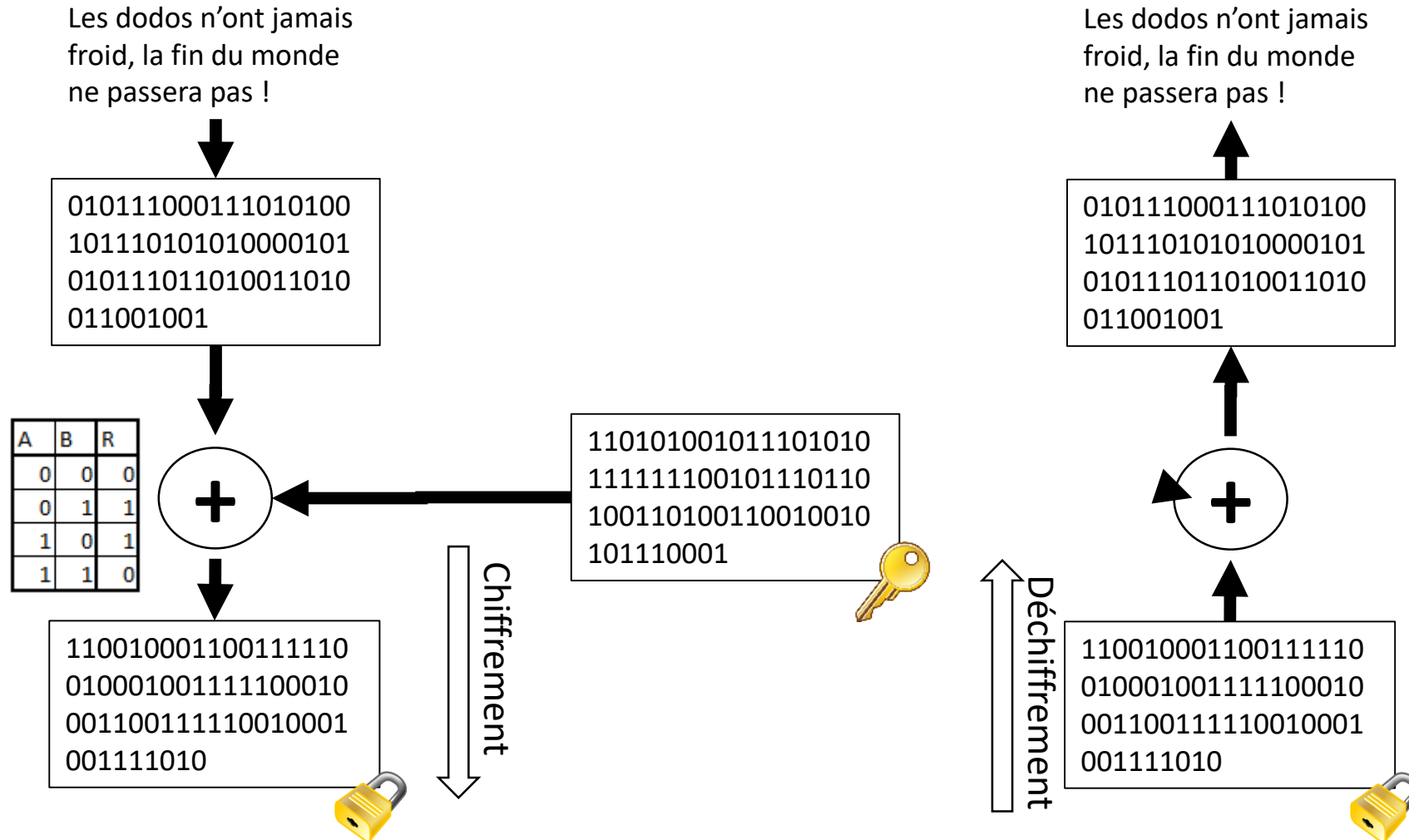
Cryptologie – les concepts

- One-Time Pad: la pierre philosophale
 - Chiffrement parfait, considéré comme incassable
 - Gilbert Vernam 1917 (chiffrement vernam)
 - Algorithme de chiffrement XOR (ou exclusif)

 - Pourquoi incassable?
 - La clé (pad) ne doit être utilisée qu'une seule fois
 - La clé (pad) doit être aussi longue que le message
 - La clé (pad) doit être distribuée de façon sécurisée avec le destinataire



Cryptologie – One-Time Pad



Cryptologie – One-Time Pad



Cryptologie – les concepts

□ Stéganographie

- Dissimuler un message dans un autre message
- Démarate, ancien roi de Sparte 485 BC

« il prit une tablette double, en gratta la cire, puis écrivit sur le bois même les projets de Xerxès ; ensuite il recouvrit de cire son message : ainsi le porteur d'une tablette vierge ne risquait pas d'ennuis. »



Cryptologie – Stéganographie



10101010 10101010

10101010 10**11011**

11101000 10**10011**

10000010 10**01111**

01111010 10**10001**

Information codée sur 16 bits
Poids fort à gauche

Remplacer l'info de
poids faible par
message secret

Reconstitution du
message secret

Cryptologie – Pourquoi

- Assurer les services de sécurité suivants:
 - Confidentialité
 - Intégrité
 - Authentification
 - Autorisation
 - Non répudiation





Introduction et définition

- Historique
- Définitions et concepts
- **Type de chiffrement**
- Méthodes de chiffrement

Cryptologie – Type de chiffrement

□ Substitution

La substitution remplace des bits, des caractères ou des blocs de caractères avec d'autres bits, caractères ou blocs de caractères

- Effet d'une substitution = **confusion**

□ Transposition

La transposition ne remplace pas les informations d'un message, mais déplace les informations (bits, caractères, blocs de caractères) du message original dans ce dernier

- Effet d'une transposition = **diffusion**

□ Transposition simples

- sensibles à l'analyse fréquentielle → **utiliser à la fois la substitution et la transposition**



Cryptologie – Type de chiffrement

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

GRAY FOX HAS ARRIVED
UKQN YGB IQL QKKOCTR

Transposition Cipher

1	2	3	4	5	6	7	8	9
↓ ↓ ↓ ↓ ↓ ↓ ↓ ↓ ↓								
2	1	5	3	4	6	8	9	7

T O P S E C R E T
O T E P S C E T R

Cryptologie – Type de chiffrement

Chiffrement par bloc

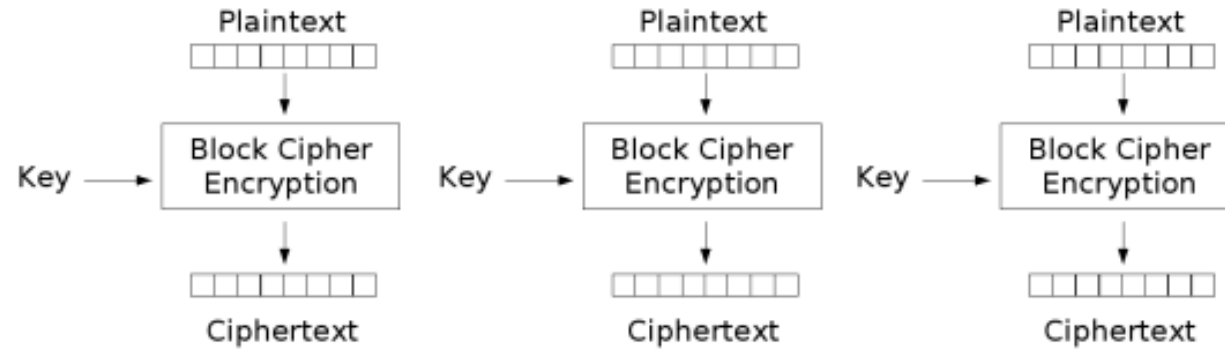
Le chiffrement par bloc, utilisé pour le chiffrement et le déchiffrement, divise le message en blocs de bits puis chiffre / déchiffre ces blocs les uns après les autres

Chiffrement par flux

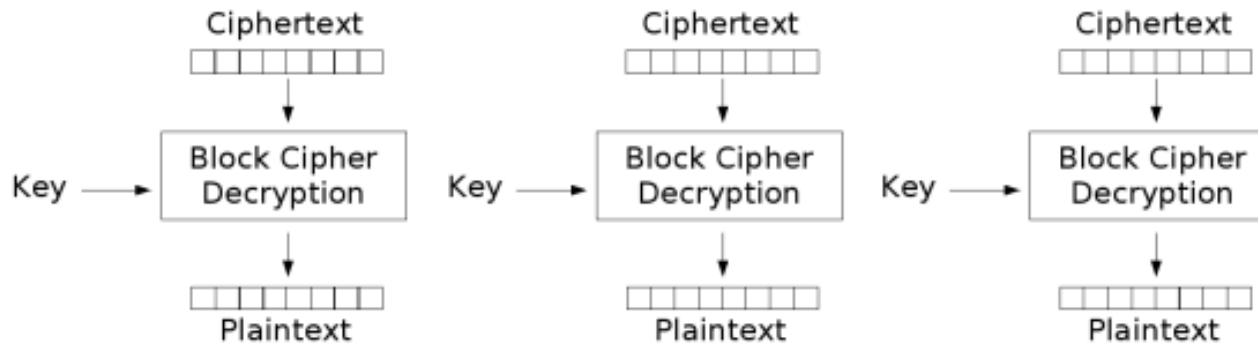
Le chiffrement traite le message comme un flux et chaque bit du message original est chiffré (fonction mathématique)



Cryptologie – Chiffrement par blocs



Electronic Codebook (ECB) mode encryption



Electronic Codebook (ECB) mode decryption

http://en.wikipedia.org/wiki/Block_cipher_modes_of_operation

Copyright © Jacques Saraydaryan

Cryptologie – Chiffrement par blocs

- Chiffrement par bloc
 - Chaque bloc est chiffré indépendamment
 - Notation $C=E(P,K)$
 - Pour un ensemble de message P_0, P_1, P_m

Chiffrement

$$C_0=E(P_0, K)$$

$$C_1=E(P_1, K)$$

$$C_2=E(P_2, K)$$

Déchiffrement

$$P_0=D(C_0, K)$$

$$P_1=D(C_1, K)$$

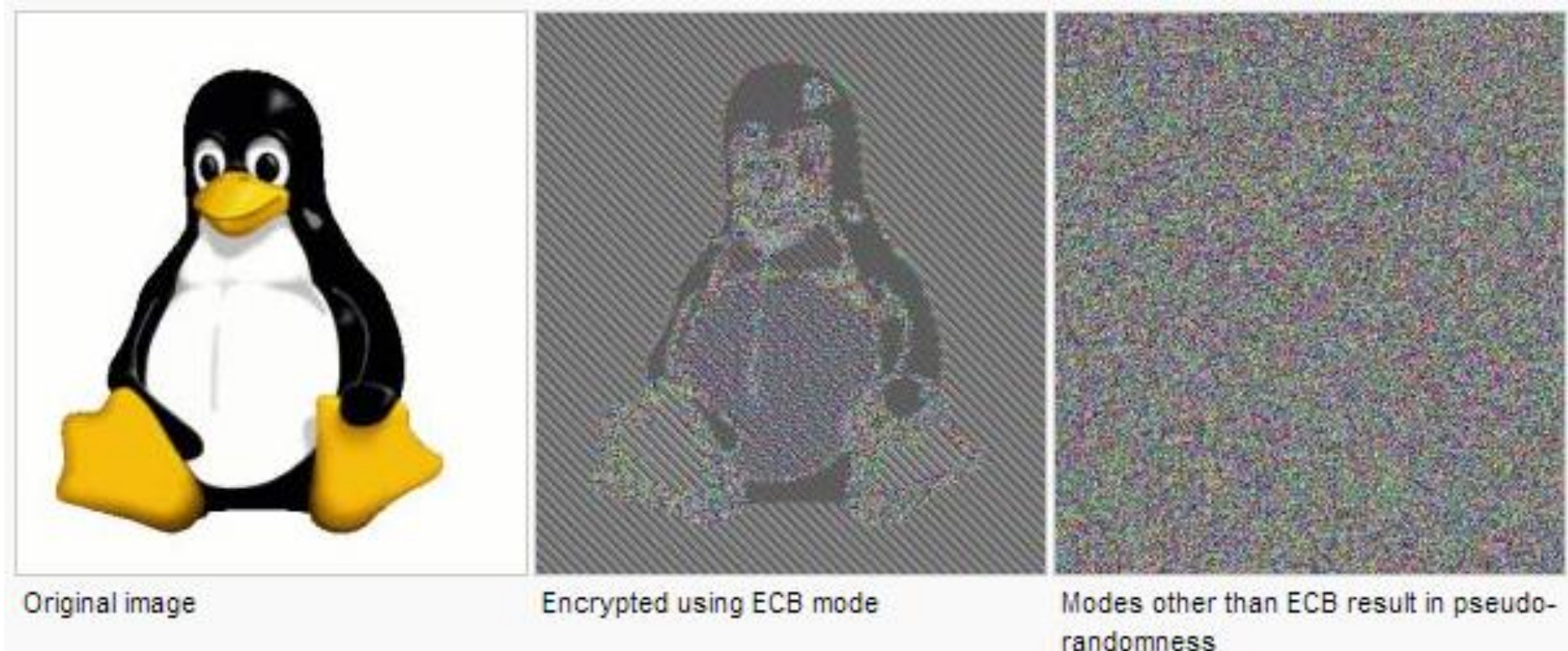
$$P_2=D(C_2, K)$$

Mêmes blocs de messages sont chiffrés de la même façon

→ **Divulgateion d'information perte de confidentialité**



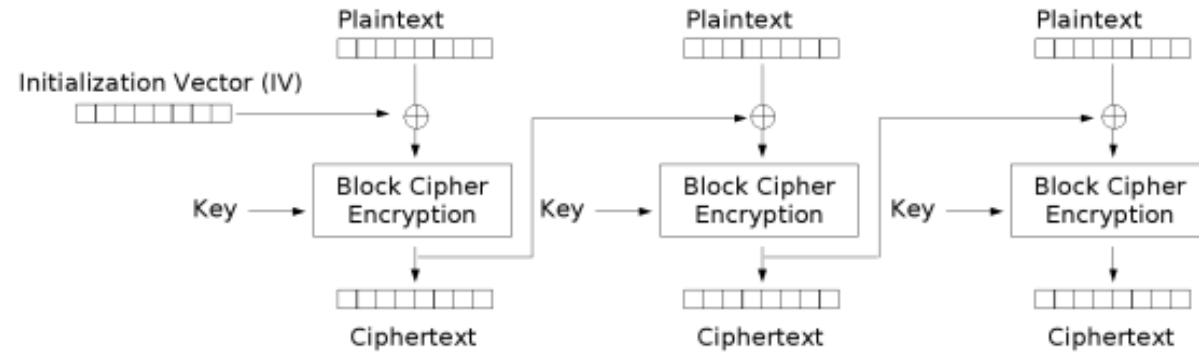
Cryptologie – Chiffrement par blocs



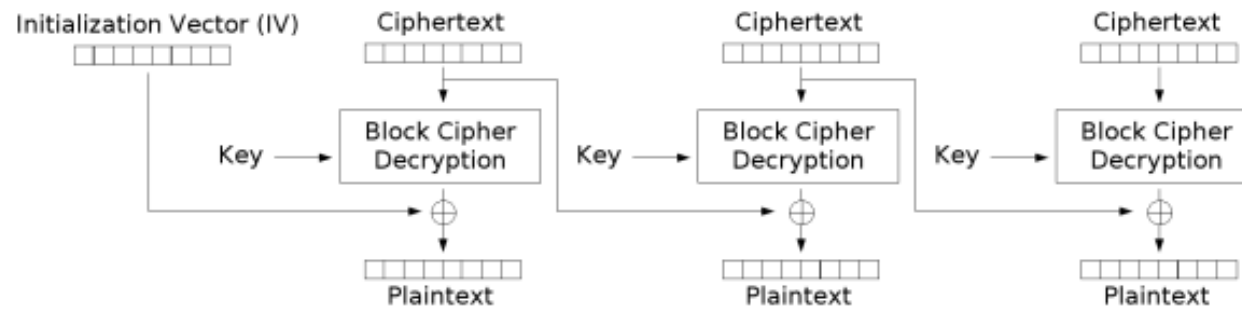
http://en.wikipedia.org/wiki/Block_cipher_modes_of_operation

Copyright © Jacques Saraydaryan

Cryptologie – Chiffrement par blocs



Cipher Block Chaining (CBC) mode encryption



Cipher Block Chaining (CBC) mode decryption

Cryptologie – Chiffrement par blocs

□ Chiffrement par bloc

- Blocs sont chaînés entre eux
- Utilisation d'un vecteur d'initialisation (VI) pour initialiser
- VI aléatoire mais pas nécessairement secret

Chiffrement

$$C_0 = E(IV \oplus P_0, K)$$

$$C_1 = E(C_0 \oplus P_1, K)$$

$$C_2 = E(C_1 \oplus P_2, K)$$

Déchiffrement

$$P_0 = VI \oplus D(C_0, K)$$

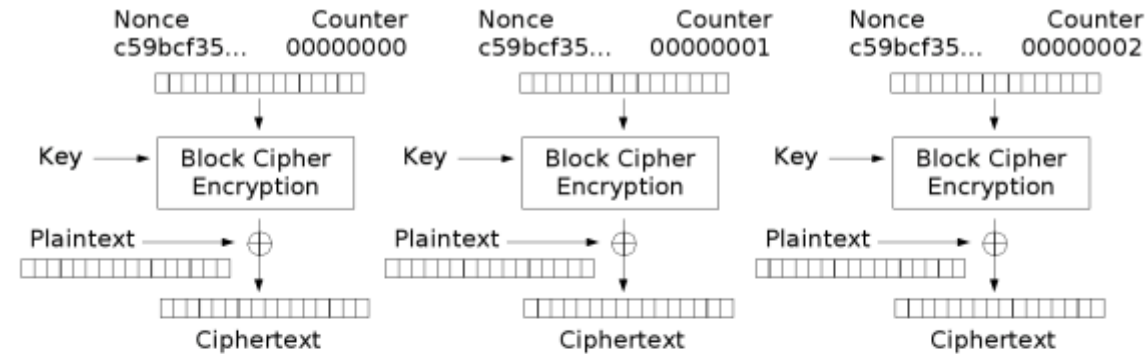
$$P_1 = C_0 \oplus D(C_1, K)$$

$$P_2 = C_1 \oplus D(C_2, K)$$

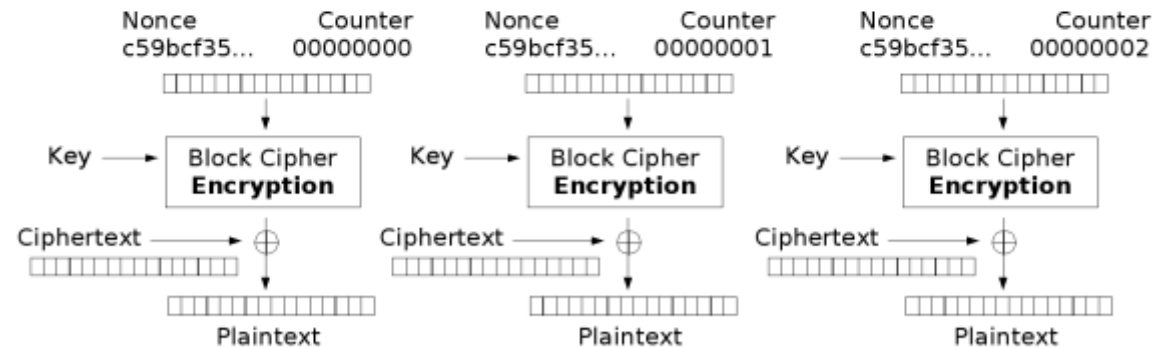
- Chiffrement séquentiel -> **lenteur**
- Découpage du message en multiple de la taille des blocs chiffrés



Cryptologie – Chiffrement par blocs



Counter (CTR) mode encryption



Counter (CTR) mode decryption

Cryptologie – Chiffrement par blocs

□ Chiffrement par bloc

- Utilise le chiffrement par bloc comme un chiffrement par flux
- Peut être utilisé pour des accès aléatoires

Chiffrement

$$C_0 = P_0 \oplus E(VI, K)$$

$$C_1 = P_1 \oplus E(VI+1, K)$$

$$C_2 = P_2 \oplus E(VI+2, K)$$

Déchiffrement

$$P_0 = C_0 \oplus E(VI, K)$$

$$P_1 = C_1 \oplus E(VI+1, K)$$

$$P_2 = C_2 \oplus E(VI+2, K)$$

- Chiffrement en parallèle possible

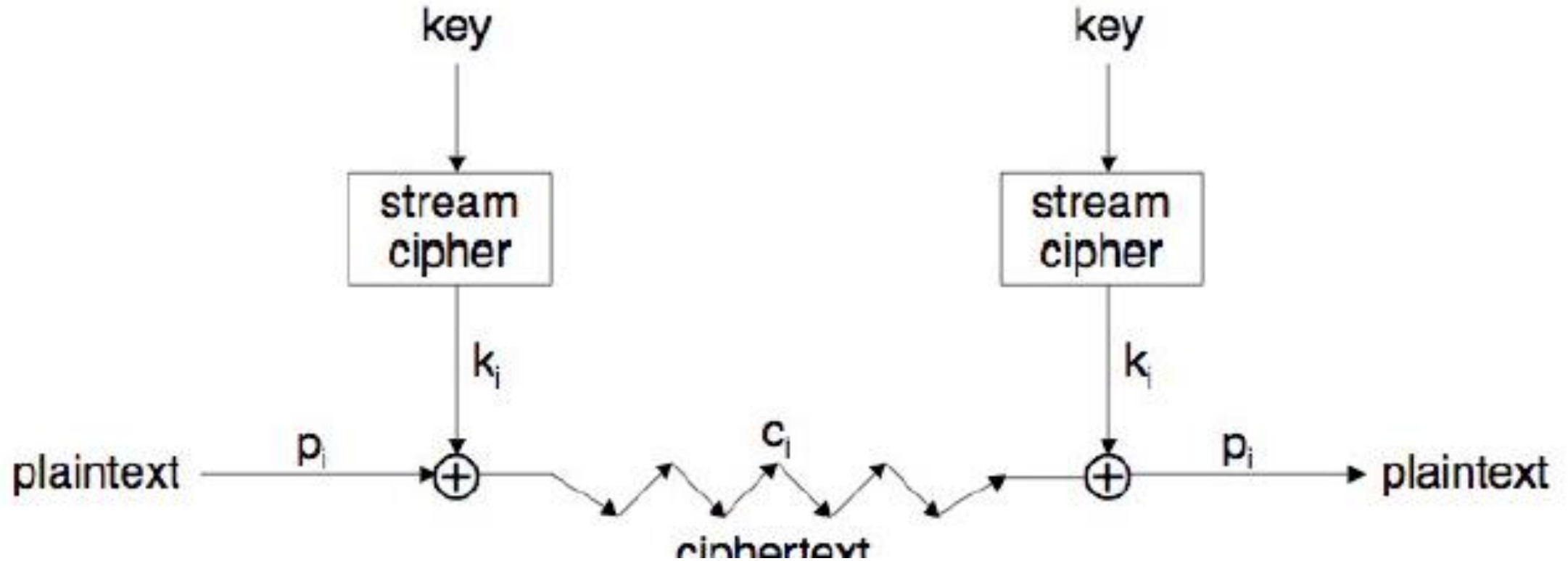


Cryptologie – Chiffrement par flux

- ❑ Généralisation de l'idée du one-time pad
- ❑ Initialisé avec une clé courte
- ❑ Clé est transformée en un keystream
- ❑ XOR pour le chiffrement et le déchiffrement



Cryptologie – Chiffrement par flux



Cryptologie – Chiffrement par flux

□ Décalage de registre

- Chiffrement par flux largement basé sur le décalage de registre
- Contient une boucle de rétroaction (feedback)
- Utilisation de fonction de rétroaction linéaire ou non

(Linear Feedback Shift register)



Cryptologie – Chiffrement par flux e.g RC4

Clef secrète K , composée de k mots de n bits, $K[0], \dots, K[k-1]$.

T tableau temporaire

S tableau de valeurs

$|K|$ taille du vecteur K

Initialisation.

Pour i de 0 à 255,

$S[i] \leftarrow i$

$T[i] = K[i \bmod (|K|)]$

$j = 0$

Pour $i = 0$ à 255 faire

$j \leftarrow (j + S[i] + T[i]) \bmod 256$

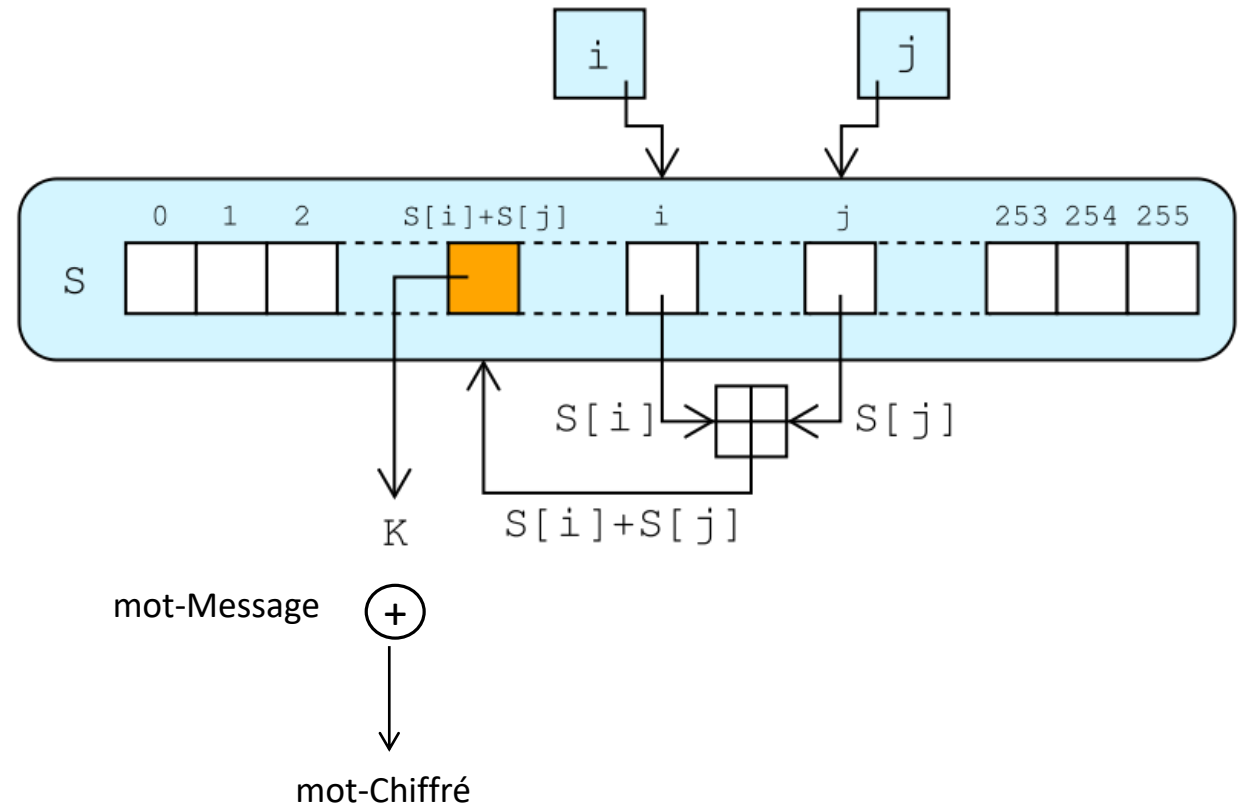
échanger $S[i]$ et $S[j]$

Génération de la suite chiffrante.

