Sécurité pratique

Chapitre 3: Chiffrement pratique

Printemps 2022

Prof. Marcelo Pasin

haute école
neuchâtel berne jura
arc ingénierie
www.he-arc.ch

Introduction au chiffrement

- Stallings & Brown, Chapitre 2

- Outils cryptographiques
- Confidentialité avec chiffrement symétrique
- Authentification des messages et fonctions de hachage
- Chiffrement asymétrique
- Signatures numériques et gestion des clés

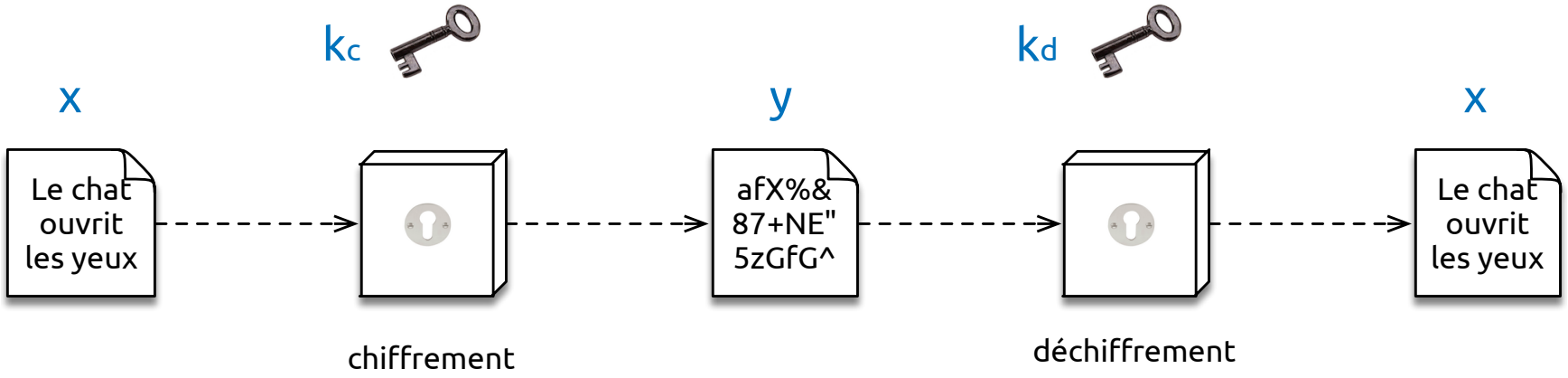
Objectifs d’apprentissage

- Être capable de:
  - Expliquer le fonctionnement de base des algorithmes de chiffrement par blocs symétriques.
  - Comparez et contrastez le chiffrement par bloc et par flot
  - Discuter l'utilisation des fonctions de hachage sécurisées pour l'authentification des messages.
  - Répertorier des applications des fonctions de hachage sécurisées
  - Expliquer le fonctionnement de base des algorithmes de chiffrement par blocs asymétriques
  - Présenter un aperçu du mécanisme de signature numérique et expliquer le concept des enveloppes numériques

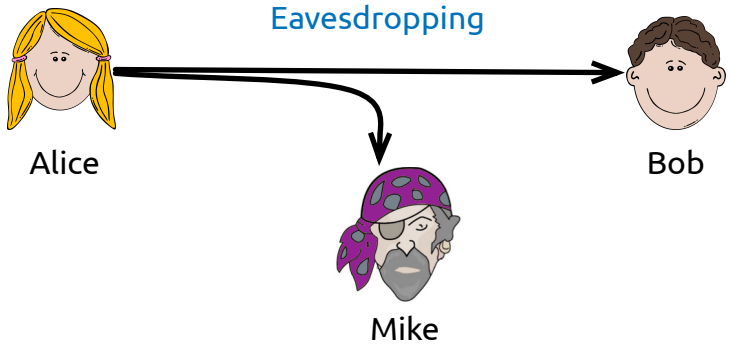
Cryptographie

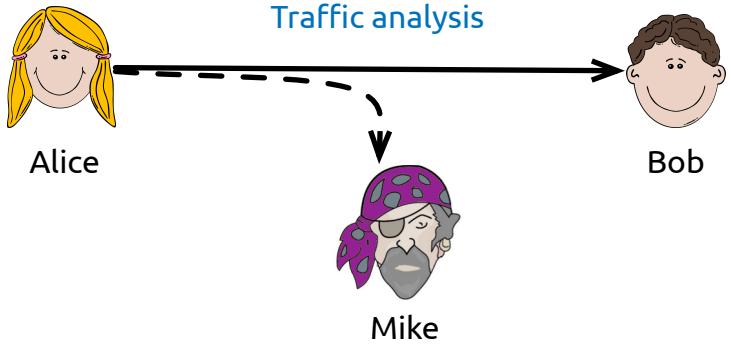
- Cryptologie
  - Cryptographie - écriture sécrète
  - Cryptanalyse - déchiffrer sans clé