$i = j = 0$

• Répéter

- $i \leftarrow (i+1) \bmod 256$
- $j \leftarrow (j+S[i]) \bmod 256$
- échanger $S[i]$ et $S[j]$.
- Retourner $S[S[i] + S[j]]$ (sous clé)



Cryptologie – Chiffrement par flux

☐ Avantages

- Très rapide
- Adapté aux applications temps réelles

☐ Inconvénients

- Propagation d'erreurs (problème de synchronisation)
- Sécurité difficile à atteindre (pas de preuve)





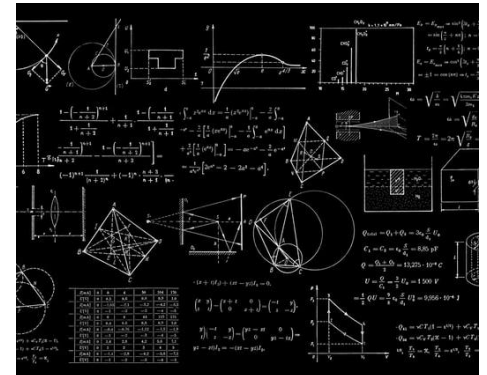
Introduction et définition

- Historique
- Définitions et concepts
- Type de chiffrement
- **Méthodes de chiffrement**

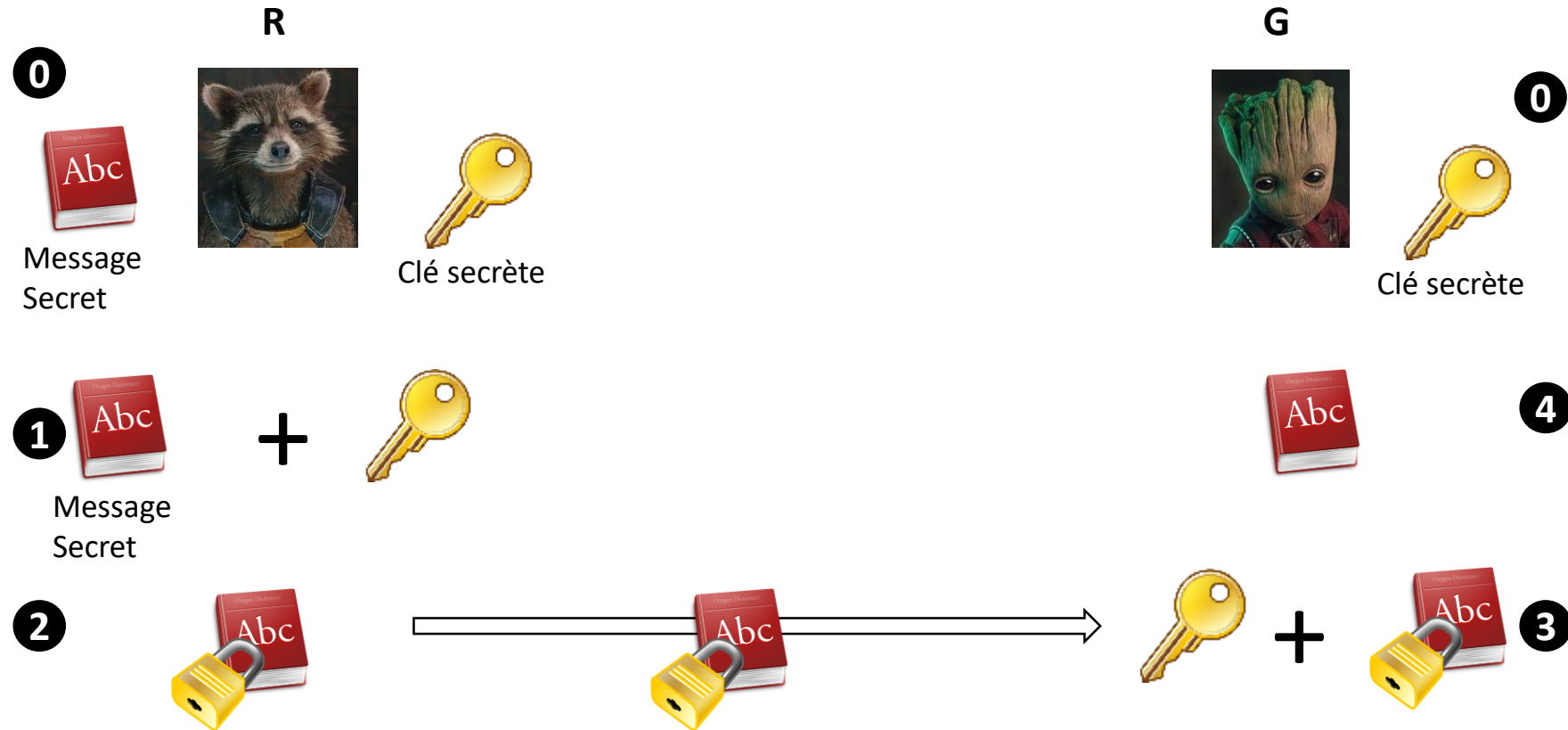
Cryptologie – Méthodes de chiffrement

- Symétrique
 - Secret partagé (clé symétrique)

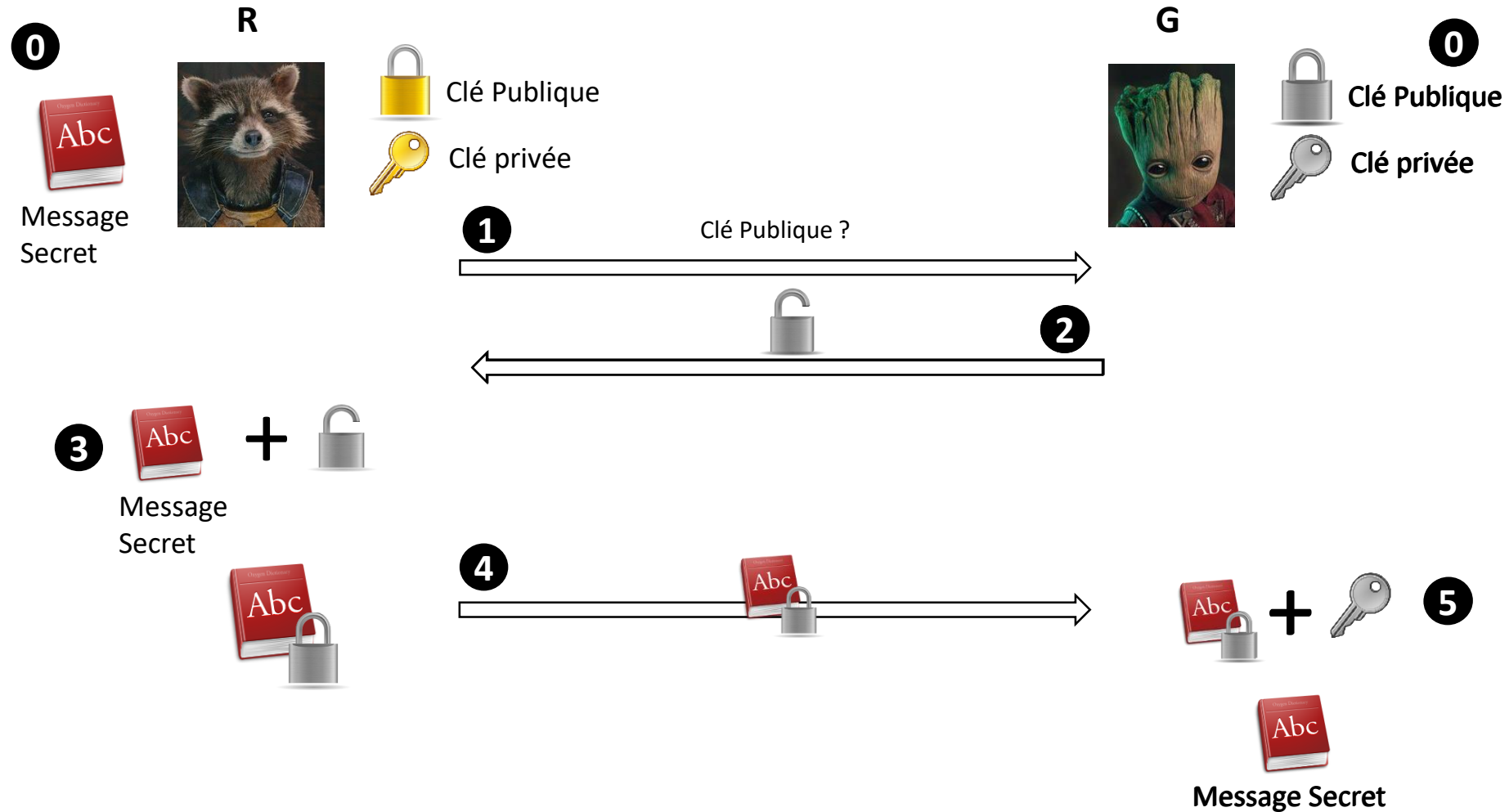
- Asymétrique
 - Utilisation de clé publique et clé privée



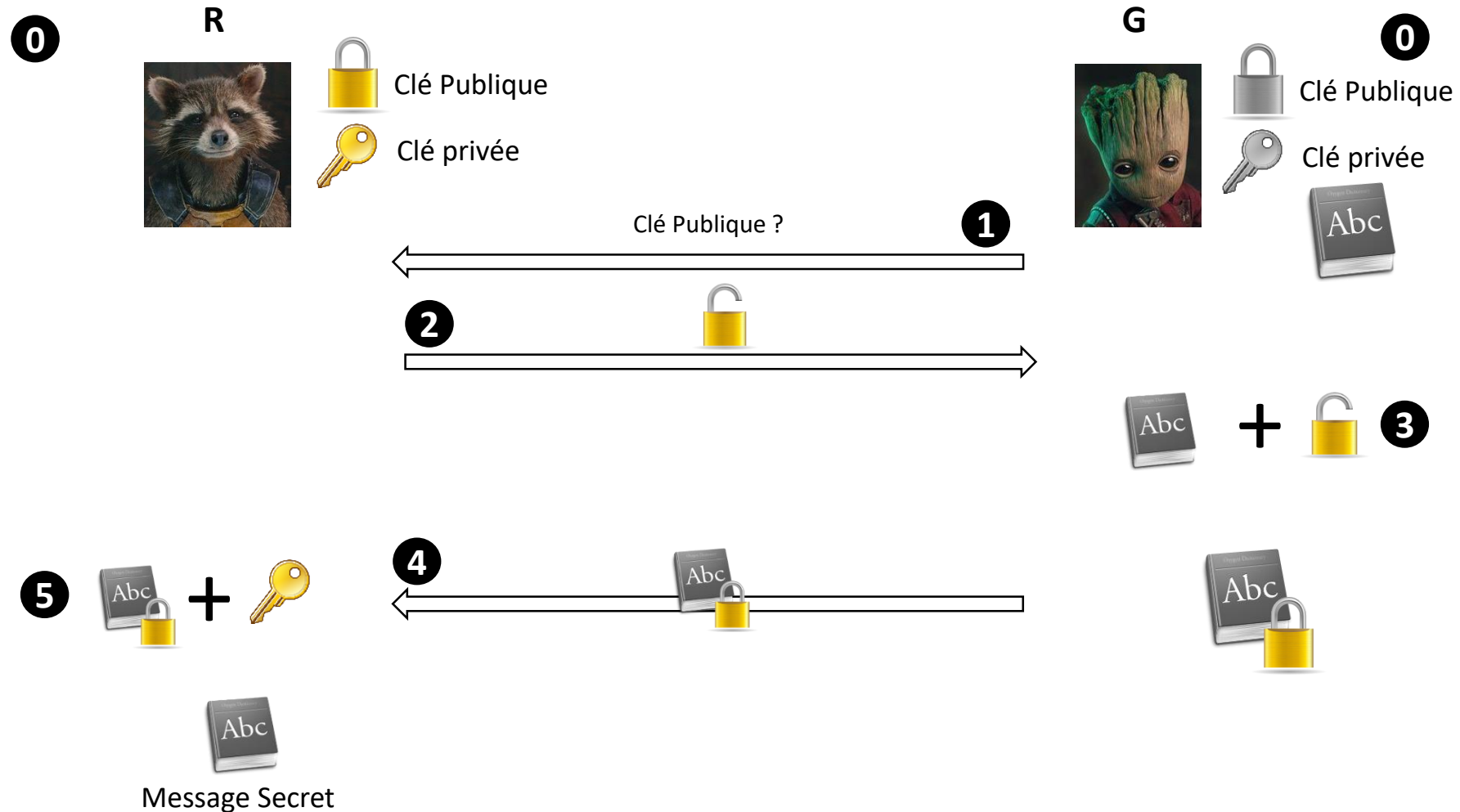
Cryptologie – Chiffrement symétrique



Cryptologie – Chiffrement asymétrique



Cryptologie – Chiffrement asymétrique



Cryptologie – Chiffrement asymétrique à vous de jouer

R



G



M



G a besoin de récupérer des informations de **R** pour les transmettre à **M**

Cryptologie – Méthodes de chiffrement

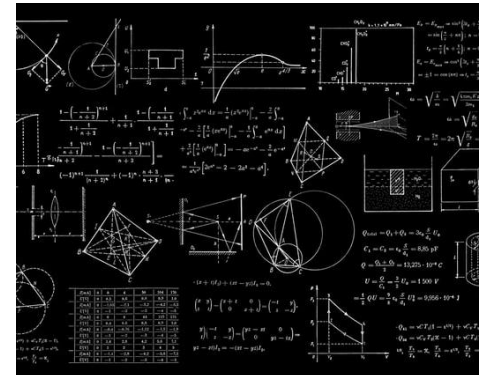
□ Symétrique

▪ Avantages

- Plus rapide que les chiffrements asymétriques
- Difficile à casser si grande taille de clé

▪ Inconvénients

- Demande un mécanisme permettant de délivrer les clés
- Chaque pair d'utilisateur à besoin d'une clé unique, problème de management des clés
- Garantit la confidentialité mais pas l'authenticité et la non répudiation



Cryptologie – Méthodes de chiffrement

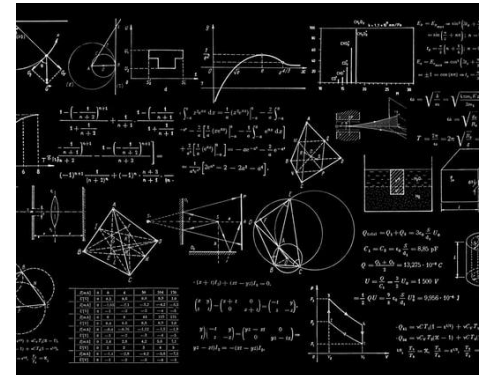
□ Asymétrique

▪ Avantages

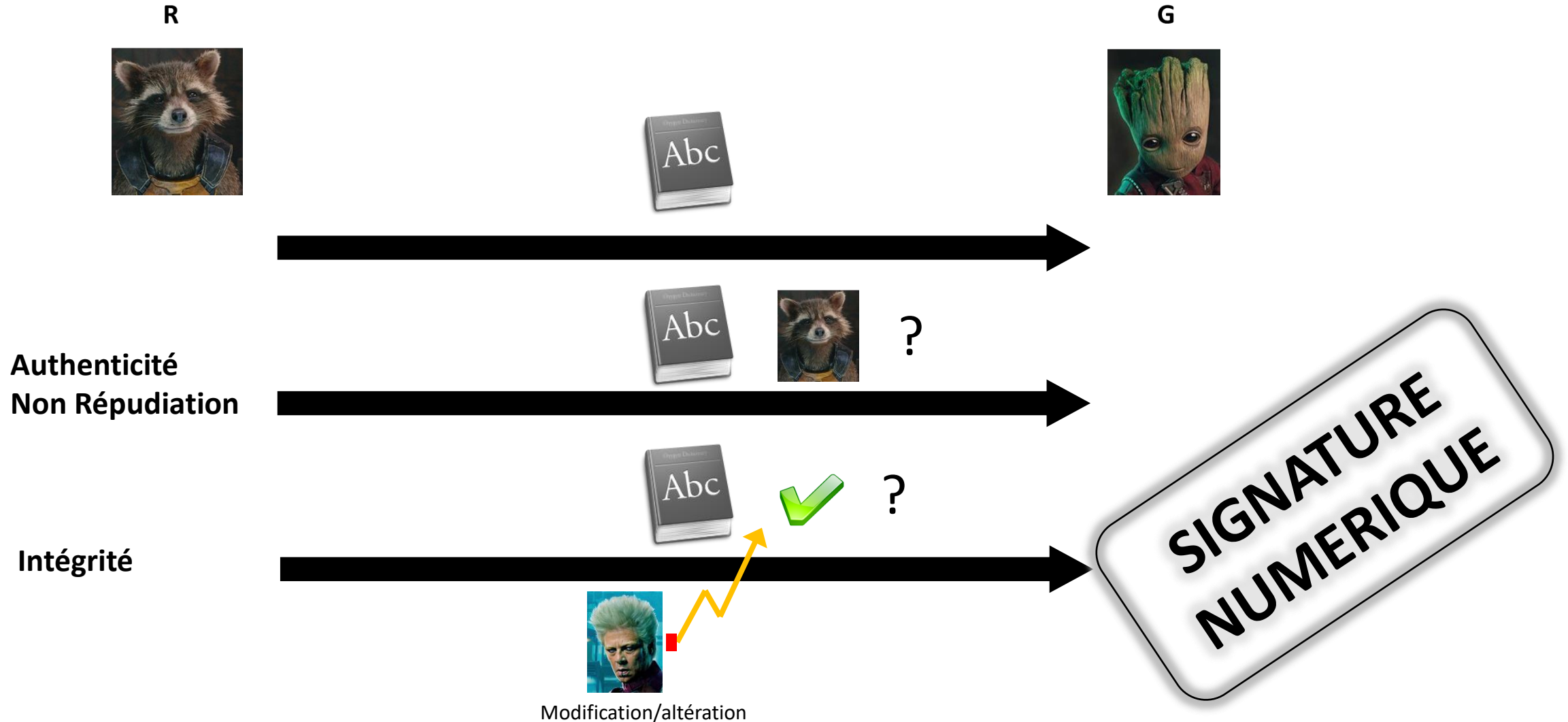
- Distribution des clés plus facile
- Meilleur passage à l'échelle
- Garantit la confidentialité mais aussi l'authenticité et la non répudiation

▪ Inconvénients

- Bien plus lent que le chiffrement symétrique
- Demande beaucoup de ressources (calcul mathématique complexe)



Cryptologie – Chiffrement asymétrique



R



G



?

Authenticité
Non Répudiation



?

Intégrité



Modification/altération



Cryptologie – Chiffrement asymétrique

R



Clé Publique



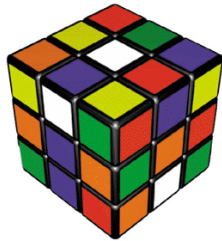
Clé privée



+



HASH



+



Clé Privée de R

Alison Richard



Document signé numériquement par R

Signature numérique

Cryptologie – Chiffrement asymétrique

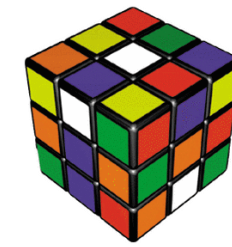
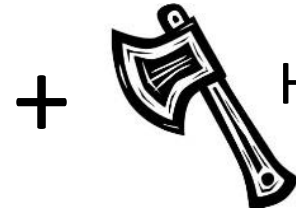
G



Clé Publique

Clé privée

Vérification
Signature numérique



Document signé numériquement par R



Clé Publique de R

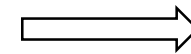
Identique ?

Cryptologie – Chiffrement asymétrique



Je **chiffre** avec une **clé publique**:

Seules les personnes possédant la clé privée associée peuvent lire le message

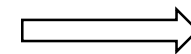


Confidentialité



Je **chiffre** avec une **clé privée**:

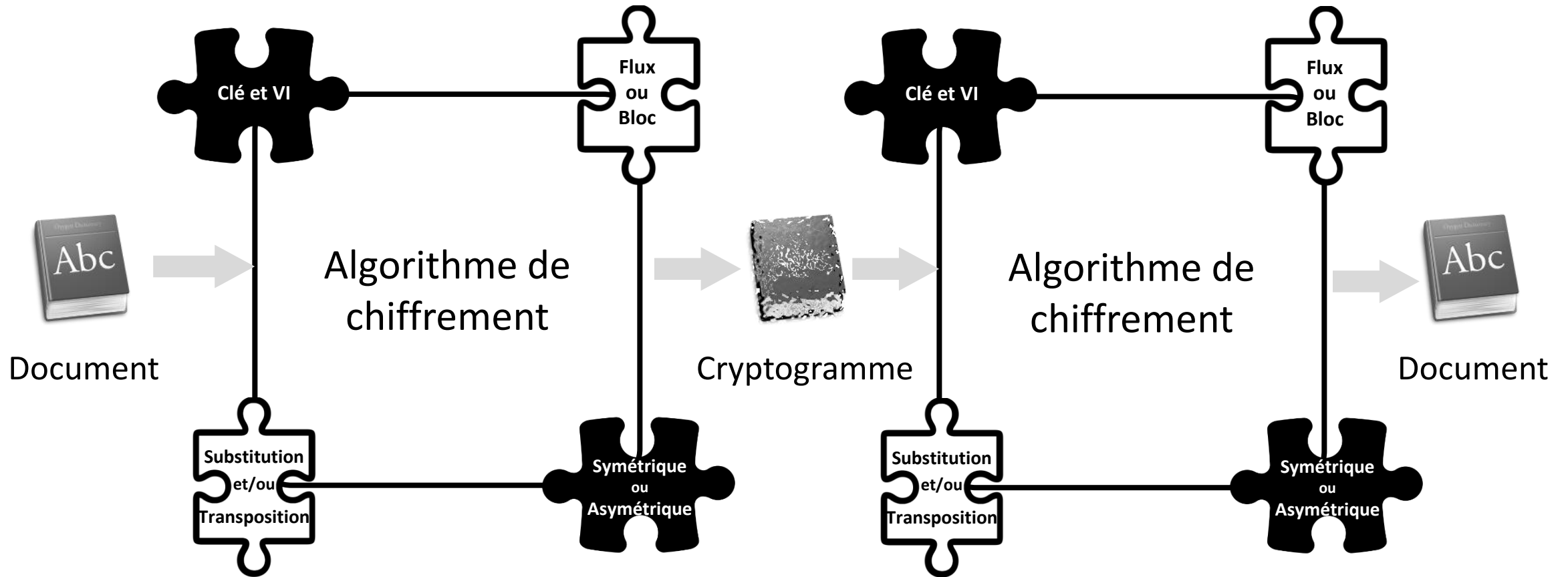
Toutes les personnes possédant la clé publique peuvent lire le message



**Authenticité, non
répudiation**

(Signature
numérique)

Introduction et définition: Bilan





Chiffrement Symétrique

- **Bilan**
- DES / 3 DES
- AES

Chiffrement symétrique

- Le plus couramment utilisé
- Principal avantage lié à la rapidité et la complexité liée à la taille de la clé
- Utilisation du chiffrement asymétrique pour la distribution de clés (voir partie Chiffrement Hybride)
- Exemples d'algorithmes de chiffrement
 - Data Encryption Standard (DES) / 3DES (triple DES)
 - Blowfish
 - Twofish
 - IDEA (Internation Data Encryption Algorithm)
 - RC4,RC5,RC6
 - AES
 - SAFER
 - Serpent





Chiffrement Symétrique

- Bilan
- **DES / 3 DES**
- AES

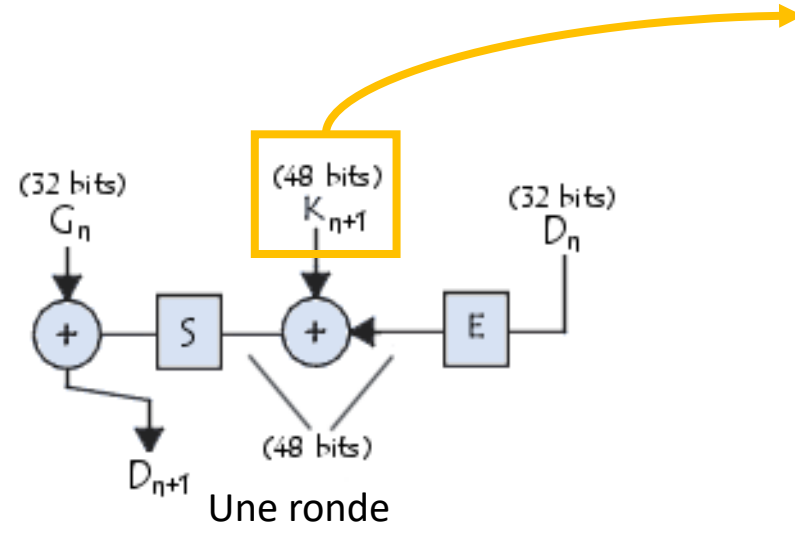
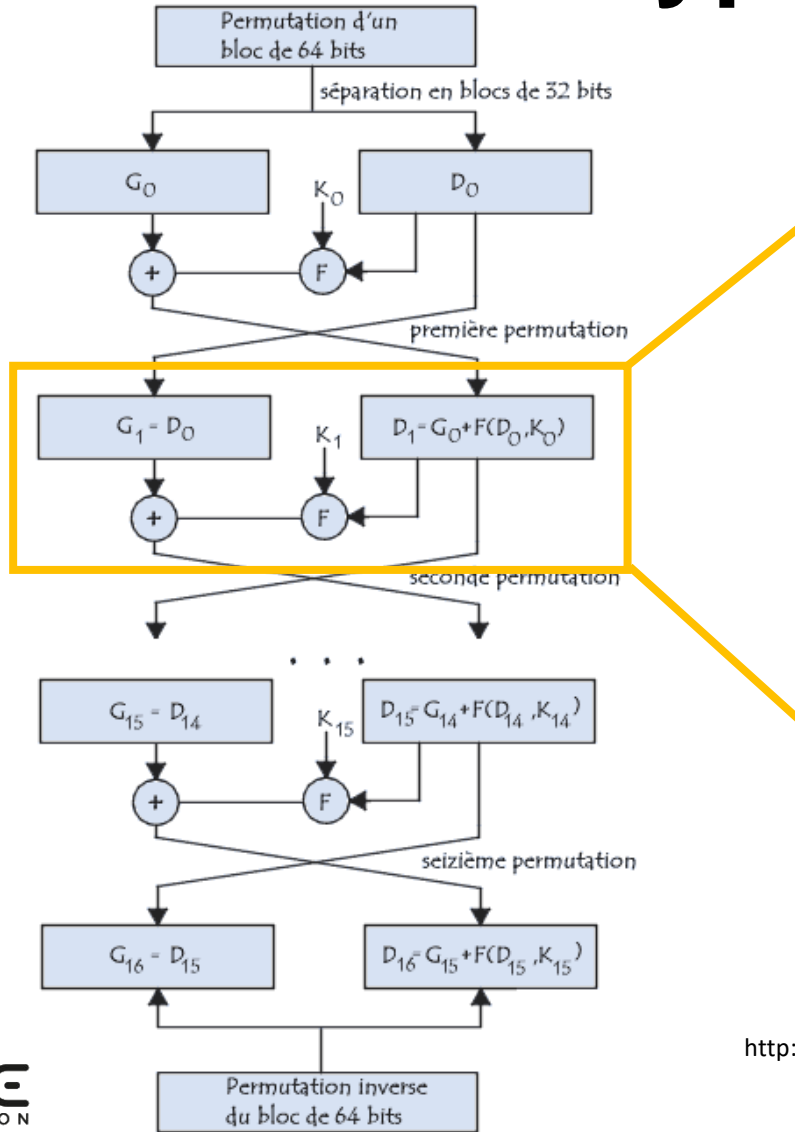
DES-Data Encryption Standard

- IBM 1977, Chiffrement symétrique
- Chiffrement par blocs (64 bits)
- Utilisation d'une clé de 64 bits (56 vrai clé 8 parité)
- Substitution et permutation

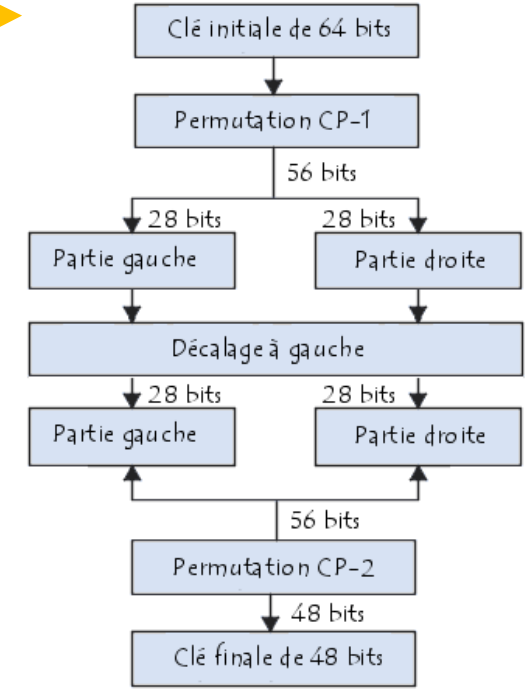
- Algorithme
 1. Fractionnement du texte en blocs de 64 bits (8 octets) ;
 2. Permutation initiale des blocs ;
 3. Découpage blocs en deux parties: gauche et droite, nommées G et D;
 4. Etapes de permutation et de substitution répétées 16 fois (appelées rondes) ;
 5. Recollement des parties gauche et droite puis permutation initiale inver



DES-Data Encryption Standard



Génération de clé

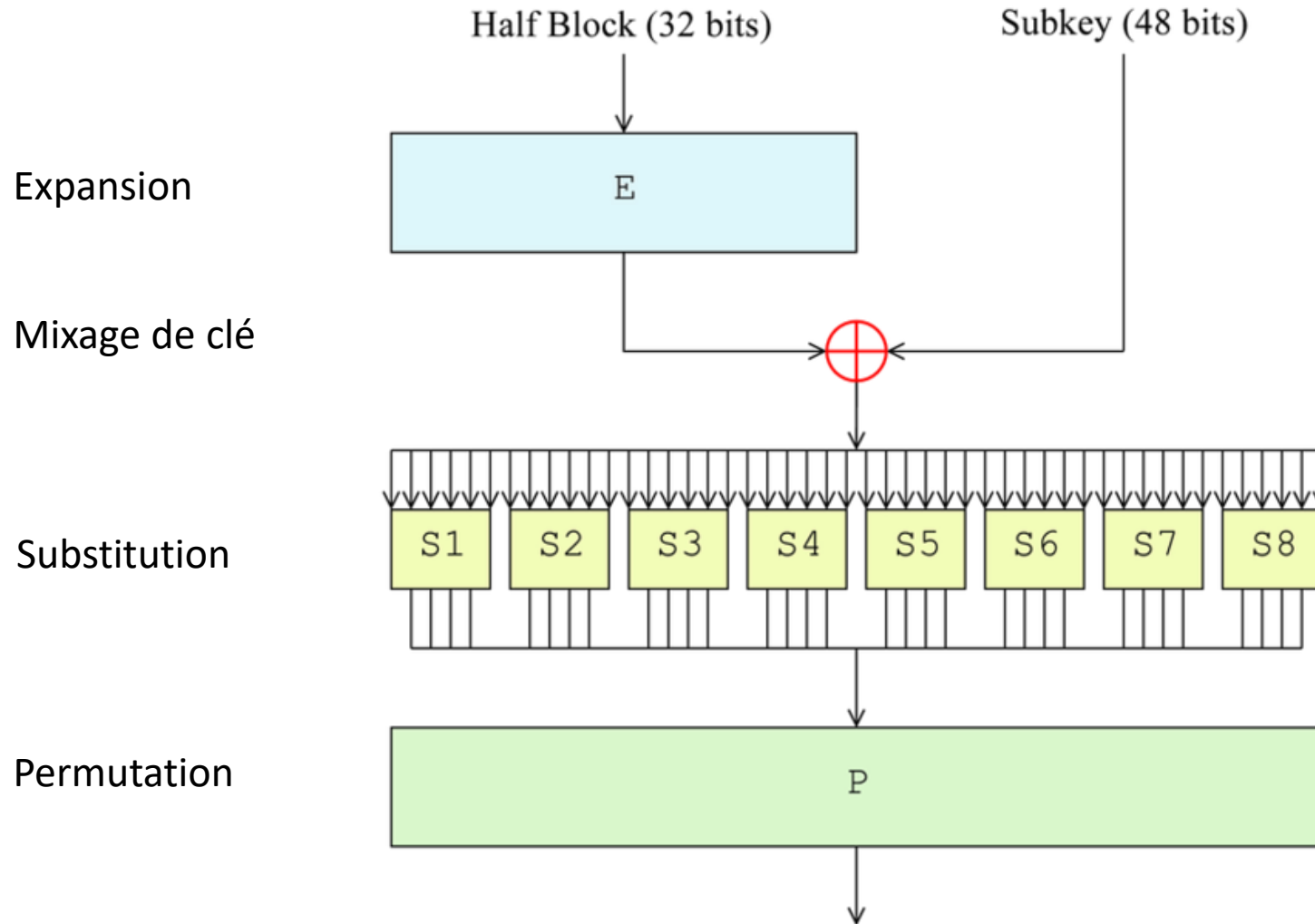


<http://www.commentcamarche.net/contents/crypto/des.php3>

Copyright © Jacques Saraydaryan

DES-Data Encryption Standard

Fonction F (Feistel) de DES

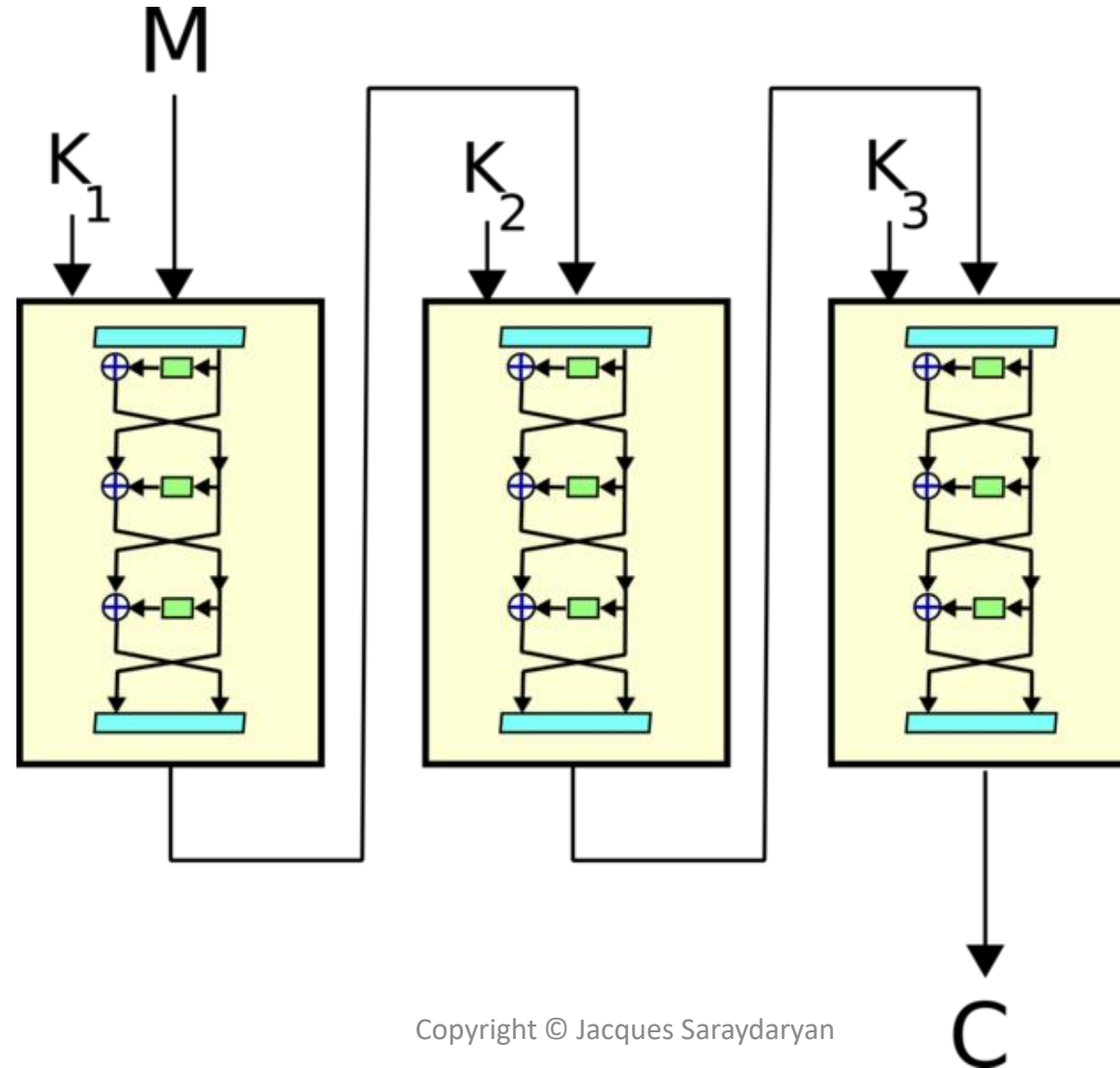


3 DES- Triple Data Encryption Standard

- ASN 1998
- Chiffrement symétrique
- Chiffrement par blocs (64 bits)
- Utilisation d'une clé de 168, 112 ou 56 bits
- Substitution et permutation
- 48 rondes équivalentes DES



3 DES- Triple Data Encryption Standard





Chiffrement Symétrique

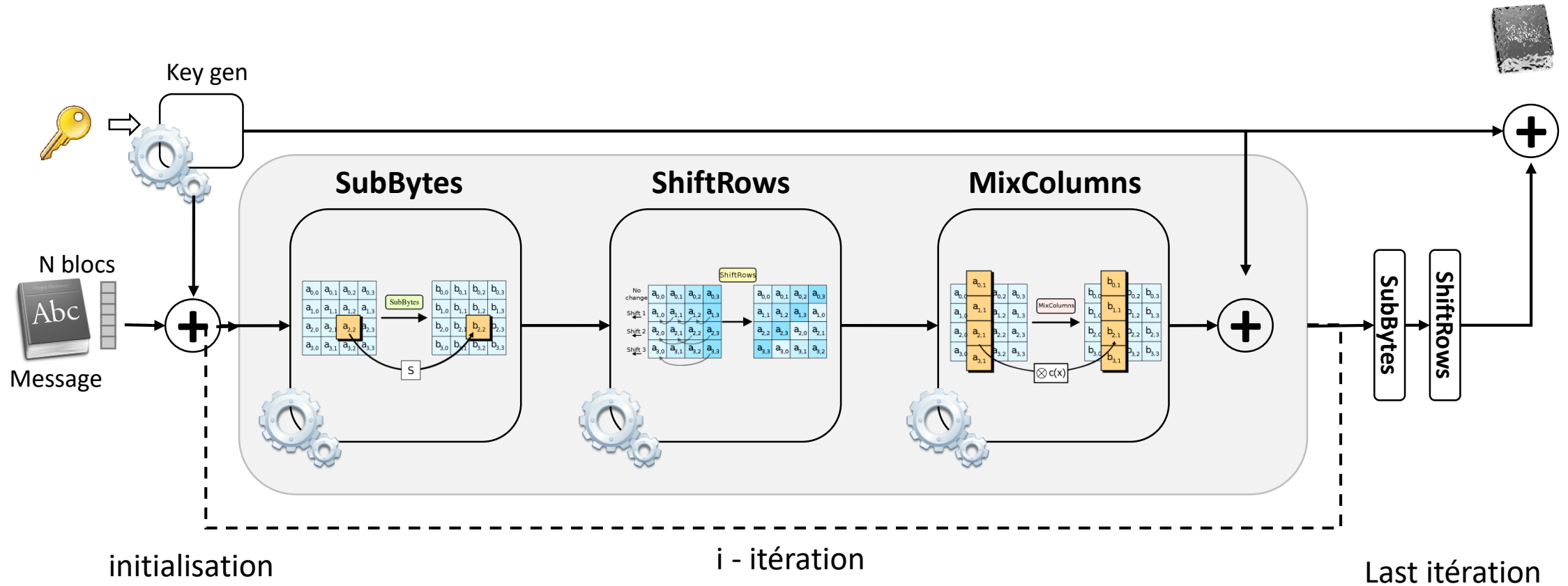
- Bilan
- DES / 3 DES
- **AES**

AES- Advanced Encryption Standard

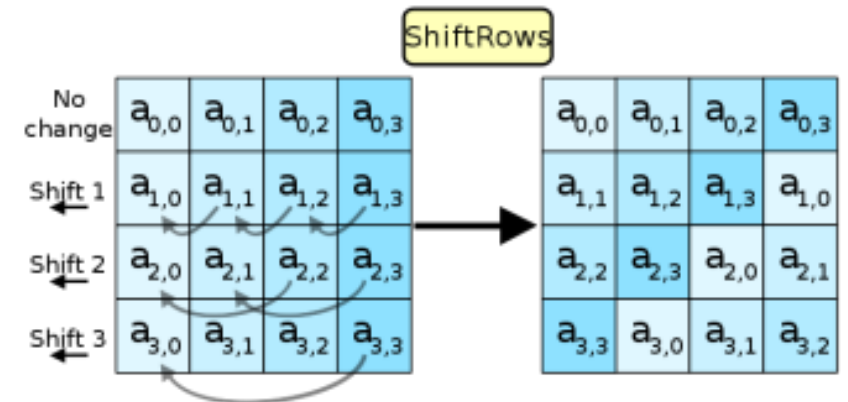
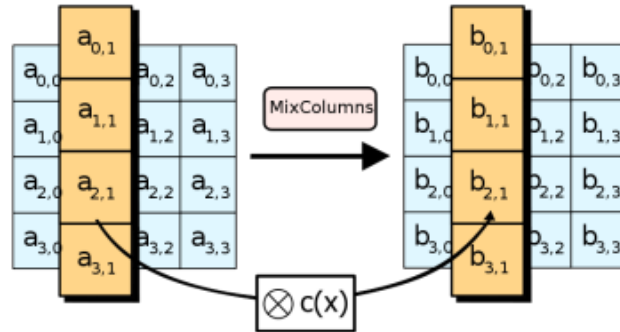
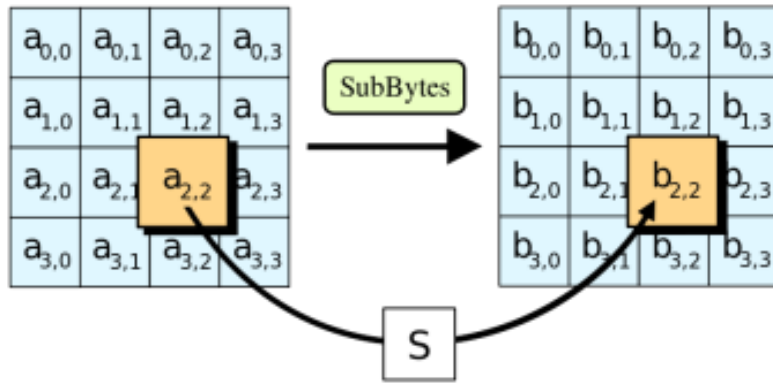
- AES ou Rijndael 2000 approuvé par la NSA
- Standard Chiffrement US
- Chiffrement symétrique
- Chiffrement par blocs (128 bits)
- Utilisation d'une clé de 128, 192 ou 256 bits
- Substitution et permutation
- 10,12 ou 14 rondes selon la taille de la clé



AES- Advanced Encryption Standard



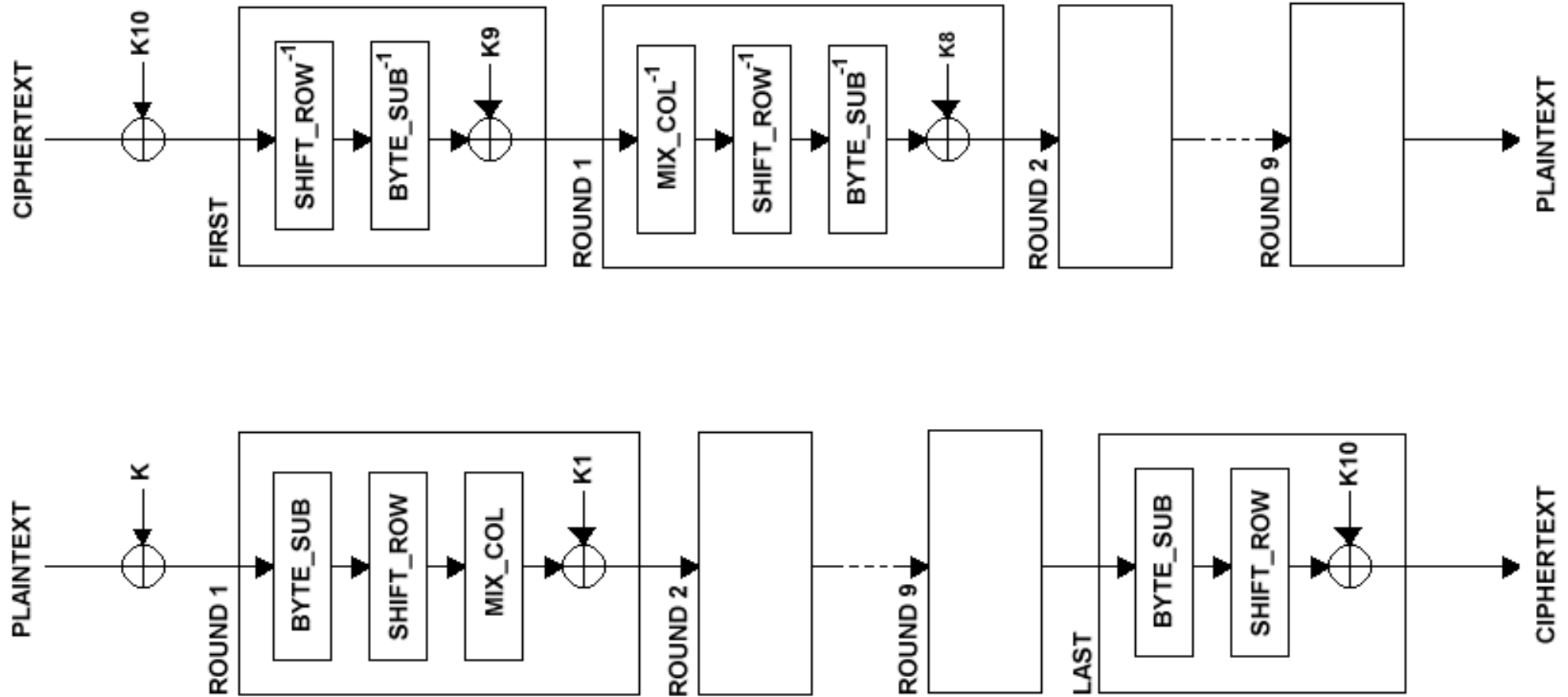
AES- Advanced Encryption Standard



http://en.wikipedia.org/wiki/Advanced_Encryption_Standard

Copyright © Jacques Saraydaryan

AES- Advanced Encryption Standard



<http://www.securiteinfo.com/cryptographie/aes.shtml>

Copyright © Jacques Saraydaryan

AES- Advanced Encryption Standard

□ Bilan

- Difficile à casser (bruteforce).
- Simplicité des calculs → rapidité de traitement
- Besoin en ressource et en mémoire faible
- flexibilité d'implémentation (taille des blocs et des clés)
- Hardware et software
- Simplicité : le design de l'AES est relativement simple



ANSSI (Agence Nationale de la Sécurité des Systèmes d'Information)

☐ Recommandation

- Algorithme: **AES**
- Taille des clés min: **128bits**
- Chiffrement par bloc: **128bits**
- Algo Chiffrement par flot: **ChaCha20**
- Plutôt **Bloc** que Flot

https://www.ssi.gouv.fr/uploads/2021/03/anssi-guide-selection_crypto-1.0.pdf

https://www.ssi.gouv.fr/uploads/2015/01/RGS_v-2-0_B1.pdf

Copyright © Jacques Saraydaryan





Chiffrement Asymétrique

- **Propriétés**
- Diffie-Hellman
- RSA
- Courbe elliptique
- Bilan

Chiffrement asymétrique

- Plus lent que le chiffrement symétrique
- Consommateur de ressource
- Permet un passage à l'échelle
- Distribution de clé
- Utiliser pour la distribution de clés de session
- Exemples d'algorithmes de chiffrement
 - Diffie-Hellman
 - Rivest, Shamir, Adleman (RSA)
 - Courbe Elliptique
 - El Gamal
 - Digital Signature Algorithm (DSA)
 - Knapsak



https://www.ssi.gouv.fr/uploads/2015/01/RGS_v-2-0_B1.pdf

Copyright © Jacques Saraydaryan



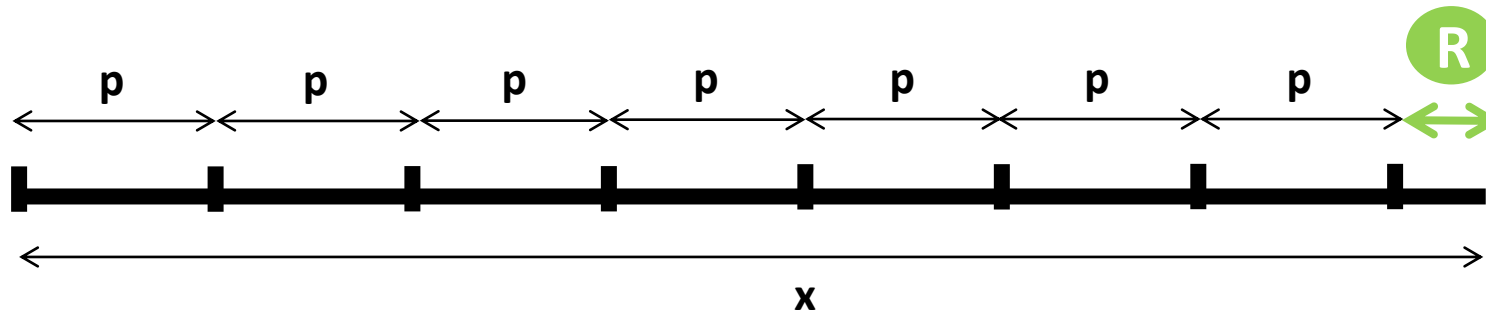
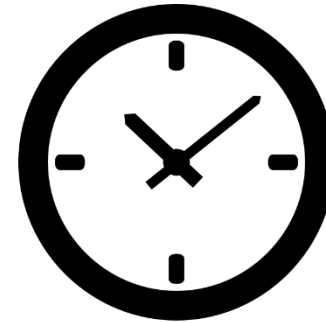
Chiffrement Asymétrique

- Propriétés
- **Diffie-Hellman**
- RSA
- Courbe elliptique
- Bilan

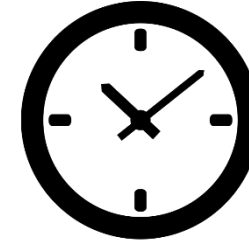
Objectif

→ Trouver une fonction qui est rapide et facile dans un sens et lente et complexe dans l'autre

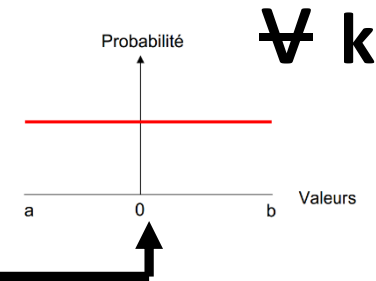
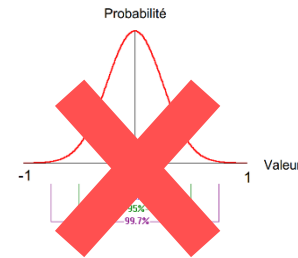
$$x \bmod p \equiv \text{R}$$



$$x \bmod p \equiv \text{R}$$
$$46 \bmod 12 \equiv 10$$



$$3^k \bmod 17$$



3 Est un générateur
17 Est le module

$$3^{15} \bmod 17 \equiv \text{R} \rightarrow \text{EASY !}$$

$$\text{HARD !} \leftarrow 3^k \bmod 17 \equiv 6$$

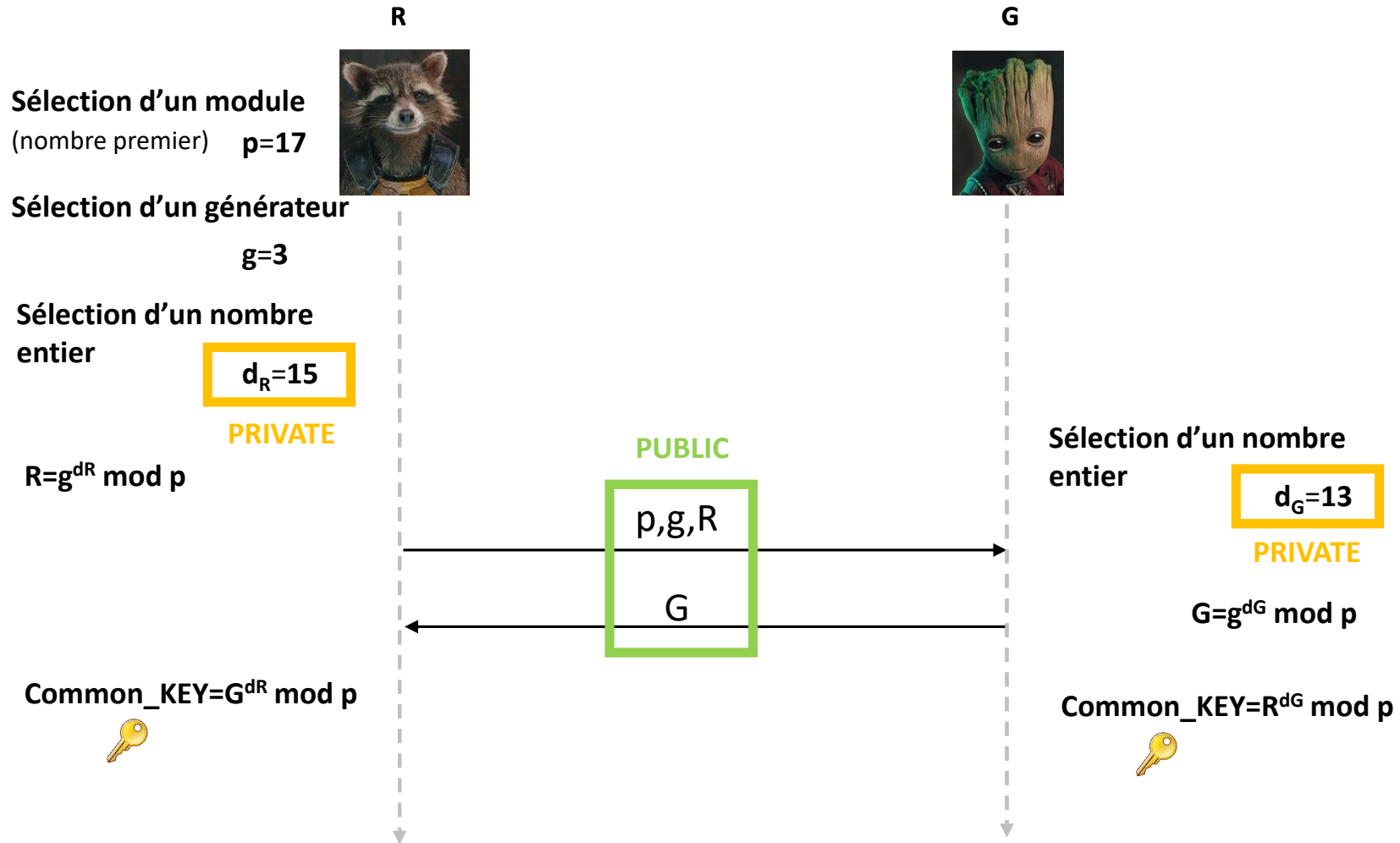
Si module = nombre premier très grand

$$3^{15} \bmod 17 \equiv \text{R} \rightarrow \text{EASY !}$$

$$\text{HARD !} \leftarrow 3^k \bmod 17 \equiv 6$$

Problème des logarithmes discrets

Diffie-Hellman



Diffie-Hellman

R



$$d_R=15$$

$$R=g^{d_R} \bmod p$$

$$\text{Common_KEY}=G^{d_R} \bmod p$$

$$(g^{d_G} \bmod p)^{d_R} \bmod p$$

$$(g^{d_G \times d_R} \bmod p) \bmod p$$

$$g^{d_G \times d_R} \bmod p$$

G



$$d_G=13$$

$$G=g^{d_G} \bmod p$$

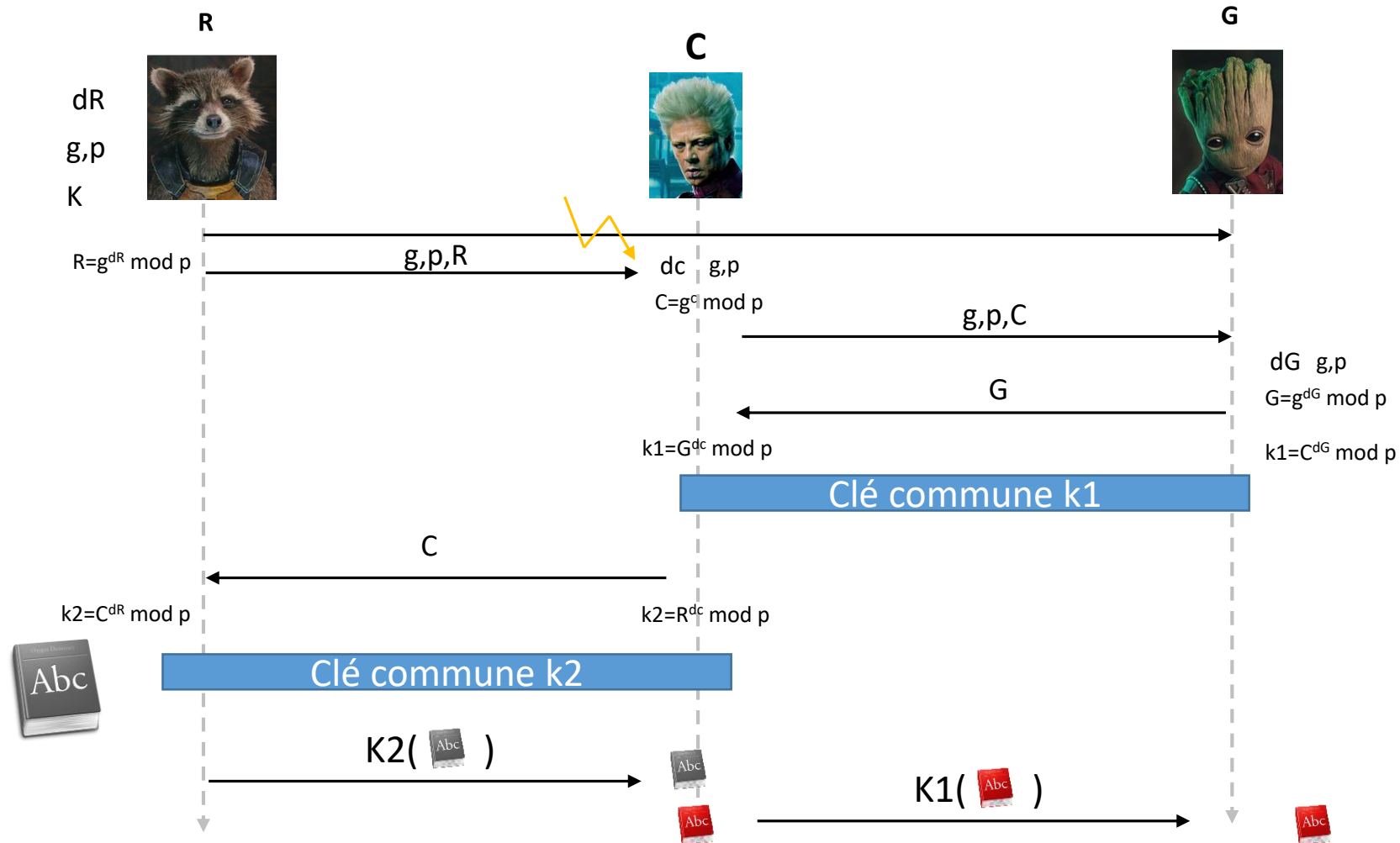
$$\text{Common_KEY}=R^{d_G} \bmod p$$

$$(g^{d_R} \bmod p)^{d_G} \bmod p$$

$$(g^{d_R \times d_G} \bmod p) \bmod p$$

$$g^{d_R \times d_G} \bmod p$$

Diffie-Hellman man in the Middle



Diffie-Hellman

- **Vulnérable** aux attaques **Man in the middle**
- **Force** de l'algorithme repose sur la difficulté du **problème de logarithme discret** retrouver g_a , g_b à partir de g_{ab} est très complexe
- Nécessiter de **vérifier l'identité** de son interlocuteur avant de prendre la clé publique





Chiffrement Asymétrique

- Propriétés
- Diffie-Hellman
- **RSA**
- Courbe elliptique
- Bilan

RSA

- Trouver une « one way function »
→ **Objectif utiliser l'exponentiation Modulaire**

$m^e \bmod N \equiv ? \rightarrow$ **EASY !**

HARD ! $\leftarrow ?^e \bmod N \equiv C$

RSA

- Trouver une « one way function »
→ **Objectif utiliser l'exponentiation Modulaire**



. $e \text{ mod } N$

R



G



Message Secret



Message Secret

RSA

- Trouver une « one way function »
 → **Objectif utiliser l'exponentiation Modulaire**

$$m^e \bmod N \equiv c$$

$$m^e \bmod N \equiv ? \rightarrow \text{EASY !}$$

$$c^d \bmod N \equiv m$$

$$\text{HARD !} \leftarrow ?^e \bmod N \equiv c$$

EASY

$$m^{ed} \bmod N \equiv m$$

$$m^{ed} \bmod N \equiv m \rightarrow \text{Comment choisir } d ?$$

Prime Factorisation

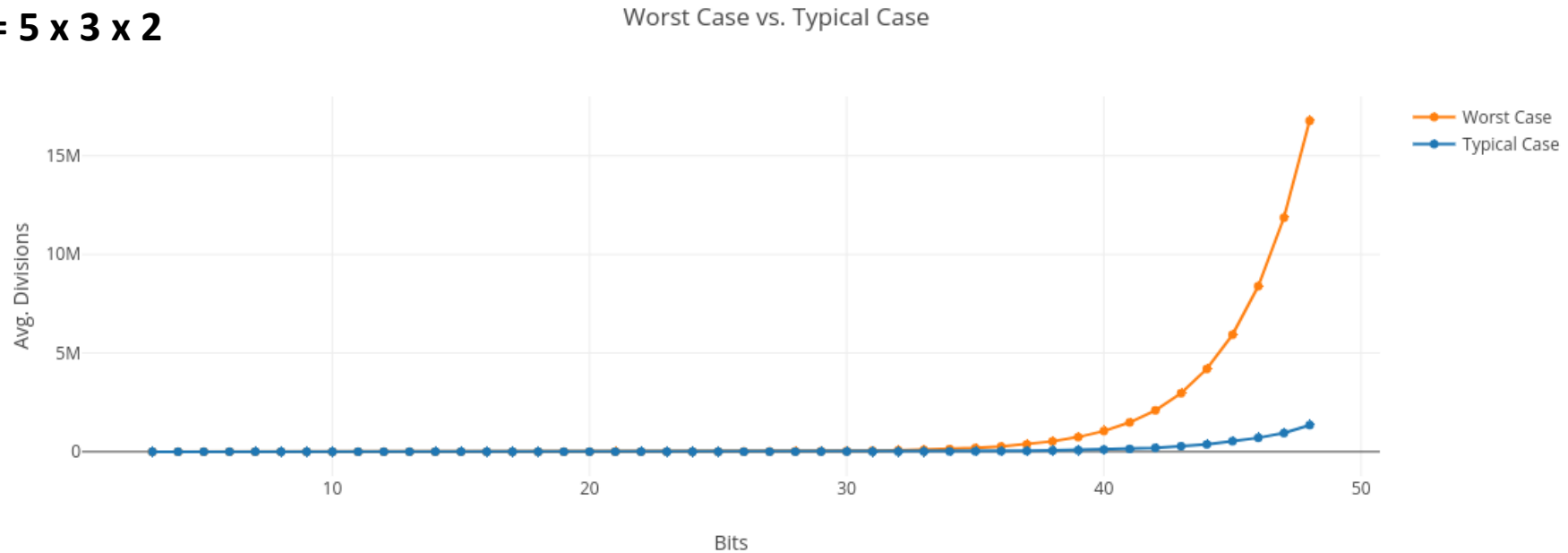
➔ **HARD !**

écrire un nombre naturel supérieur à 1 sous la forme d'un produit de facteurs premiers.

$$P1 \times P2 = N$$

$$12 = 2 \times 2 \times 3.$$

$$30 = 5 \times 3 \times 2$$



<https://nestedsoftware.com/2018/12/18/big-o-prime-factors-and-pseudo-polynomial-time-55cp.69665.html>

RSA

- La fonction Phi ou indicateur d'Euler
- Propriétés:

$\phi(n)$

$\forall n \in \mathbb{N}^*$

$\phi(n) = \text{vcard}(\{m \in \mathbb{N}^* \mid m \leq n, m \text{ premier avec } n\})$

$\phi(A \times B) = \phi(A) \times \phi(B)$

Exemple 1:

$$\phi(8) = 4$$

1
2
3
4
5
6
7
8

Exemple 2:

$$\phi(7) = 6$$

1
2
3
4
5
6
7

RSA

- La fonction Phi ou indicateur d'Euler $\phi(n)$
- Calculer $\phi(n)$ est **difficile sauf pour les nombres premiers** :

$$\phi(7) = 6$$

1
2
3
4
5
6
7

$$\phi(\text{Prime}) = \text{Prime} - 1$$

$\forall P1, P2$ nombre premier

$$\phi(P1 \times P2) = \phi(P1) \times \phi(P2)$$

$$\phi(P1 \times P2) = (P1 - 1) \times (P2 - 1)$$

RSA

- La fonction Phi ou indicateur d'Euler $\phi(n)$
- Calculer $\phi(n)$ est **difficile sauf pour les nombres premiers**

$$\phi(P1 \times P2) = \phi(P1) \times \phi(P2) = \text{R} \rightarrow \text{EASY !}$$

$$\text{HARD !} \leftarrow \phi(n) = \phi(P1) \times \phi(P2) = R$$

RSA

- La fonction Phi ou indicateur d'Euler $\phi(n)$

Comment utiliser $\phi(n)$
avec l'exponentiation
modulaire $m^e \bmod n$?

RSA

Théorème d'Euler

$$m^{\phi(n)} \equiv 1 \pmod{n}$$

Avec m et n sans facteur commun

$$1^k = 1 \quad \longrightarrow$$

$$m^{k \times \phi(n)} \equiv 1^k \pmod{n}$$

$$1 \times m = m \quad \longrightarrow$$

$$m \times m^{k \times \phi(n)} \equiv m \times 1^k \pmod{n}$$

$$m^{k \times \phi(n) + 1} \equiv m \pmod{n}$$

Hypothèse $m^{\boxed{e} \times d} \equiv m \pmod{\boxed{n}}$

PUBLIC

$$e \times d = k \times \phi(n) + 1$$

$$\boxed{d} = \frac{k \times \phi(n) + 1}{e}$$

PRIVATE

RSA

p et q


$pq=n$

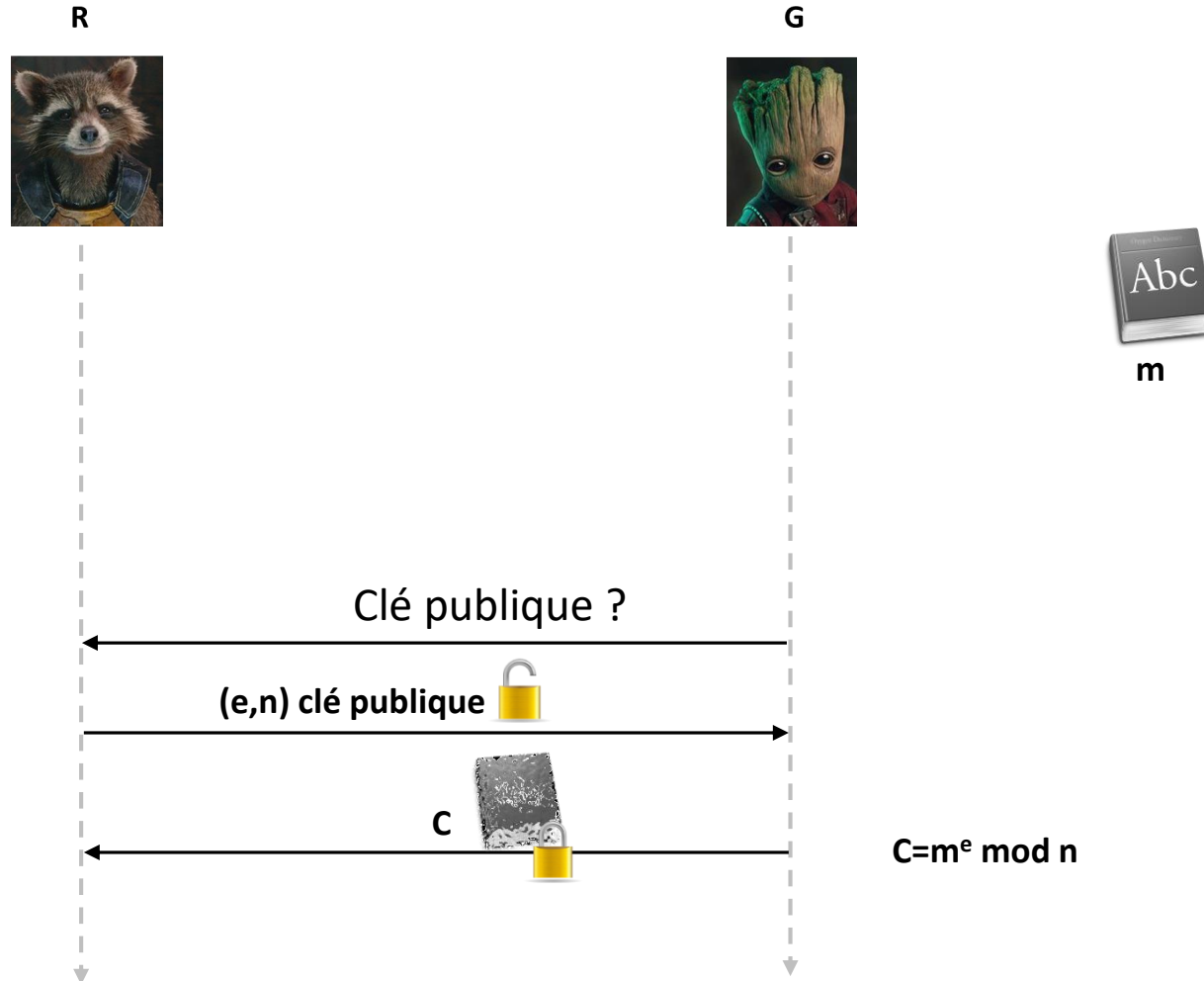
e aucun facteur commun
avec $(p-1)(q-1) \rightarrow \phi(n)$

$$d = \frac{k \times \phi(n) + 1}{e}$$

(e,n) clé publique 

(d,n) clé privée 




 $m=c^d \text{ mod } n$



RSA

p et q e aucun facteur commun
 $pq=n$ avec $(p-1)(q-1) \rightarrow \phi(n)$

$$d = \frac{k \times \phi(n) + 1}{e}$$

(e,n) clé publique 
 (d,n) clé privée 

Théorème d'Euler

$$m^{k \times \phi(n) + 1} \equiv m \pmod{n}$$



$$C^d \pmod{n}$$

$$m^e \pmod{n} \cdot d \pmod{n}$$

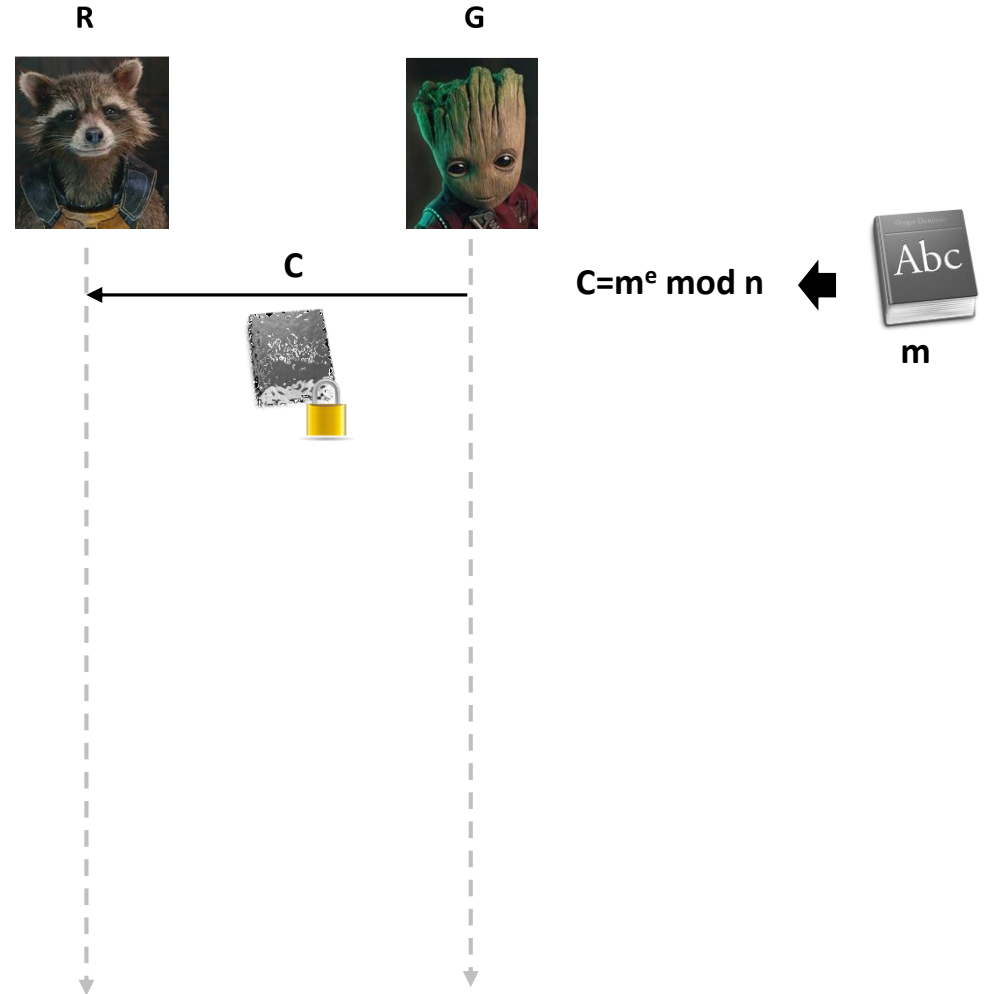
$$m^{e \times d} \pmod{n} \pmod{n}$$

$$m^{e \times d} \pmod{n}$$

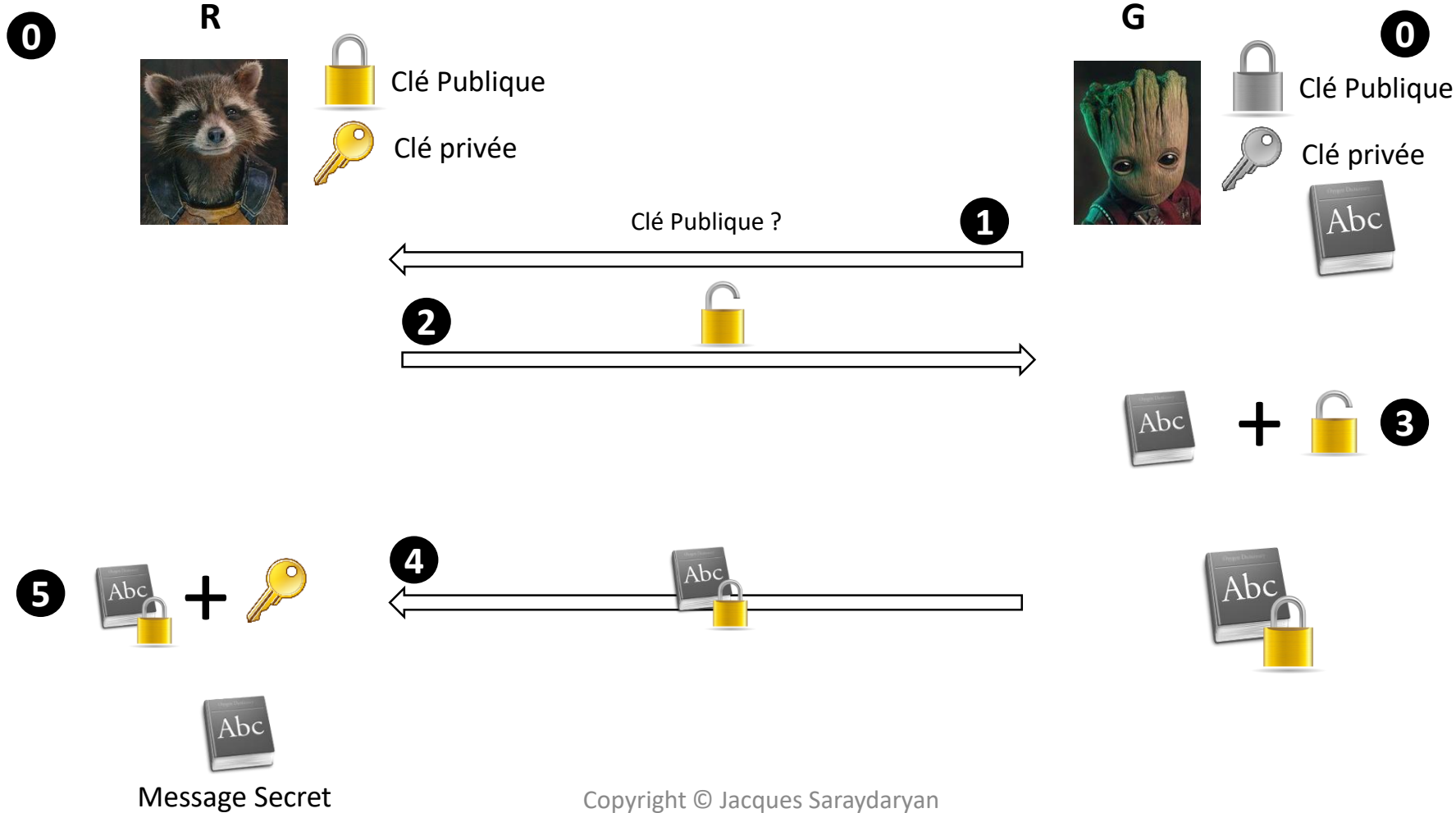
$$m^{e \times \frac{k \times \phi(n) + 1}{e}} \pmod{n}$$

$$m^{k \times \phi(n) + 1} \pmod{n}$$

$$m \pmod{n}$$



RSA



RSA

- Rivest, Shamir, Adleman
- Sélection des paramètres:
 - p et q choisis au hasard de façon à ce que $p \cdot q$ pas trop petit
 - p et q nombres premiers forts
 - $p-1$ possède un grand facteur premier
 - $p+1$ possède un grand facteur premier
- Peut être utilisé pour la **signature numérique**
- **Force** de l'algorithme repose sur la **difficulté à factoriser n** (calculer p et q)

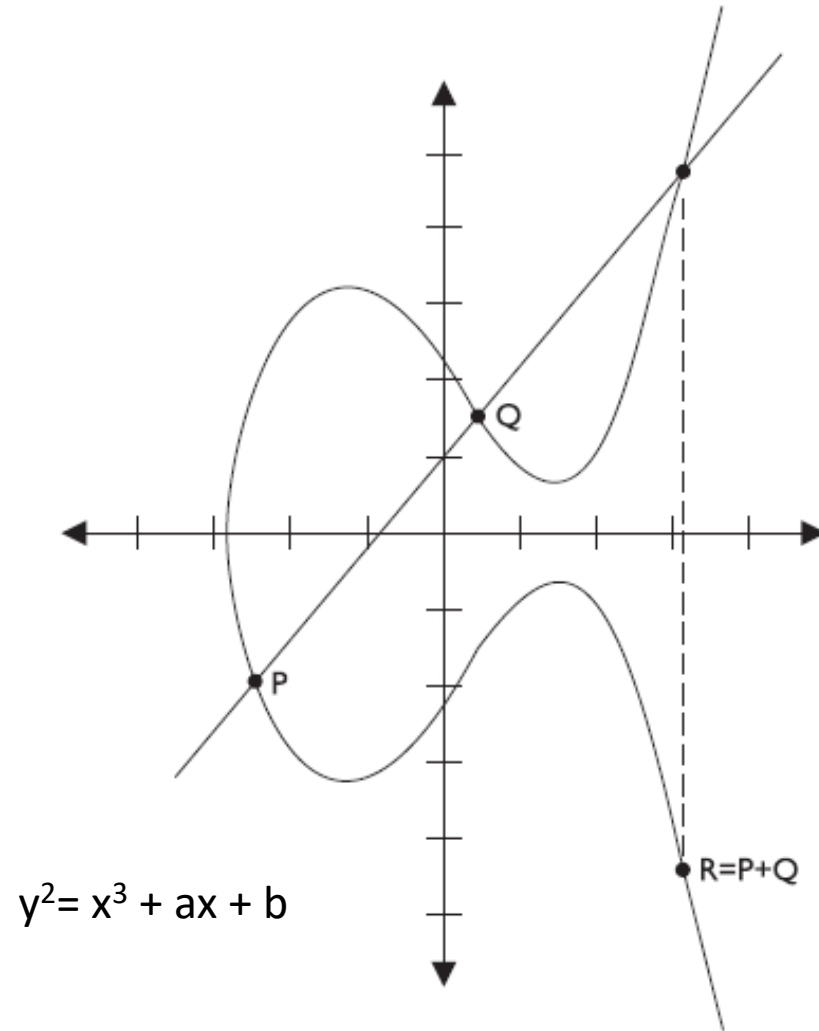




Chiffrement Asymétrique

- Propriétés
- Diffie-Hellman
- RSA
- **Courbe elliptique**
- Bilan

ECC Elliptic Curve Cryptosystem



ECC Elliptic Curve Cryptosystem

Choix d'une courbe elliptique $E(a,b,K)$

Choix d'un point P sur la courbe

Sélection d'un entier k_a

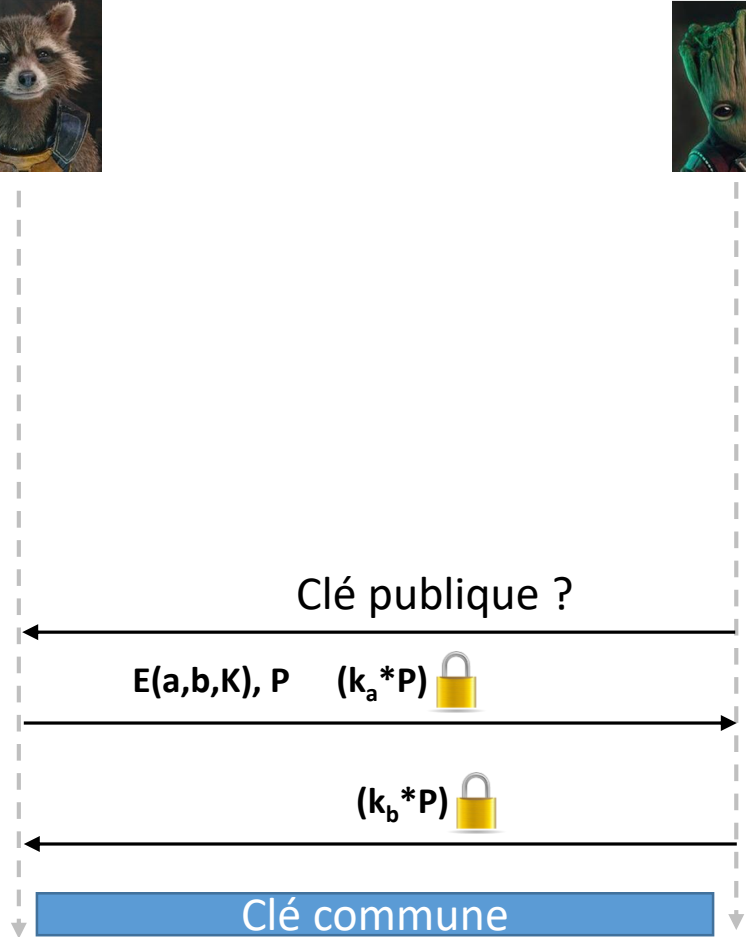
$(k_a * P)$ clé publique 
 (k_a) clé privée 

$(k_a k_b)P$ clé commune 

R



G



Sélection d'un entier k_b

$(k_a k_b)P$ clé commune 

ECC Elliptic Curve Cryptosystem

- **Calcul d'une clé commune** (semblable Diffie-Hellman)
- Complexité mathématique plus élevée que RSA pour cryptanalyse
- Taille de **clé plus petite permettant d'assurer une sécurité**
- équivalente à RSA (200 bits ECC contre 1024 bits pour RSA)
- **Complexité** des calculs **peu élevée** pour le calcul de la clé commune
- Beaucoup de brevets sur les courbes elliptiques dans la cryptographie (couteux)
- Théorie des courbes elliptiques encore récentes (trappes potentielles)



ANSSI (Agence Nationale de la Sécurité des Systèmes d'Information)

□ Recommandation

- Algorithme:
- Taille des clés min:
- Propriétés:

RSAES-OAEP,...

3072 bits

sous-groupes dont l'ordre est multiple d'un nombre premier d'au moins 256 bits (pour RSA)



https://www.ssi.gouv.fr/uploads/2021/03/anssi-guide-selection_crypto-1.0.pdf

https://www.ssi.gouv.fr/uploads/2015/01/RGS_v-2-0_B1.pdf

Quel futur pour les algorithmes de chiffrement ?

- Comment casser un RSA ? Trouver p et q de $n=p.q$
- Trouver un a tel que $a < N$ et relativement premier à N $PGCD(a,N)=1$,

Très long !

- Trouver r tel que r est la période de a mod N
- Vérifier que r est pair et $a^{r/2} + 1 \not\equiv 0 \pmod N$

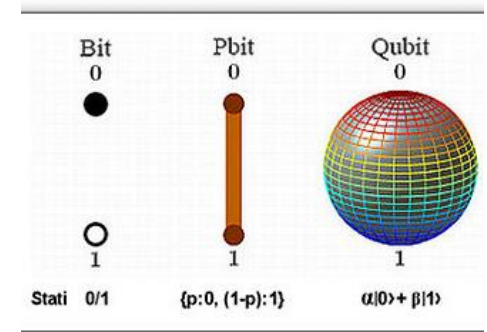
$$a^r \equiv 1 \pmod N$$

$$a^r - 1 \equiv 0 \pmod N \rightarrow a^r - 1 \equiv k.N \rightarrow (a^{\frac{r}{2}} - 1). (a^{\frac{r}{2}} + 1) \equiv k.p.q$$

- Résoudre

$$PGCD\left((a^{\frac{r}{2}} - 1), p\right)$$

$$PGCD\left((a^{\frac{r}{2}} + 1), q\right)$$

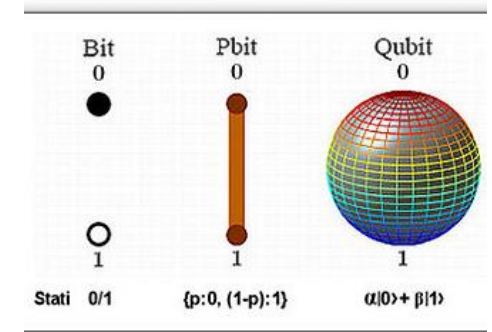
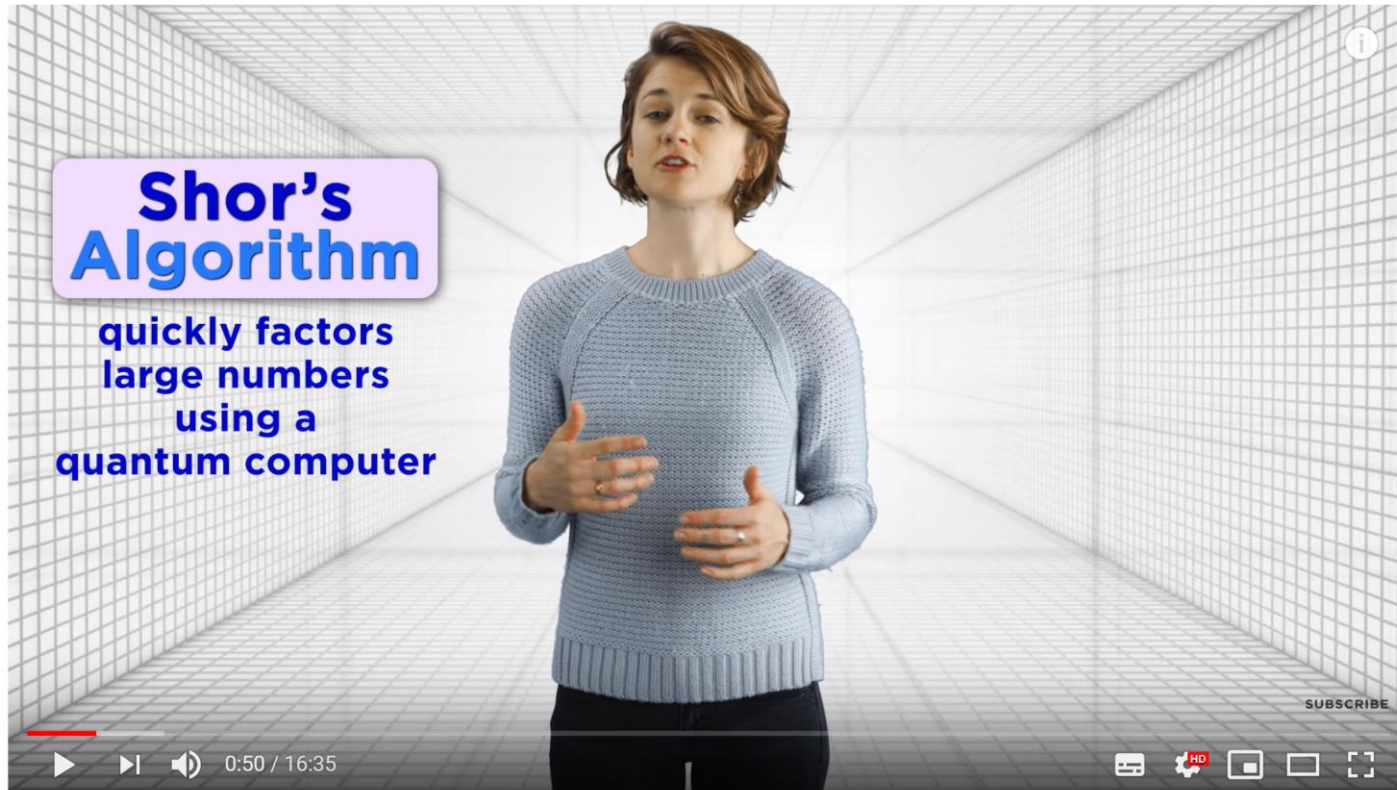


<https://taglidotme.files.wordpress.com/2013/10/qubit.jpg>

Quel futur pour les algorithmes de chiffrement ?

FACILE avec un ordinateur quantique

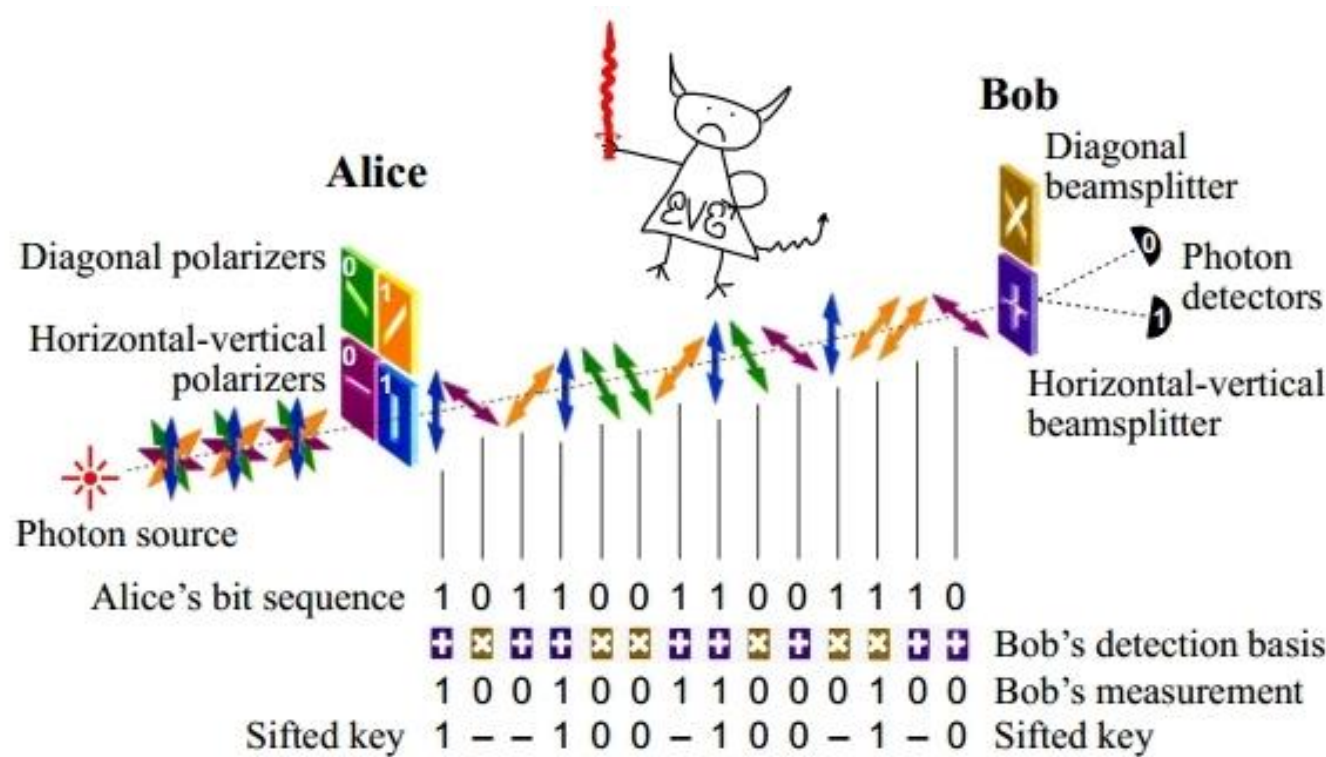
- Trouver r tel que r est la période de $a \bmod N$



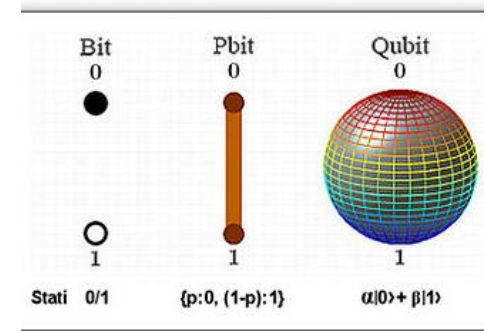
<https://taglidotme.files.wordpress.com/2013/10/qubit.jpg>

Quel futur pour les algorithmes de chiffrement ?

- Une nouvelle alternative : **Quantum Key Distribution**



http://qubitekk.com/wp-content/uploads/2015/12/QKD_product_small.jpg



<https://www.techrepublic.com/blog/it-security/how-quantum-cryptography-works-and-by-the-way-its-breakable/>

<https://taglidotme.files.wordpress.com/2013/10/qubit.jpg>



Chiffrement Asymétrique

- Propriétés
- Diffie-Hellman
- RSA
- Courbe elliptique
- **Bilan**

Bilan symétrique asymétrique

- Utilisation de système hybride
- Utilisation de la puissance des algorithmes asymétriques pour l'échange de clé
- Utilisation du chiffrement symétrique rapide pour chiffrer les contenus





Fonctions de Hachage

- **Propriétés**
- MD5
- SHA

Fonctions de Hachage

- Fonction de hachage ou One Way Hash

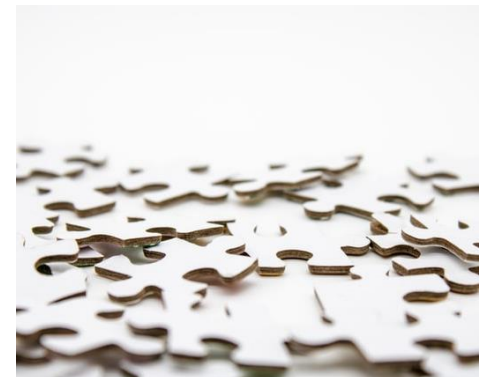
Fonction capable à partir un élément de taille variable de fournir une valeur de taille fixe appelée empreinte ou hash.

- Utilisation de fonction à sens unique

Fonction facile à calculer dans un sens mais très difficile à inverser

- Propriétés

- Calcul rapide
- Eviter les collisions (2 données différentes représentées par une même empreinte)
- Possibilité d'avoir une empreinte plus grande que les données initiales
(protection des mots de passe)
- Volonté qu'un seul changement de bits entraîne un changement important dans l'empreinte résultante



Fonctions de Hachage

- Propriétés nécessaires pour la cryptographie
 - Très difficile de trouver un message à partir de son empreinte
 - Très difficile à partir d'un message et de son empreinte de générer un message différent possédant la même empreinte
 - Très difficile de trouver 2 messages aléatoires possédant la même empreinte
- Notion de **salting** (grain de sel)
 - Ajout d'une chaîne pseudo-aléatoire au message avant le hash
 - e.g. password + MD5(login) -> SHA (password + MD5(login))
 - > **évite les attaques par table de hash.**
 - > Cf. **Bcrypt**



Fonctions de Hachage

□ Exemple de fonction de Hachage

- HMAC
- CBC-MAC
- MD5
- **SHA**
- **Bcrypt**

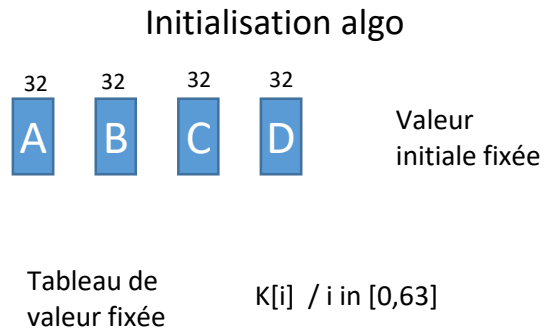
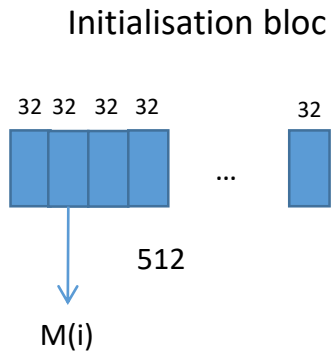
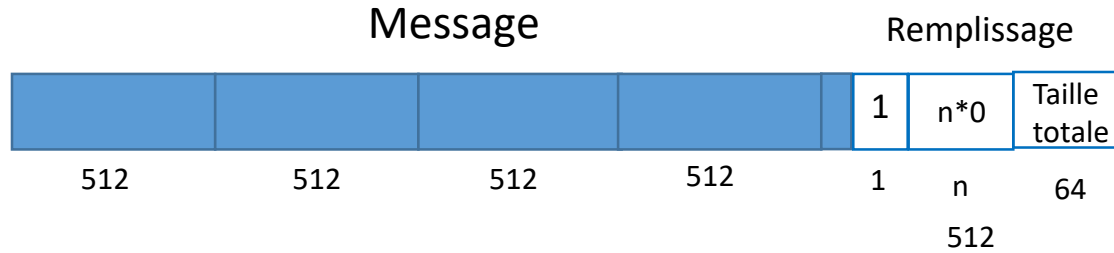




Fonctions de Hachage

- Propriétés
- **MD5**
- SHA

Fonctions de Hachage : MD5



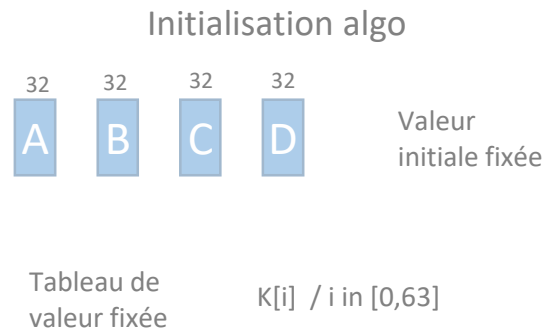
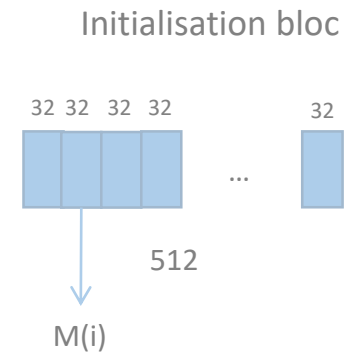
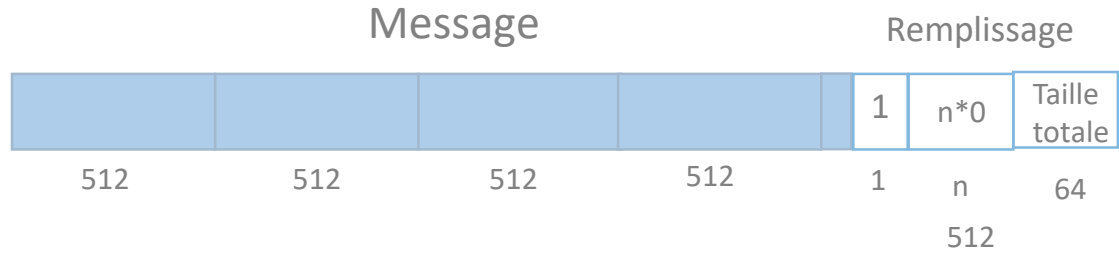
$$F(x,y,z) = (x \text{ AND } y) \text{ OR } (\text{not}(x) \text{ AND } z)$$

$$G(x,y,z) = (x \text{ AND } z) \text{ OR } (y \text{ AND } \text{not}(z))$$

$$H(x,y,z) = x \text{ XOR } y \text{ XOR } z$$

$$I(x,y,z) = x \text{ XOR } (x \text{ AND } \text{not}(z))$$

Fonctions de Hachage : MD5

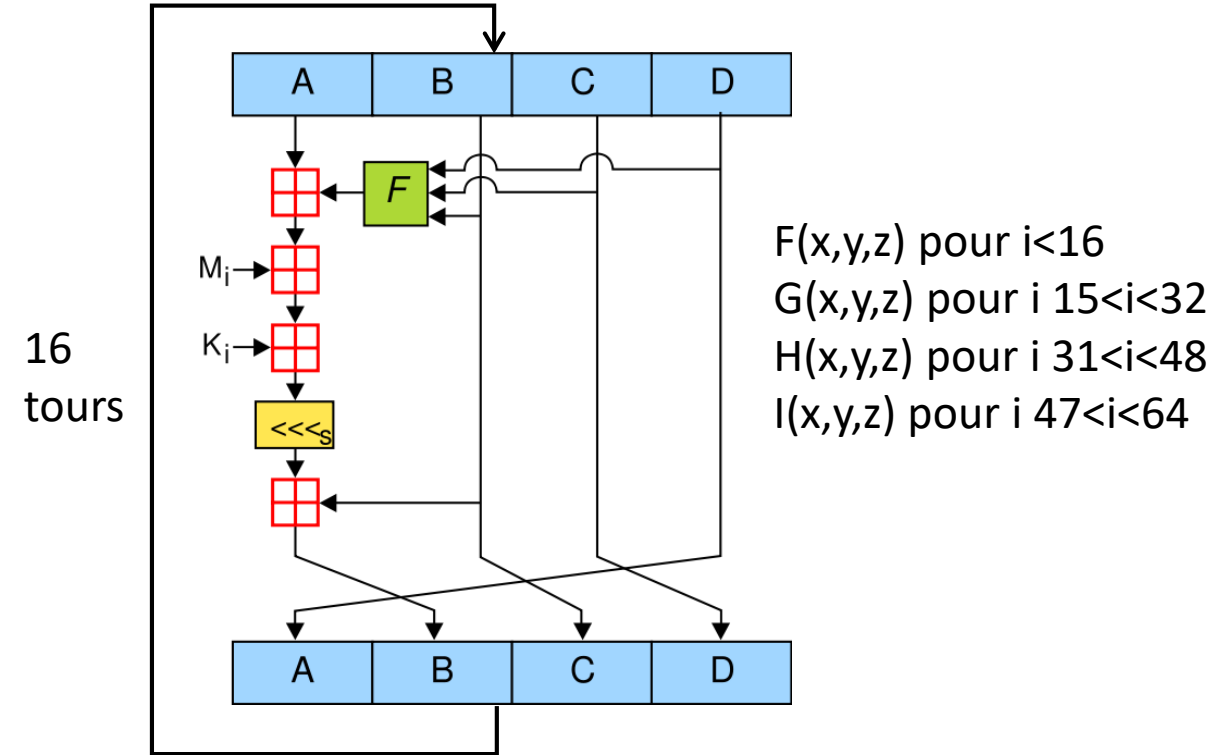


$$F(x,y,z) = (x \text{ AND } y) \text{ OR } (\text{not}(x) \text{ AND } z)$$

$$G(x,y,z) = (x \text{ AND } z) \text{ OR } (y \text{ AND } \text{not}(z))$$

$$H(x,y,z) = x \text{ XOR } y \text{ XOR } z$$

$$I(x,y,z) = x \text{ XOR } (x \text{ AND } \text{not}(z))$$



MD5(" The quick brown fox jumps over the lazy dog ")

9e107d9d372bb6826bd81d3542a419d6

MD5

- ❑ Message Digest 5
- ❑ Ronald Rivest 1991
- ❑ 1996 faille **grave** de **collisions**
- ❑ 2004 découvert des **collisions complètes** → SHA 256

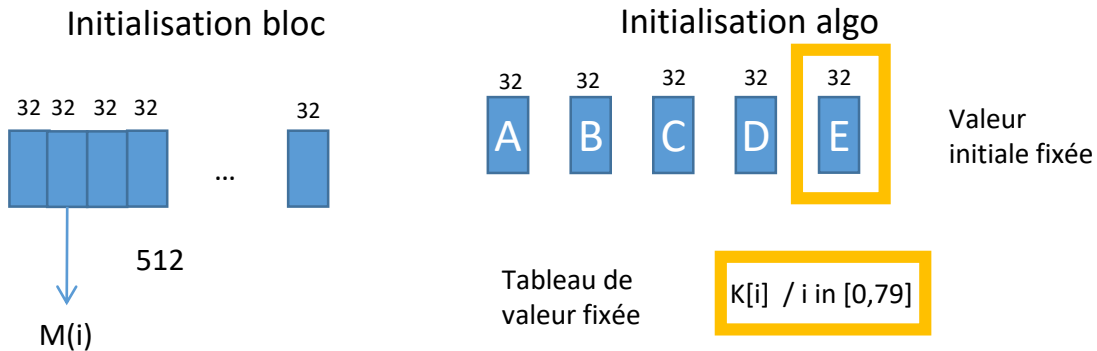
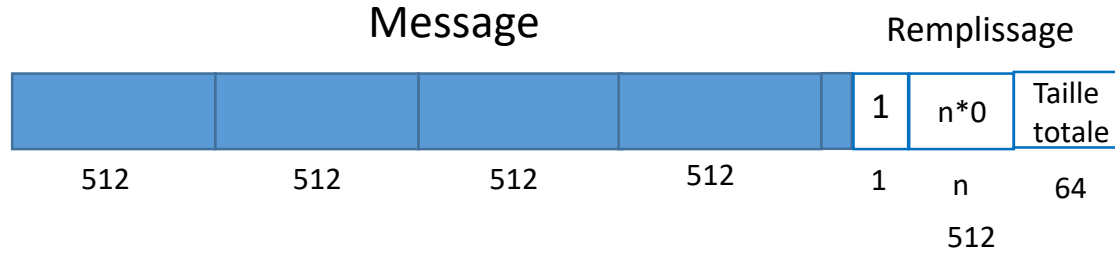




Fonctions de Hachage

- Propriétés
- MD5
- **SHA**

Fonctions de Hachage: SHA

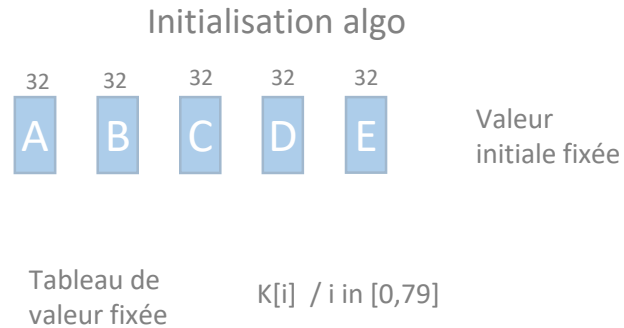
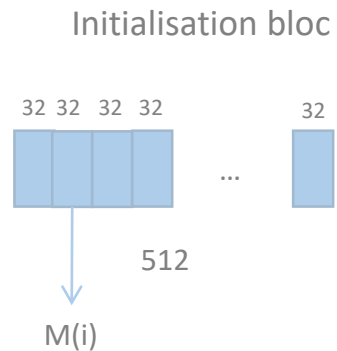
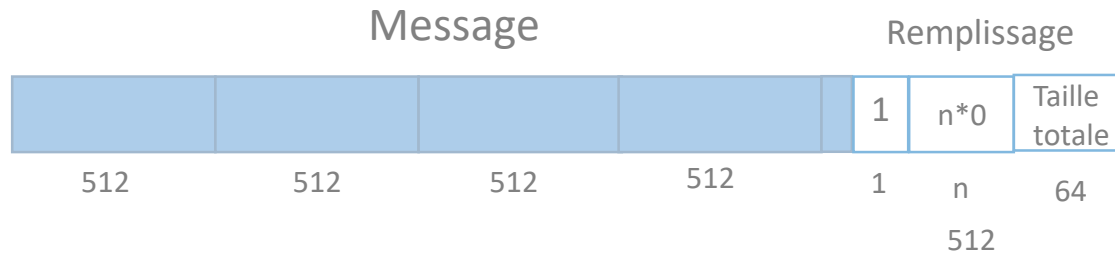


$$F(x,y,z) = (x \text{ AND } y) \text{ OR } (\text{not}(x) \text{ AND } z)$$

$$G(x,y,z) = x \text{ XOR } y \text{ XOR } z$$

$$H(x,y,z) = (x \text{ AND } z) \text{ OR } (y \text{ AND } z) \text{ OR } (x \text{ AND } y)$$

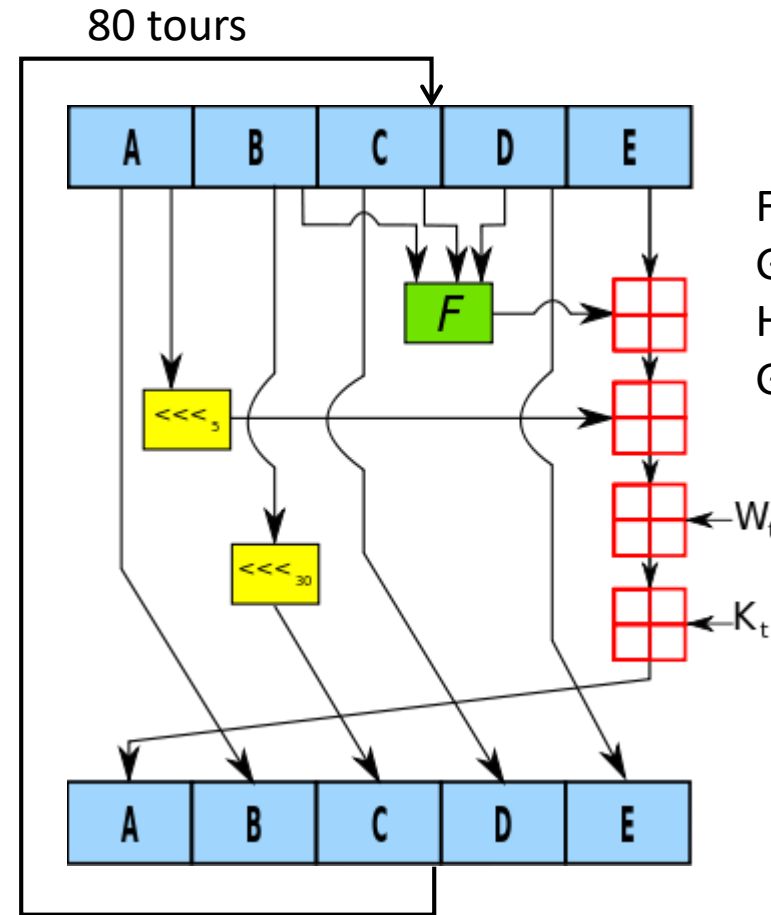
Fonctions de Hachage: SHA



$$F(x,y,z) = (x \text{ AND } y) \text{ OR } (\text{not}(x) \text{ AND } z)$$

$$G(x,y,z) = x \text{ XOR } y \text{ XOR } z$$

$$H(x,y,z) = (x \text{ AND } z) \text{ OR } (y \text{ AND } z) \text{ OR } (x \text{ AND } y)$$



F(x,y,z) pour i < 20
 G(x,y,z) pour i 21 < i < 40
 H(x,y,z) pour i 39 < i < 60
 G(x,y,z) pour i 59 < i < 80

SHA

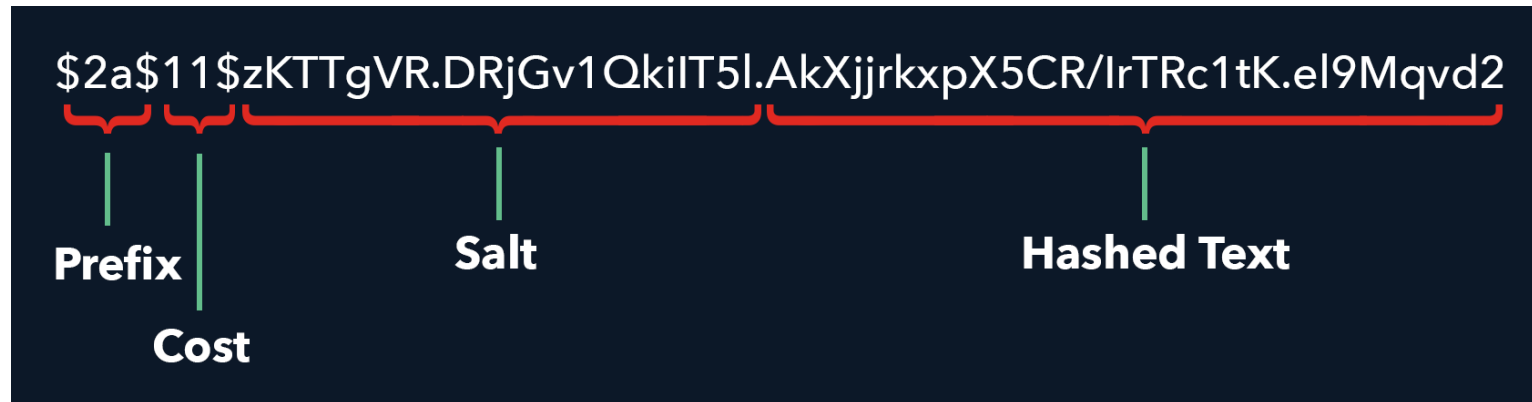
- Message Digest 5
- Ronald Rivest 1991
- 1996 faille **grave** de **collisions**
- 2004 découvert des **collisions complètes** → SHA-2/3 ≥ 256

Algorithm and variant		Output size (bits)	Block size (bits)	Rounds	Operations	Security against collision attacks (bits)	Security against length extension attacks (bits)	First published
MD5 (as reference)		128	512	64	And, Xor, Rot, Add (mod 2^{32}), Or	≤ 18 (collisions found)[60]	0	1992
SHA-0		160	512	80	And, Xor, Rot, Add (mod 2^{32}), Or	< 34	0	1993
SHA-1		160	512	80	And, Xor, Rot, Add (mod 2^{32}), Or	< 63	0	1995
SHA-2	SHA-256	256				128	0	2001
	SHA-512	512	1024	80	And, Xor, Rot, Add (mod 2^{64}), Or, Shr	256	0[62]	2001
	SHA-512/256	256	1024	80	And, Xor, Rot, Add (mod 264), Or, Shr	128	256	2012
SHA-3	SHA3-256	256	1088			128	512	
	SHA3-512	512	576	24	And, Xor, Rot, Not	256	1024	2015

<http://en.wikipedia.org/wiki/SHA-1>

Bcrypt

- Niels Provos, David Mazières 1999
- Stockage de mots de passe (usage principal)
- Usage de grain de sel (protection contre Rainbow tables)
- Fonction adaptative (augmentation du nombre d'itérations possible)
- Basé sur l'algorithme de chiffrement de Blowfish



Bilan

- MD5 et SHA1 encore très utilisés
- Préférable d'utiliser SHA256
- Permettent **d'assurer l'intégrité** d'un document
- Utilisées pour la **signature numérique** conjointement avec le chiffrement asymétrique
- Utilisées pour **protéger du contenu stocké**
- Ancienne version linux/Windows -> MD5

- Possible de préciser la méthode

```
password sufficient pam_unix.so min=4 sha256
```



ANSSI (Agence Nationale de la Sécurité des Systèmes d'Information)

□ Recommandation

▪ Fonction de hachage

- Algorithme: **SHA-2, SHA-3**
- Taille de sortie **≥ 256**

▪ Stockage des mots de passes

- Algorithme: **PBKDF2** (RFC8018)
- Usage: grain de sel et fonction de hash >128bits



https://www.ssi.gouv.fr/uploads/2021/03/anssi-guide-selection_crypto-1.0.pdf



Bilan Eléments Chiffrement

Bilan éléments chiffrement

Algorithm Type	Encryption	Digital Signature	Hashing Function	Key Distribution
Asymmetric Key Algorithms				
RSA	X	X		X
ECC	X	X		X
Diffie-Hellman				X
El Gamal	X	X		X
DSA		X		
LUC	X	X		X
Knapsack	X	X		X
Symmetric Key Algorithms				
DES	X			
3DES	X			
Blowfish	X			
IDEA	X			
RC4	X			
SAFER	X			
Hashing Algorithms				
Ronald Rivest family of hashing functions: MD2, MD4, and MD5			X	
SHA			X	
HAVAL (variable-length hash values using a one-way function design)			X	



ANSSI

Guide de sélection d'algorithmes Cryptographiques (2021)

https://www.ssi.gouv.fr/uploads/2021/03/anssi-guide-selection_crypto-1.0.pdf



PKI: Public Key Infrastructure

- **Besoin et définition**
- Architecture
- Bilan

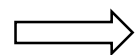
PKI : Besoins



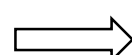
Comme faire confiance à son interlocuteur ?



Comment s'assurer que son interlocuteur est bien là personne qu'elle prétend être ?

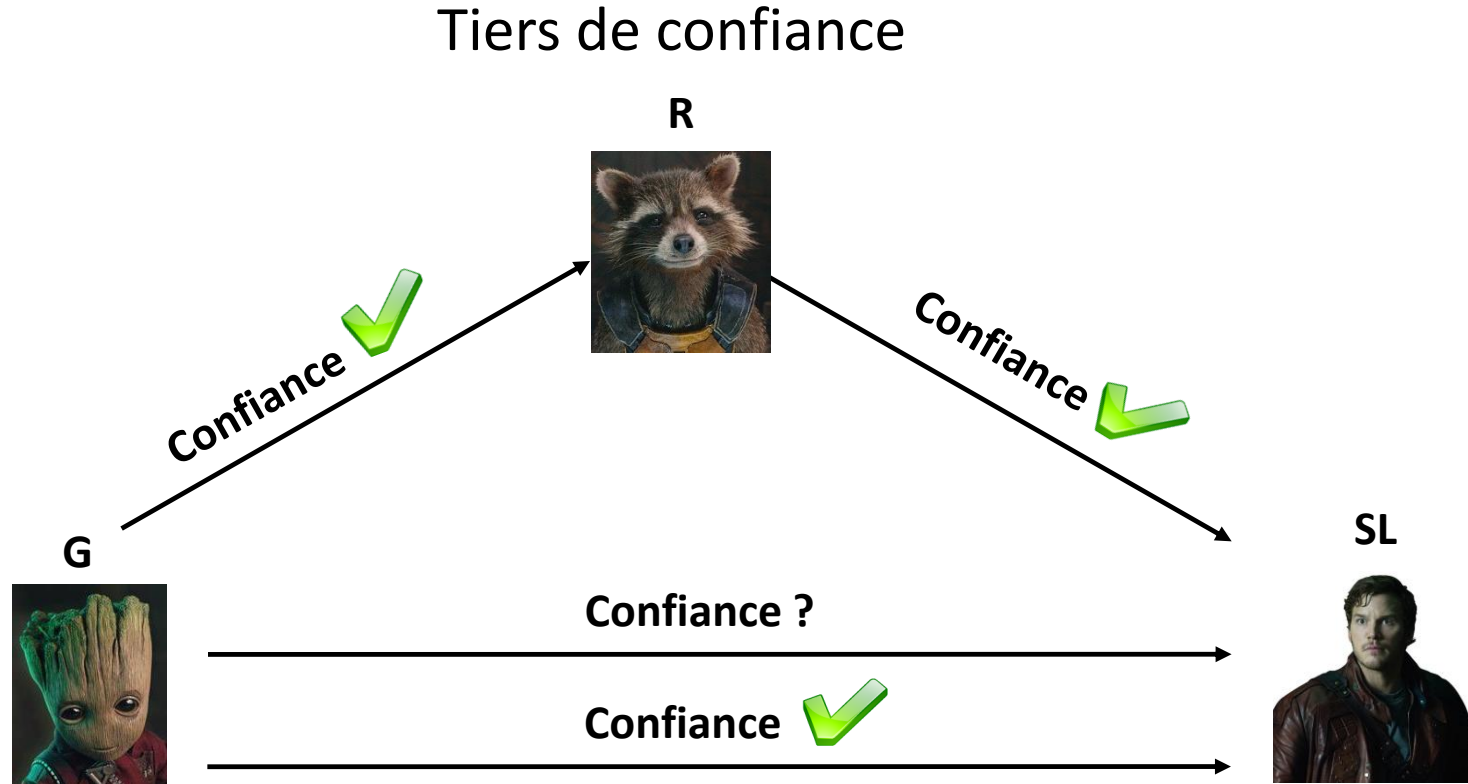


Utilisation d'un Tiers de confiance



Utilisation de certificats

PKI : Besoins



PKI : Risques

❑ Objectif

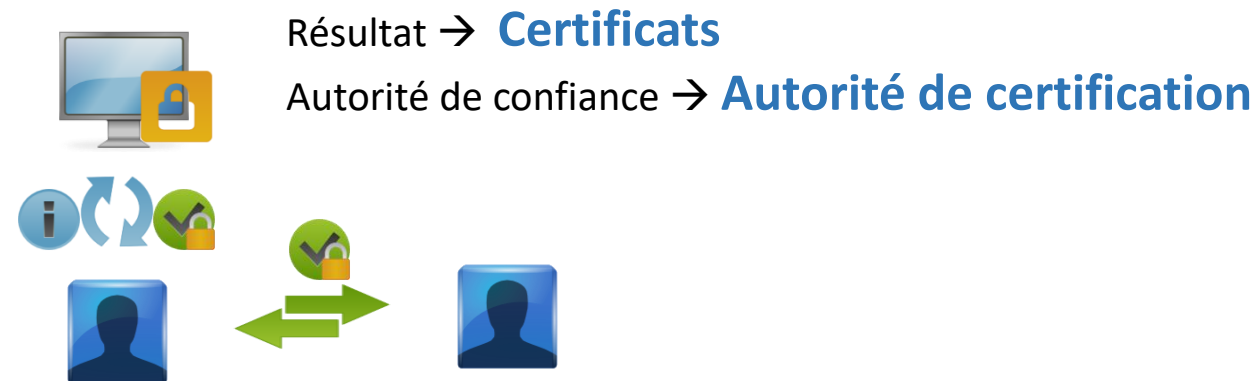
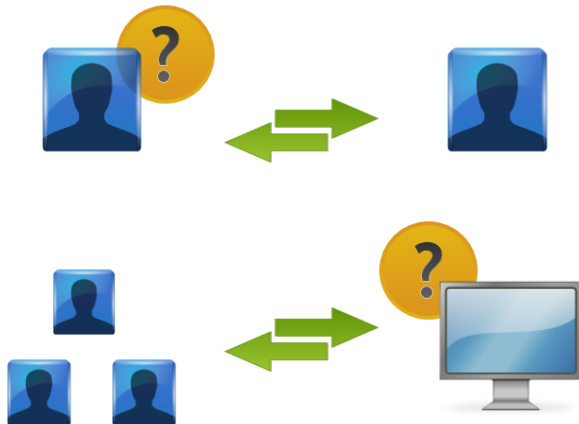


❑ Risques



PKI : Risques

- Comment assurer son identité vis-à-vis d'un tiers ?
- Comment assurer que des entités sont bien celles qu'elles prétendent être?
- Une « autorité de confiance » signe avec sa clé privée un document contenant
 - L'identité d'une entité possédant un couple de clé
 - La clé publique
 - Des informations décrivant l'usage de cette clé



PKI : Usage

- Qui utilise les certificats ?
 - IPsec
 - SSL
 - S/MIME (PGP)
 - Signature de code de package (Java, Javascript, ActiveX,...)
 - Signature de formulaire,...

- Format de type de certificats
 - X509 PKIX (UIT, 1988, RFC 5280)
 - PKCS (rsa)
 - PGP (Phil Zimmermann, 1991, GnuPG)
 - SPKI/SDSI (IETF,1996, RFC 2692, RFC 2693)



PKI : Les acteurs

☐ Les utilisateurs (homme, machine, service)

Entités utilisant les certificats afin de vérifier l'identité d'autres utilisateurs mais aussi afin de connaître la clé publique des ces derniers

☐ L'autorité de certification – Certification Authority (CA)

Entité de confiance délivrant et révoquant des certificats (certificats à clé publique)

☐ L'autorité d'enregistrement – Registration Authority (RA)

Entité en qui le CA a confiance pour vérifier l'identité de l'utilisateur



PKI : Les acteurs

❑ Certificat

Object représentant l'identité d'un utilisateur et contenant la clé publique de ce dernier

❑ Annuaire de certificats -Certificate Repository

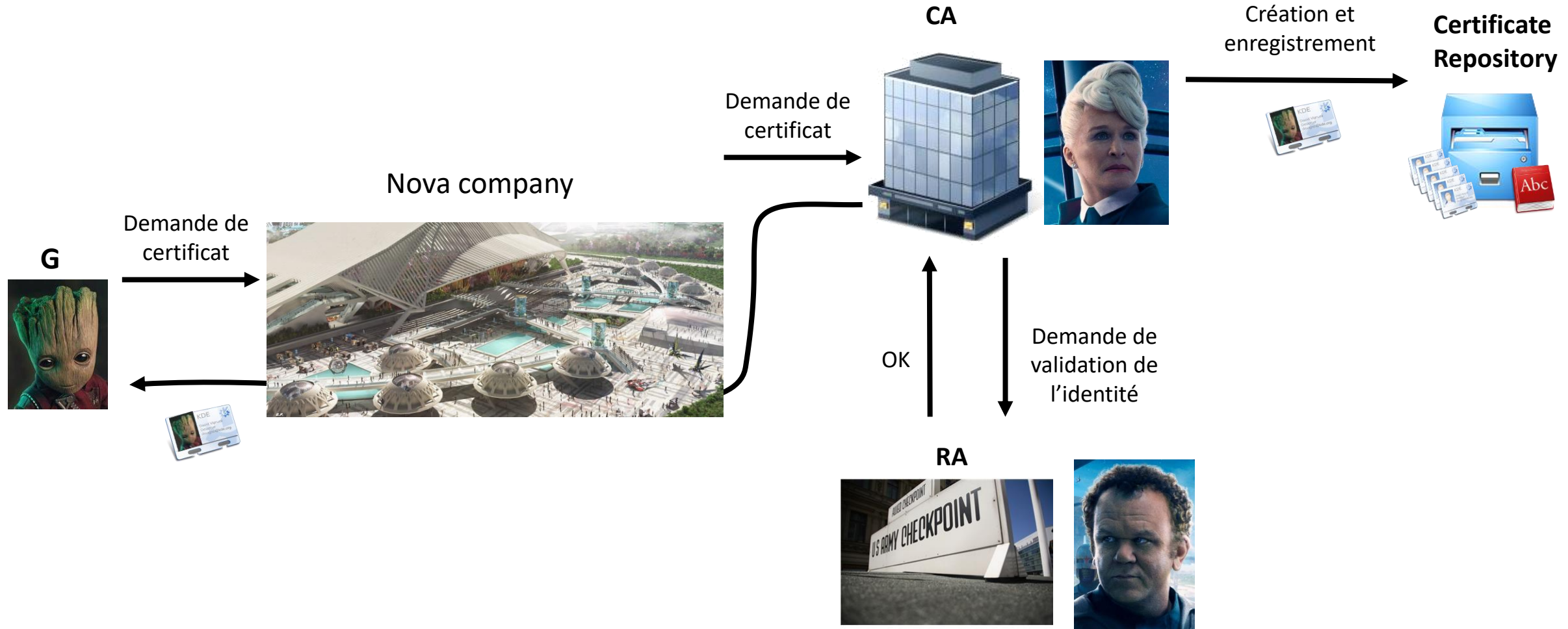
Object regroupant l'ensemble des certificats et des listes de révocation et les rend publique

❑ Liste de révocation des certificats – Certificate Revocation List (CRL)

Object regroupant l'ensemble des certificats révoqués



PKI : Les acteurs

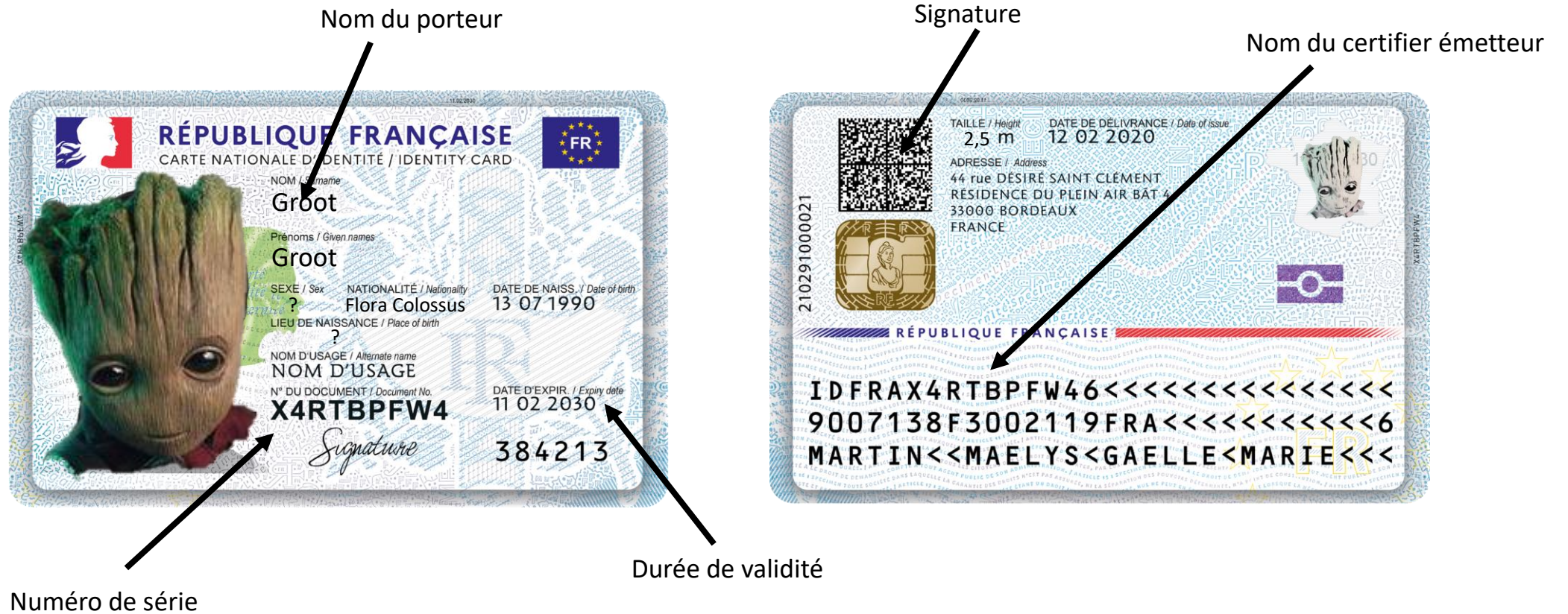


PKI : Contenu d'un certificat

- Numéro de série
- Identité du porteur (owner)
- Identité du certifier émetteur (issuer)
- Période de validité (début-fin)
- Classe de certificat
- Clé public du porteur (+algo utilisé, longueur des clés,...)
- Signature (+algo utilisé, longueur des clés,...), auto-signé ou non



PKI : Contenu d'un certificat



- + Classe
- + Clé publique du porteur

PKI : Contenu d'un certificat

:

Numéro de série

Data:
Version: 3 (0x2)
Serial Number: 1 (0x1)

Nom du certifier émetteur

Signature Algorithm: sha1WithRSAEncryption
Issuer: C=FR, ST=Rhone_Alpes, L=Villeurbanne, O=INSA-LYON,
OU=Dept Telecom, CN=CA/emailAddress=mitsuco26@hotmail.com

Durée de validité

Validity
Not Before: Jun 9 08:43:11 2011 GMT
Not After : May 9 08:43:11 2013 GMT

Nom du porteur

Subject: C=FR, ST=Rhone_Alpes, L=Villeurbanne, O=INSA-LYON,
OU=Dept Telecom, CN=serveur radius/emailAddress=mitsuco26@hotmail.com

Clé publique du porteur

Subject Public Key Info:
Public Key Algorithm: rsaEncryption
RSA Public Key: (1024 bit)
Modulus (1024 bit):
00:b8:d1:ce:aa:e7:36:07:7f:46:5d:15:8d:24:25:
a7:2b:08:7d:5d:2c:78:21:94:8d:f0:c3:99:dd:d9:
18:8d:7d:89:5c:7a:43:b8:a5:4c:2c:69:db:49:4b:
e1:ea:9f:83:59:53:6b:6f:da:9e:5a:d3:ac:46:2f:
33:21:50:ac:f3:cc:c2:27:6e:e2:f2:d4:50:4d:fb:
f1:15:4f:3e:60:9b:07:6a:6c:65:17:bd:7c:c2:f7:
a1:d5:25:2f:23:35:39:d1:1f:ff:66:4e:ff:d6:7b:
04:50:e0:12:6e:71:7e:f3:bf:01:3a:d2:29:4a:bd:
7d:e1:89:9c:bf:1e:4a:60:99
Exponent: 65537 (0x10001)

X509v3 extensions:
X509v3 Basic Constraints: critical
CA:FALSE
X509v3 Authority Key Identifier:
keyid:30:5B:05:AA:6E:D3:AE:2D:CD:45:25:05:0A:1F:A0:68:62:E5:67:7
X509v3 Subject Key Identifier:
54:52:FF:F4:94:39:18:5F:0A:9D:51:5C:AD:01:39:35:78:39:6F:35
X509v3 Key Usage:
Digital Signature, Key Encipherment
X509v3 Extended Key Usage:
TLS Web Server Authentication, TLS Web Client
Authentication
Netscape Cert Type: SSL Server
Netscape Comment: Certificat delivre par Dept Telecom

Classe

X509v3 Key Usage:
Digital Signature, Key Encipherment
X509v3 Extended Key Usage:
TLS Web Server Authentication, TLS Web Client
Authentication

Signature

Signature Algorithm: sha1WithRSAEncryption
14:d2:ca:7d:66:5e:73:50:e3:28:14:30:cc:8c:ce:29:a8:d0:
2c:fc:bd:ed:55:8c:60:43:c4:dc:1b:c9:6c:ef:59:ae:a8:54:
e7:fa:e0:16:3b:2e:27:80:97:3c:f2:35:82:eb:4d:b3:33:ee:
19:78:7e:f2:51:be:75:5f:78:32:23:65:9e:7f:f8:65:41:90:
9c:41:6e:5d:5a:8c:94:52:06:e8:5c:b5:c1:d2:35:8d:90:37:
1d:50:1e:7e:91:2b:67:b0:bf:c3:94:8e:0a:f5:54:3d:57:7b:

PKI : Génération pair de clés

❑ Par le client

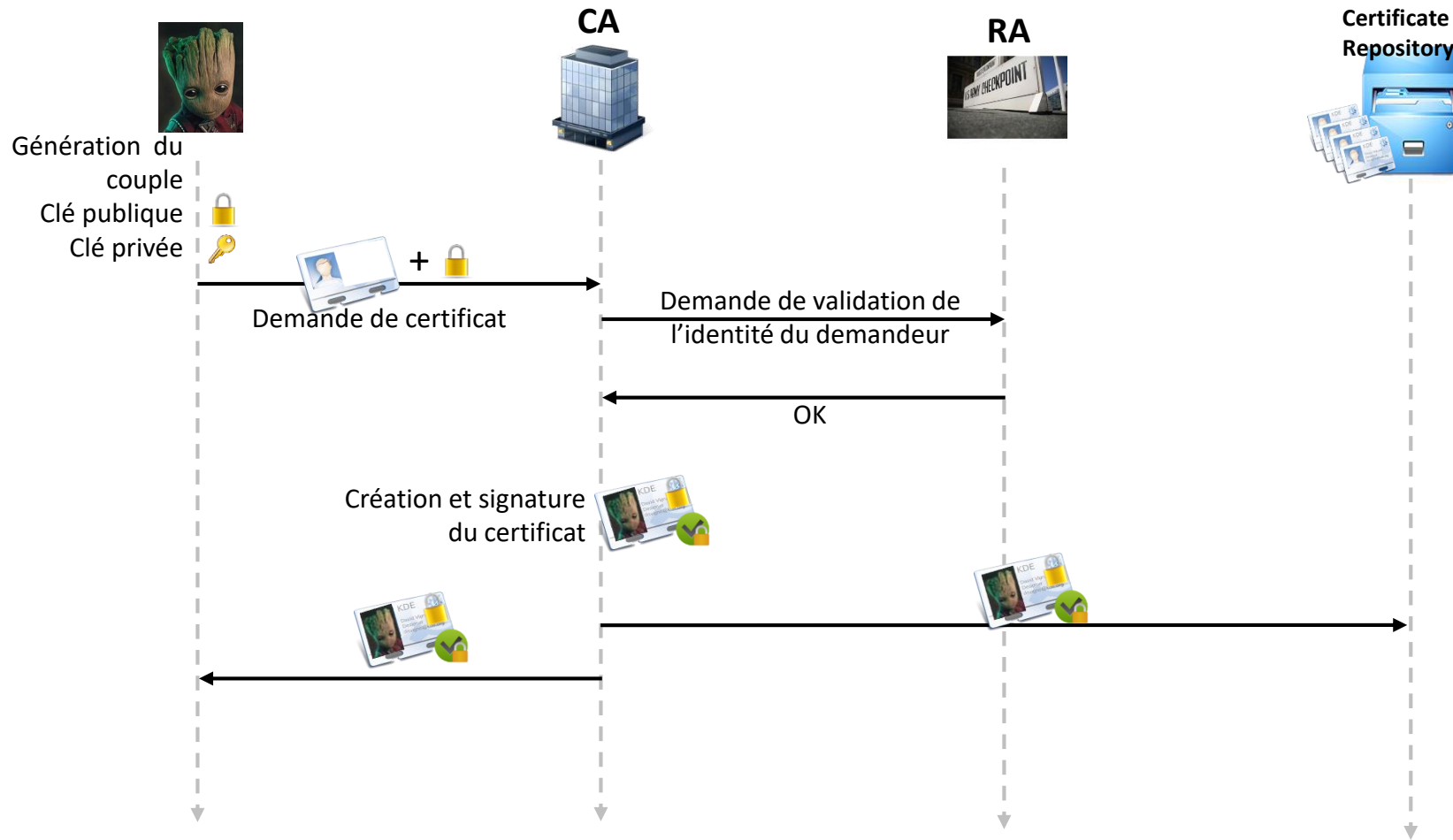
- Pas de communication de clés privées
- CA ne connaît pas la clé (perte de clé? Départ?)

❑ Par le CA

- Génération de clés plus sur (complexité, nombres aléatoires)
- Archivage de la clé privée
- Historique des paires de clés
- Doit transmettre de façon sécurisée la clé privée



PKI : Cycle de vie

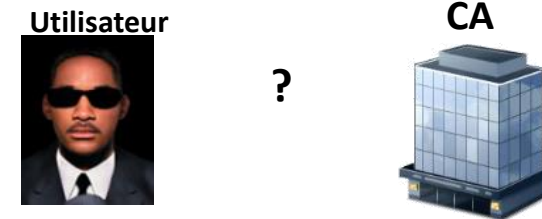


PKI : Certification des certificats A vous de jouer

1. Comment le CA fait –il pour certifier le certificat ?



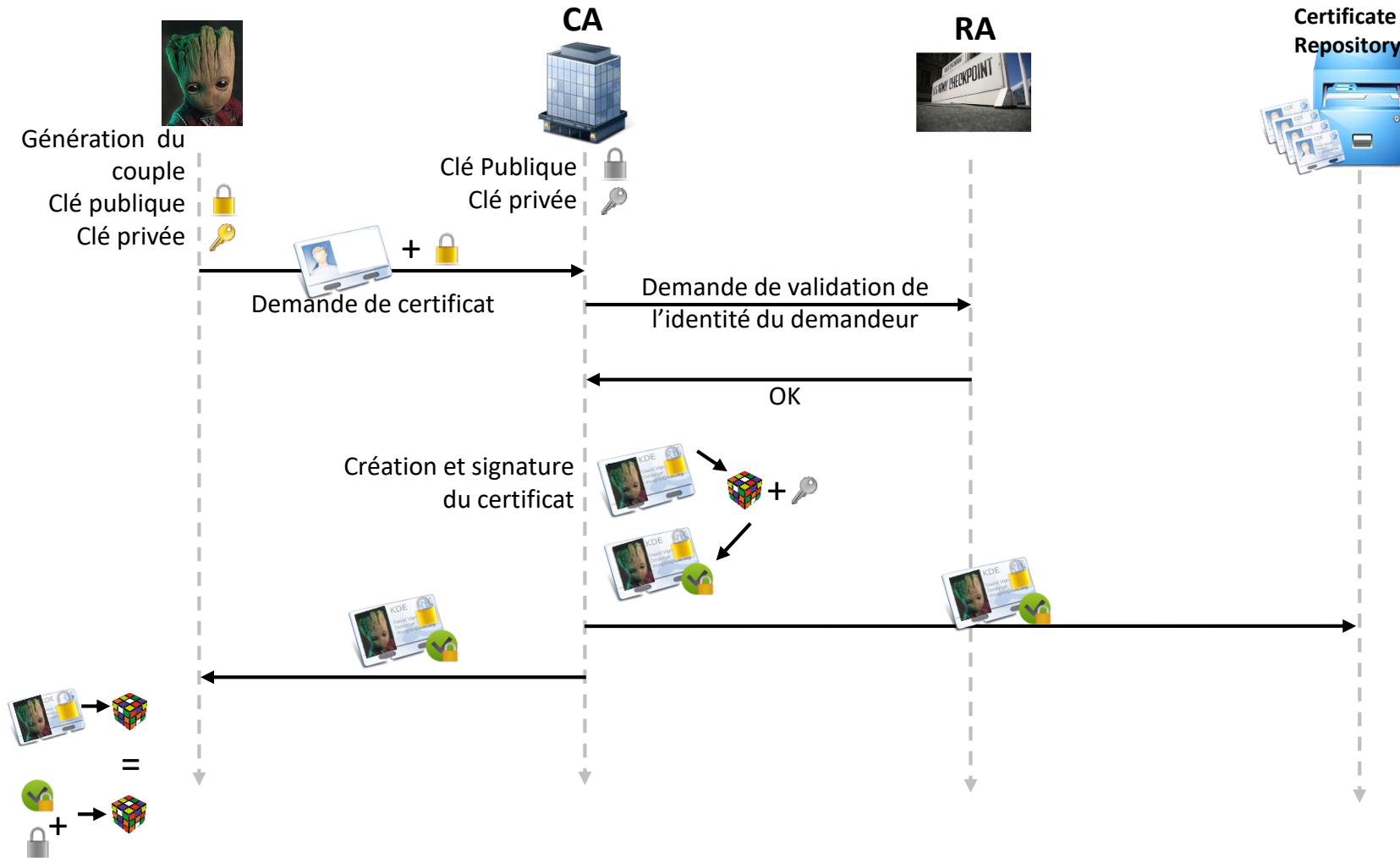
2. Comment l'utilisateur peut –il être sur de communiquer avec le CA ?



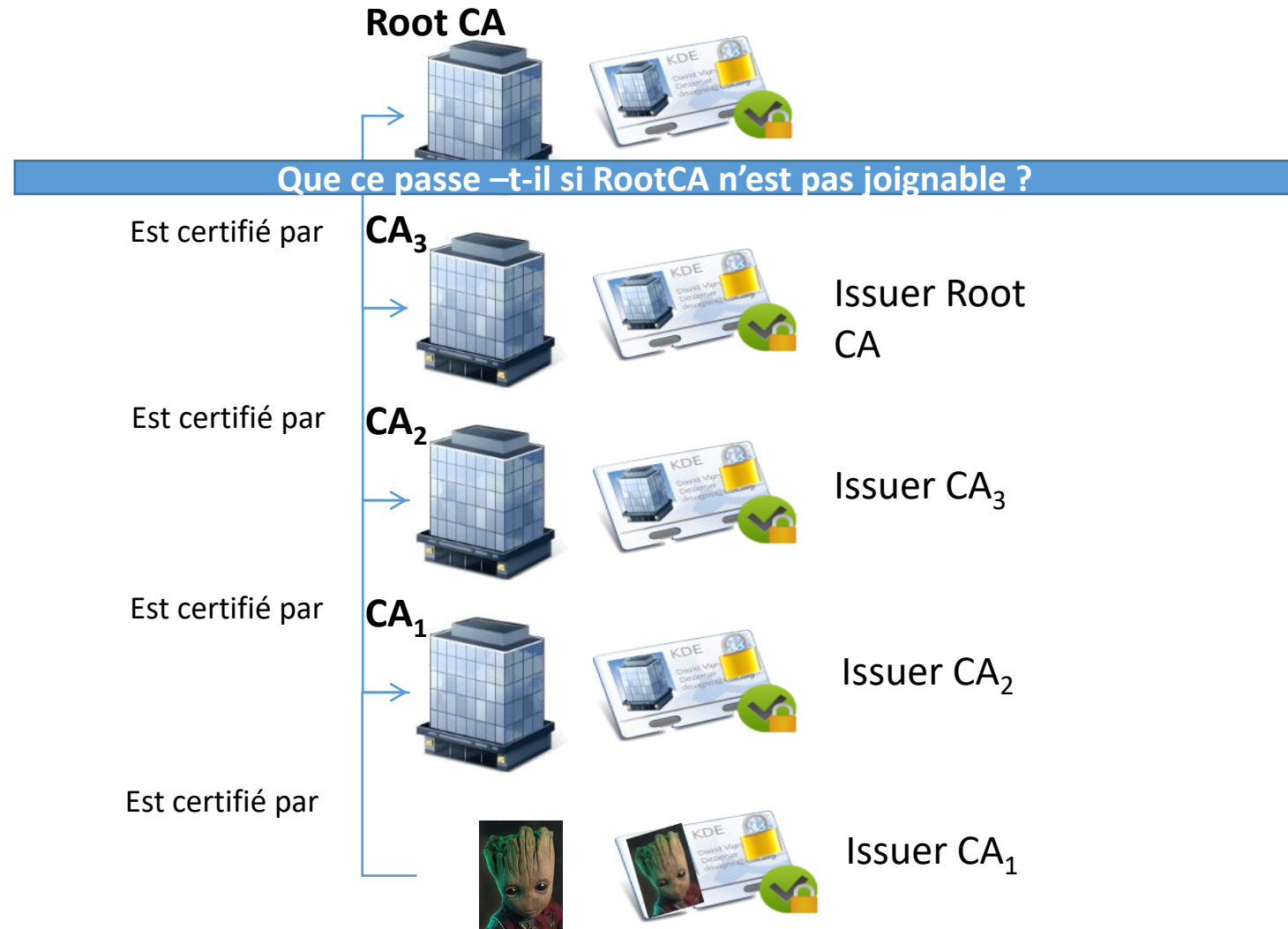
3. Comment l'utilisateur est sur que son certificat n'a pas été modifié et provient bien du CA ?



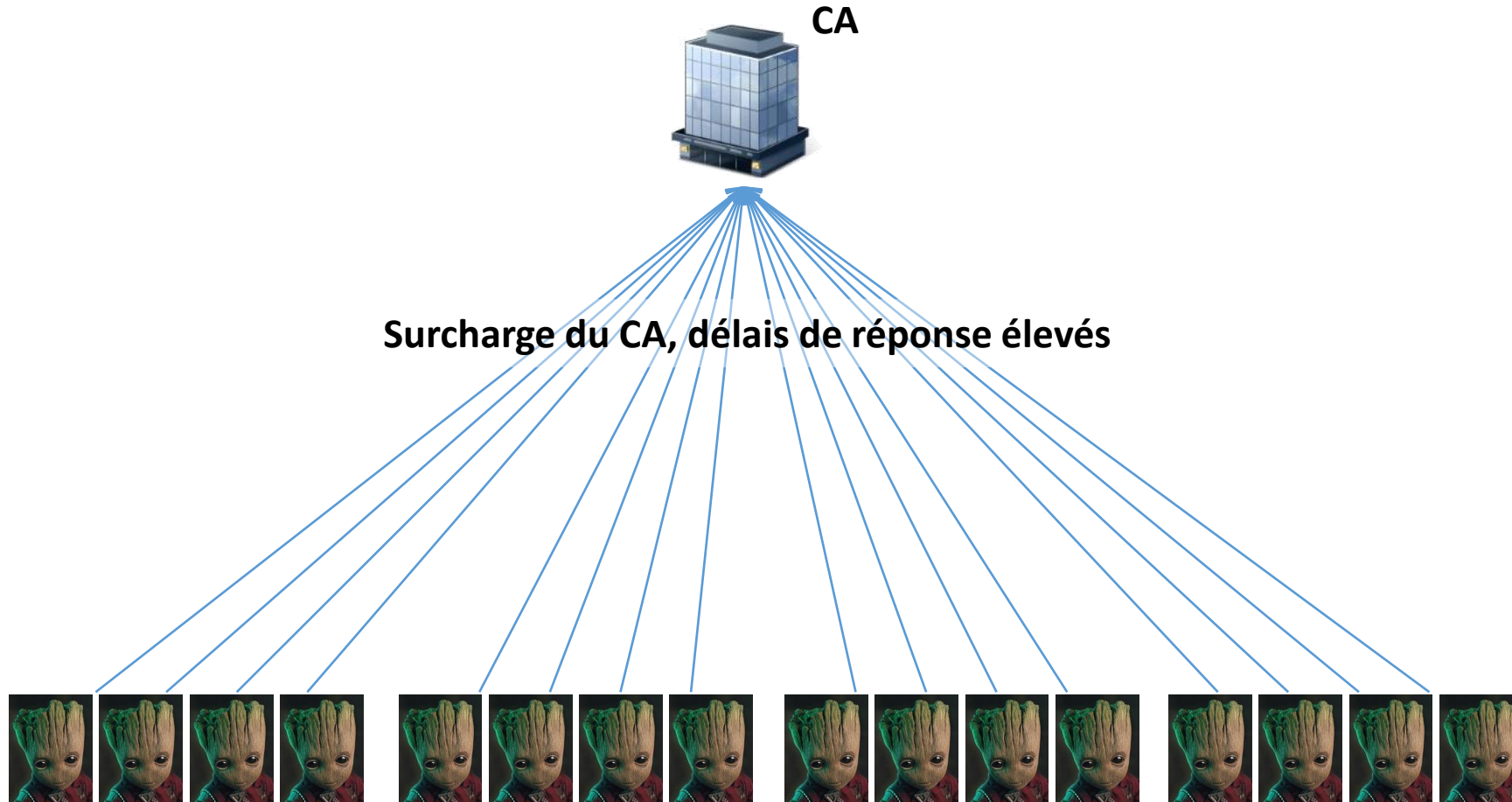
PKI : Cycle de vie



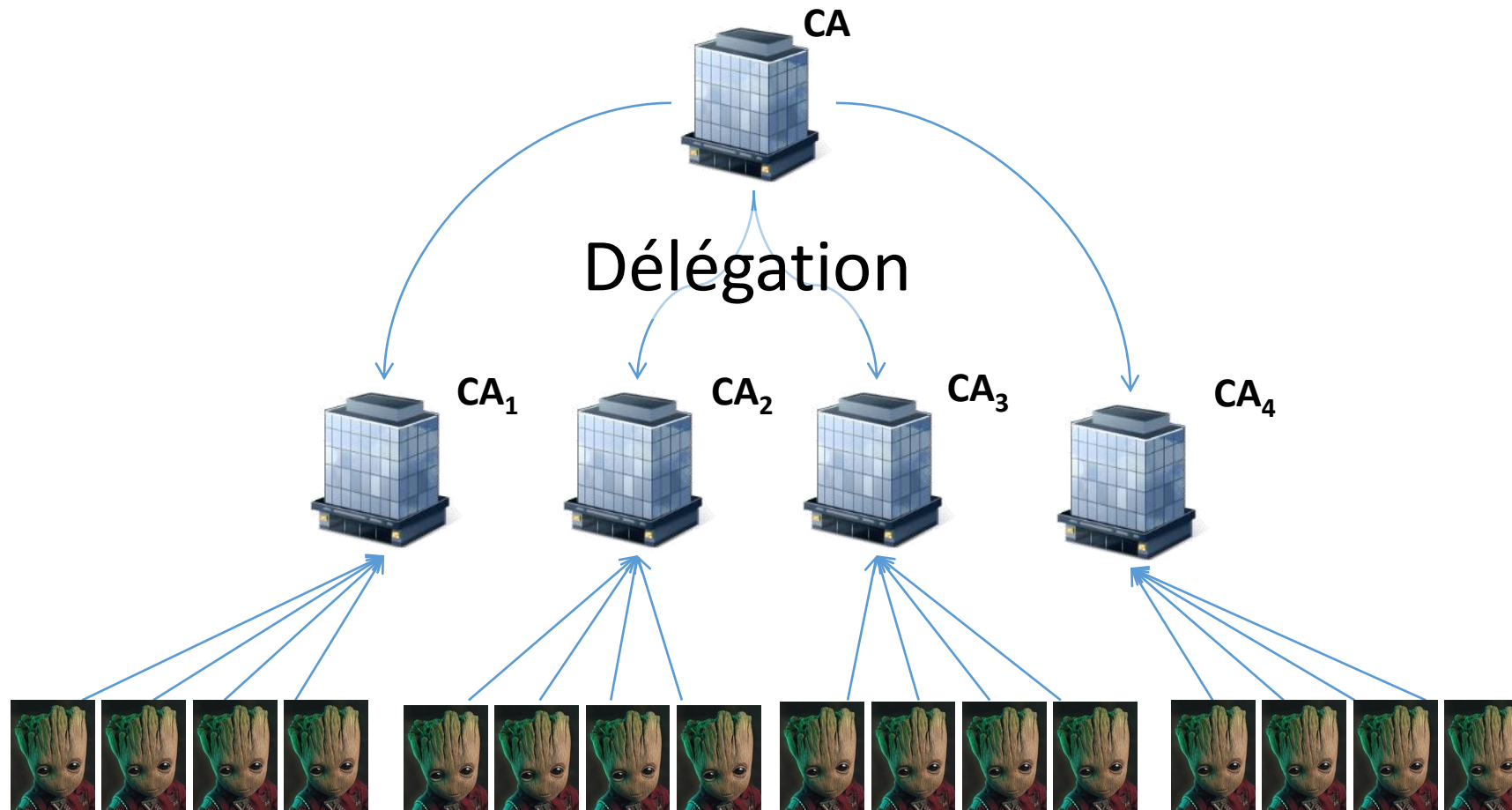
PKI : Chaîne de certification



PKI : Délégation



PKI : Délégation



PKI : Génération pair de clés

- Organisme publique
 - Pas gratuit
 - Verisign, Thawte, Entrust, Baltimore
 - Certinomis (la poste, chambre du commerce,...)
 - Certplus (Verisign,Matra, France Telecom, Gemplus)
 - Reconnaissance externe, internationale

- Locale privée
 - Gestion de sa propre autorité de certification
 - Périmètre de reconnaissance limitée
 - Flexibilité de gestion
 - Openssl, OpenCa, IDX-PKI , iPlanet Certificate Manager server



PKI : Certification des certificats A vous de jouer

1. A quelle problématique réponds les PKI



2. Quelles objectifs de sécurité permettent d'assurer les certificats?



PKI : Le contenu de vos postes

Demo



Sécurité Internet

- **HTTPS/Secure HTTP**
- Secure Electronic Transaction
- SSH

Sécurité Internet : HTTPS

- Besoin comment sécuriser des communications sur internet sécurisée ?
 - utilisation de http over SSL/TLS → HTTPS
- Nouveau port de communication 443 (http port 80)
- SSL utilise le chiffrement asymétrique afin de fournir
 - Chiffrement de données (via une clé de session)
 - L'authentification du serveur (et celle du client optionnelle)
 - L'intégrité des données



Free 3D rendering - resolution 400x250 px - www.psdgraphics.com

Sécurité Internet : HTTPS

- Pourquoi toutes les communications ne sont pas en HTTPS ?
 - Consommation de ressources (liée au chiffrement asymétrique)
 - Certificat du server web (coût)
 - Communications plus lentes (liées au chiffrement)



Free Vector, PNG file download ... Resolution: 4000x2500 px ... www.psdgraphics.com

Sécurité Internet : HTTPS

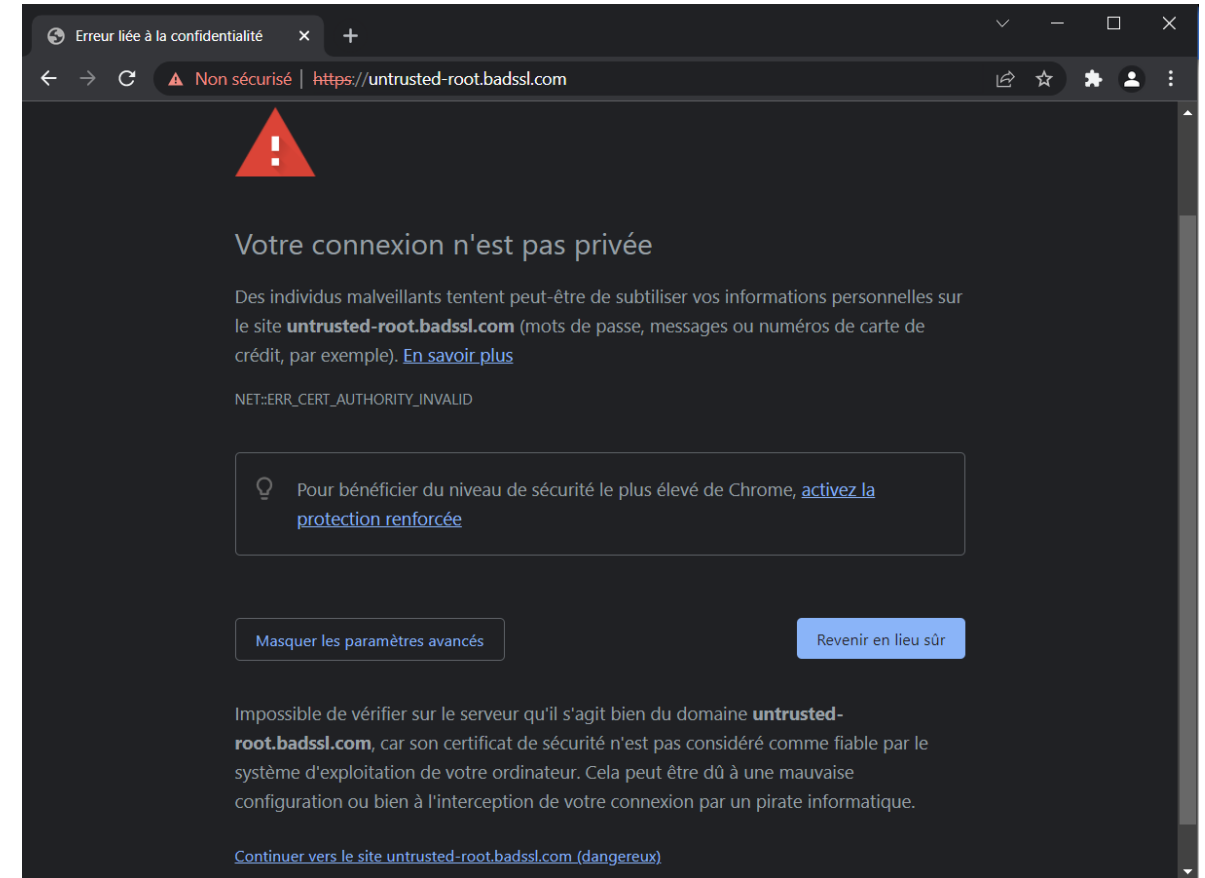
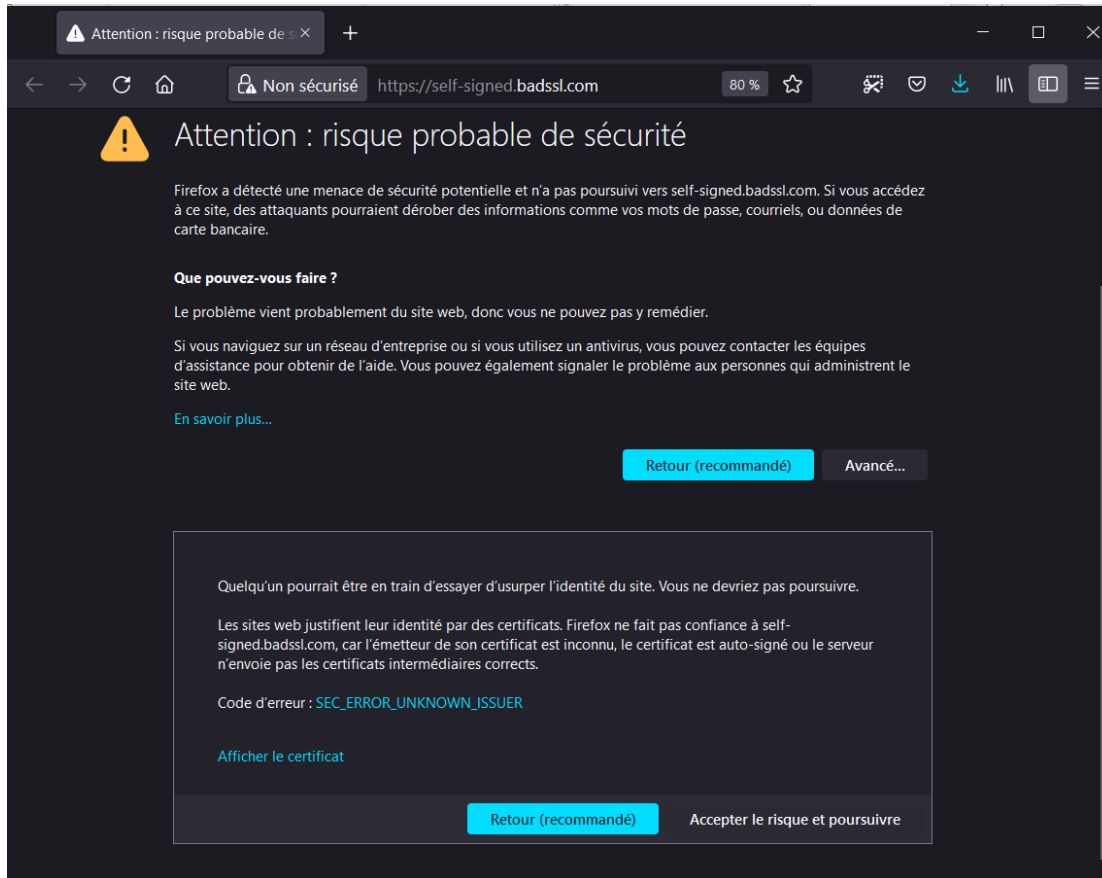
Le maillon faible



VOUS !

Copyright © Jacques Saraydaryan

Sécurité Internet : HTTPS



Sécurité Internet : HTTPS

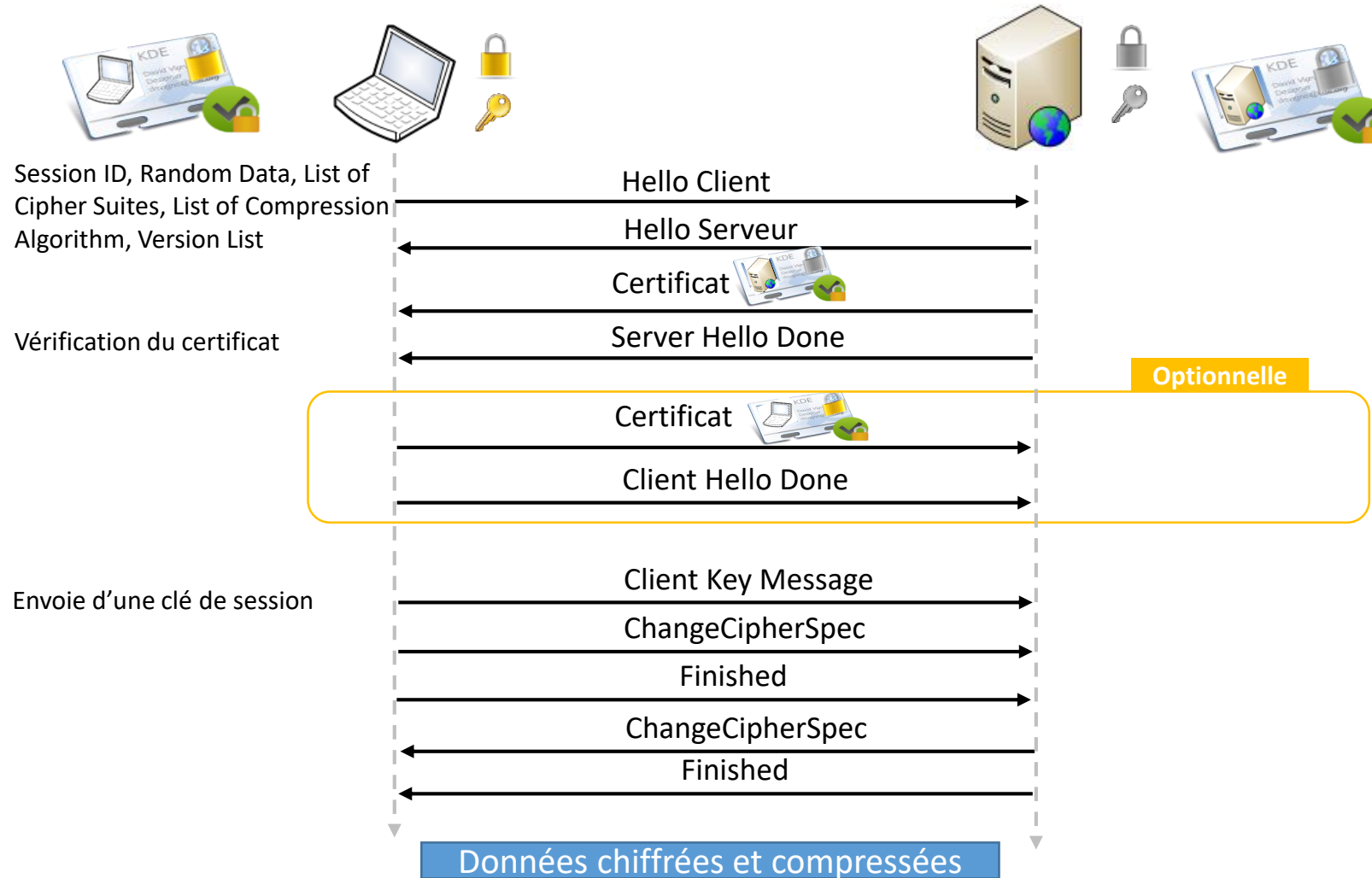
- TLS Transport Layer Security anciennement (SSL Secure Socket Layer)

Application		
Présentation	HTTPS	
Session		
Transport	SSL/TLS	TCP
Réseau	IP	
Liaison		
Physique		



Free 3D rendering of https://www - resolution 400x250 px - www.psdgraphics.com

Sécurité Internet : HTTPS- SSL/TLS



Sécurité Internet : HTTPS- SSL/TLS

Demo wireshark



Sécurité Internet

- HTTPS/Secure HTTP
- **Secure Electronic Transaction**
- SSH

Secure Electronic Transaction

- 1996 VISA/MasterCard
- Objectif: Sécuriser les transactions bancaires sur un réseau non sécurisé
- Repose essentiellement sur le chiffrement asymétrique et la signature numérique
- Permet d'assurer l'authenticité des utilisateurs, la confidentialité de l'information et l'intégrité du paiement

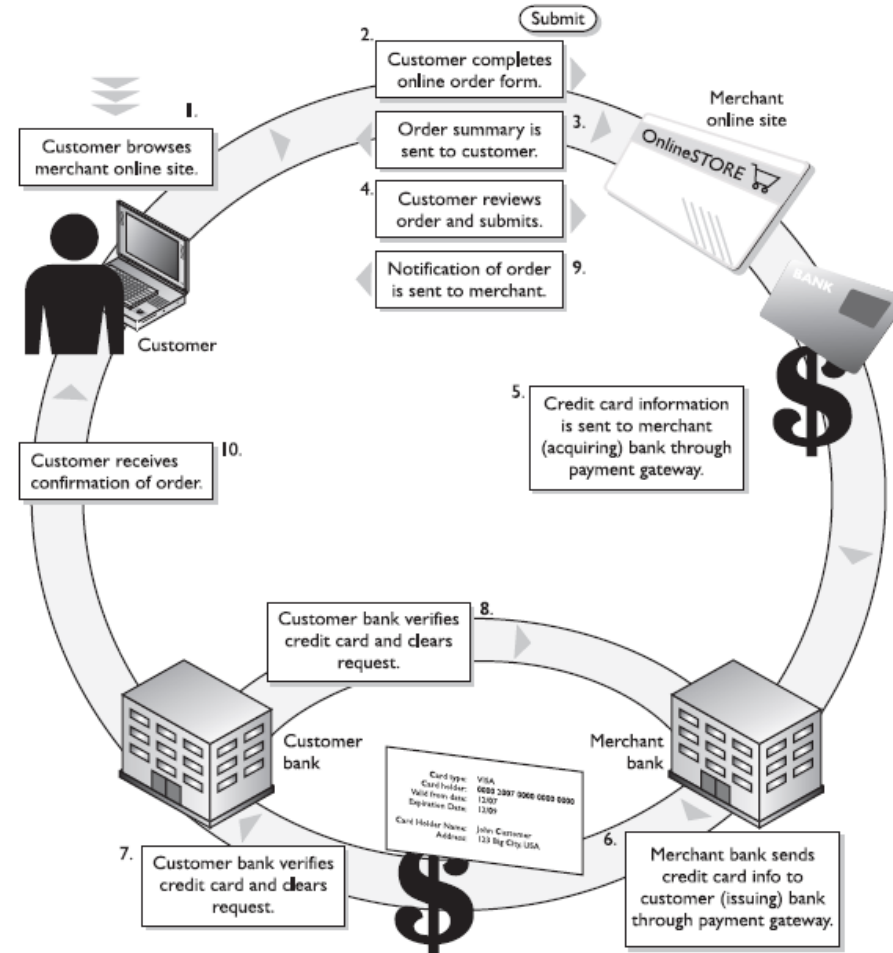


Secure Electronic Transaction

- Les entités
 - Banque du demandeur (issuer)
 - L'utilisateur de la carte de crédit (Cardholder)
 - Marchand (merchant)
 - Banque du marchand (Acquierer)
 - Passerelle de paiement (Payment gateway)



Secure Electronic Transaction

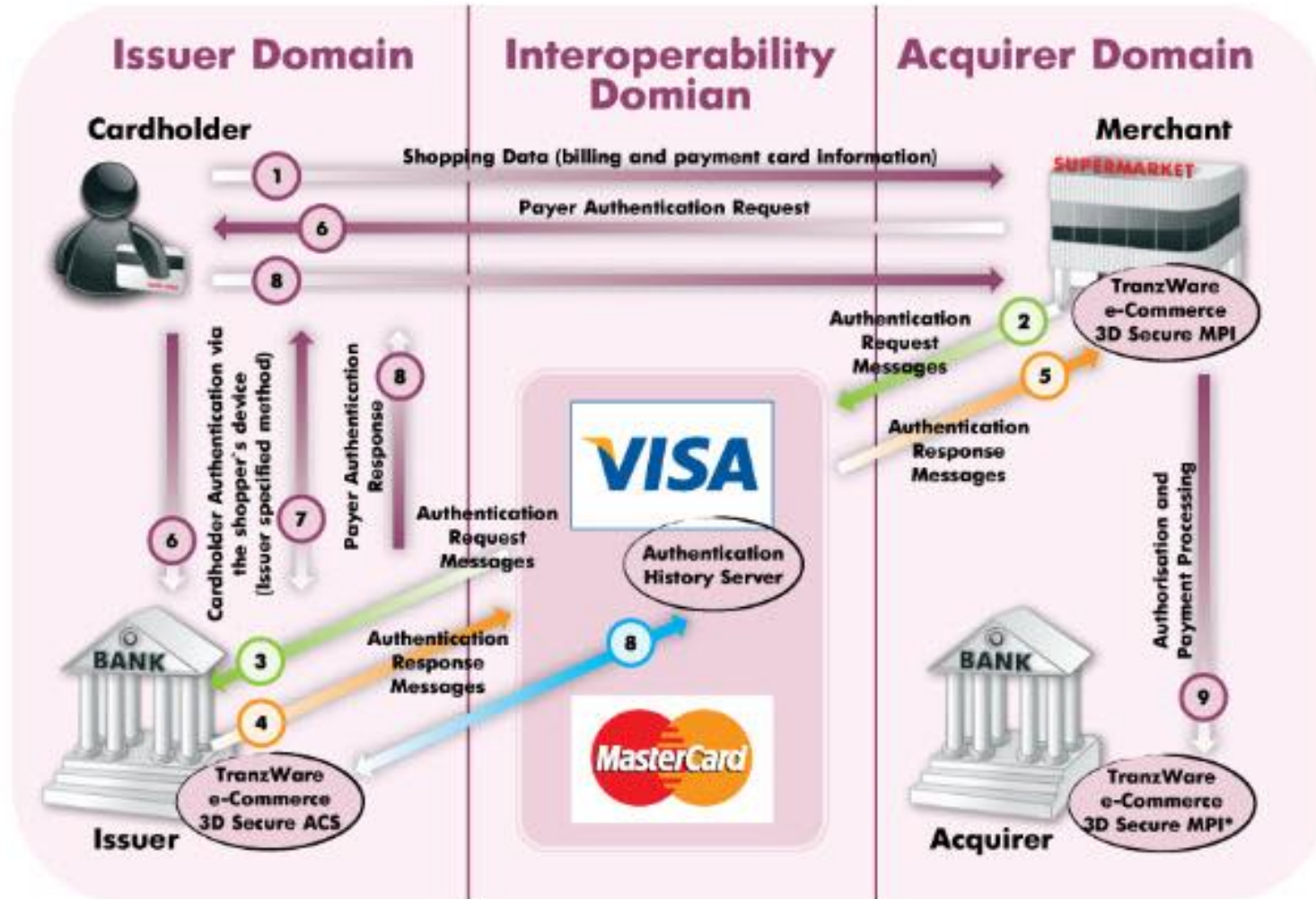


3D-Secure

- VISA/MasterCard
- Objectif: Autorisation financière avec authentification en ligne
- Actuellement le système de paiement le plus utilisé



3D-Secure



www.infogram.co.id/solutions/electronic-payment-system/3d-secure-compliant-solution

Copyright © Jacques Saraydaryan



Sécurité Internet

- HTTPS/Secure HTTP
- Secure Electronic Transaction
- **SSH**

Secure Shell - SSH

- Protocole de communication V1 (1995), V2 (2006)
- Utilisation du port 22
- Mode client serveur
- Redirection de port (forwarding)
- Objectif
 - Chiffrer et compresser un canal de communication
 - Ensemble d'outils permettant de remplacer des outils de connexions non sécurisés (rpc, rlogin, rsh, telnet)
 - Mots de passe et données chiffrés lors de la communication

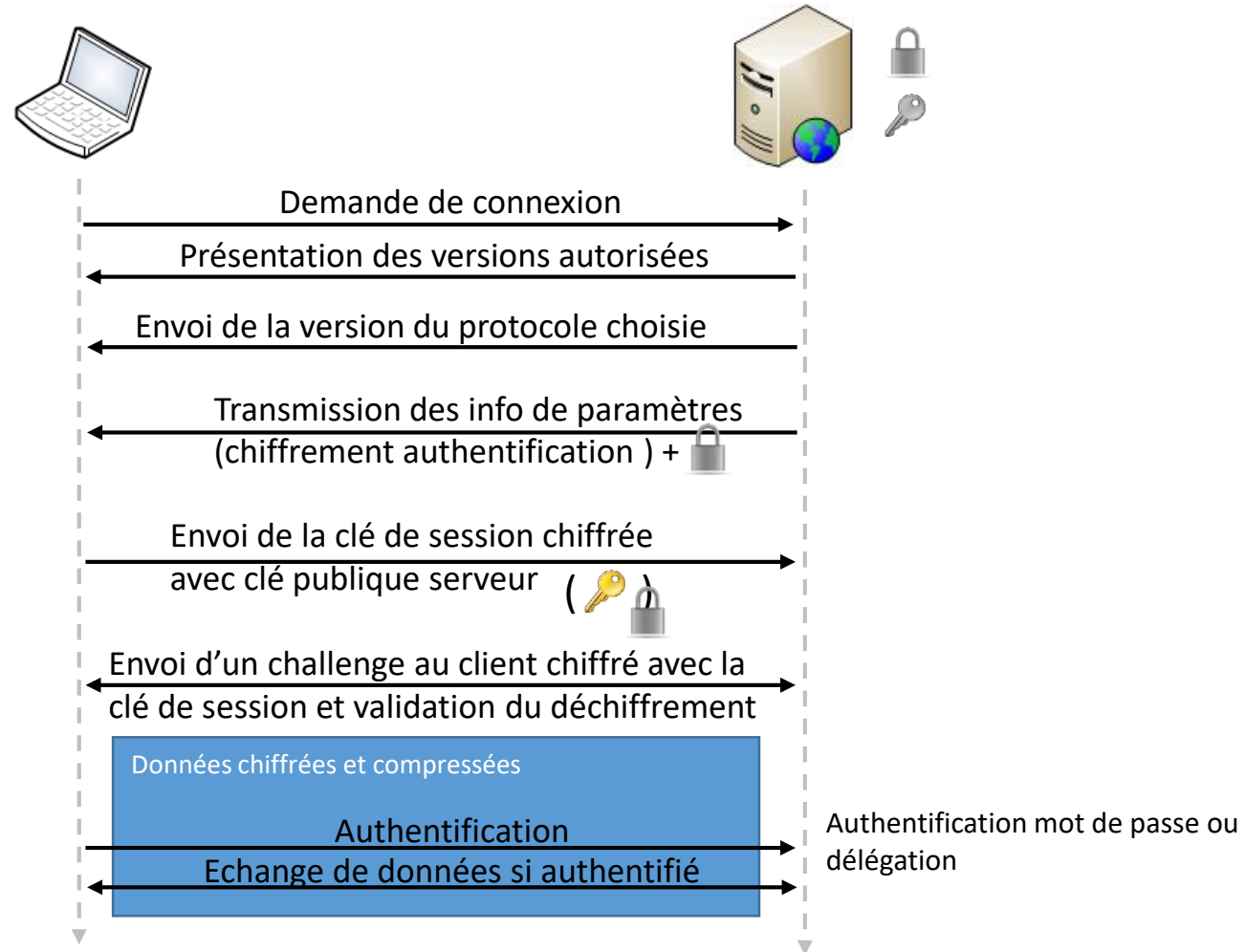


Secure Shell - SSH

- Exemple d'utilisation d'algorithme sous linux
 - Chiffrement asymétrique
 - RSA, DSA
 - Chiffrement symétrique
 - 3DES, Blowfish, AES..
- Gestion de l'authentification
 - Possibilité d'activer le support de l'interface PAM (Pluggable Authentication Modules)



Secure Shell - SSH





Conclusion



Questions ?



Jacques Saraydaryan

Jacques.saraydaryan@cpe.fr