- Message non-chiffré
  (texte non-crypté, en clair / *clear text, plain text*)
- Message chiffré (texte crypté / *cipher text*)
- Chiffrement (*encryption cipher*) / déchiffrement (*decryption*)
- Clé, paramètre secret (*key*)

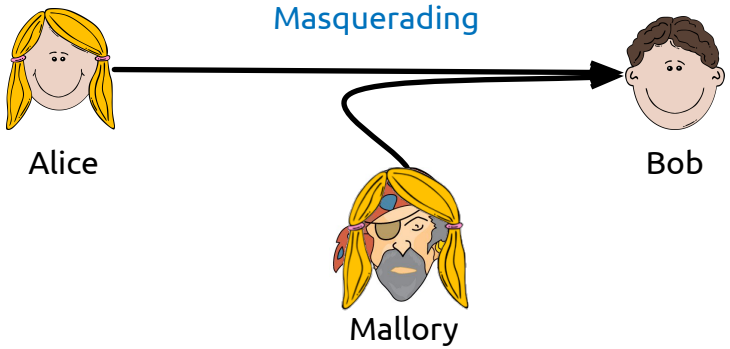


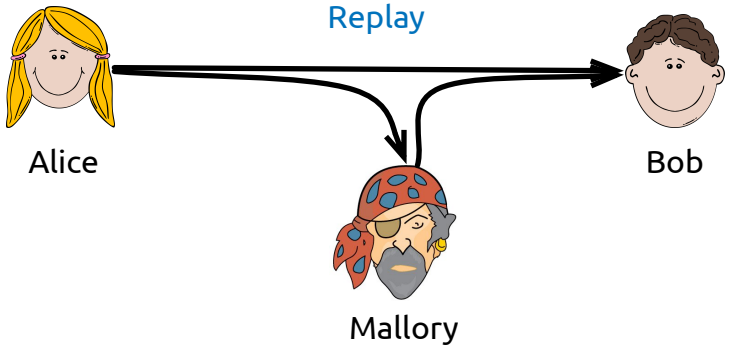
Attaques passives

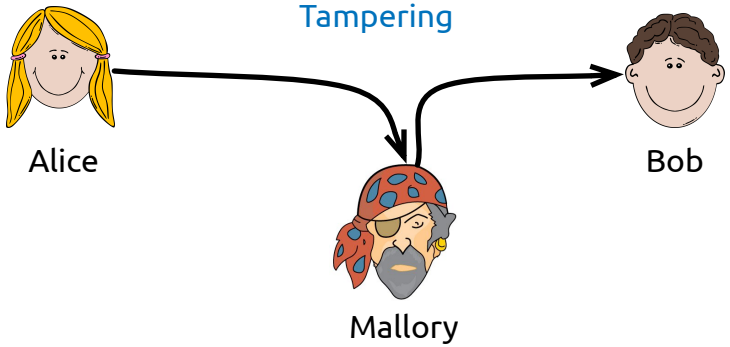




Attaques actives







Attaques résolus
par le chiffrement
(a voir comment)

Historique

- Scytale
  (7ème siècle avant J.C.?)

- Le disque de César
  100-44 avant J.C.

- Chiffre de Vigenère
  1586

Key	Plaintext																									
	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

- Enigma
  1920-1970

La Scytale - transposition

- Chiffrement par transposition
- Exemple “WHAT WAS THE WEATHER LIKE ON FRIDAY"

```
WHAT WAS
 THE  WEA
THER LIK
E ON FRI
DAY
```

- Message chiffré

“W TEDHTH AAHEOYTERN WWLF AEIR SAKI ”

- Facile à déchiffrer :
- Clé est un diviseur de la taille du message

Permutation

$$\pi = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 4 & 3 & 1 & 6 & 2 & 5 \end{pmatrix}$$

- Chiffrement par permutation
- La clé donne les positions a échanger dans un bloc

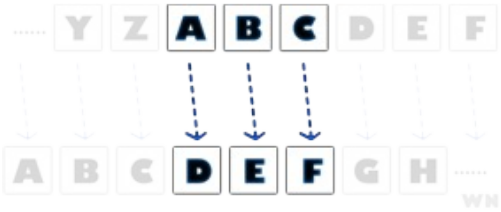
- “WHAT WAS THE WEATHER LIKE ON FRIDAY”

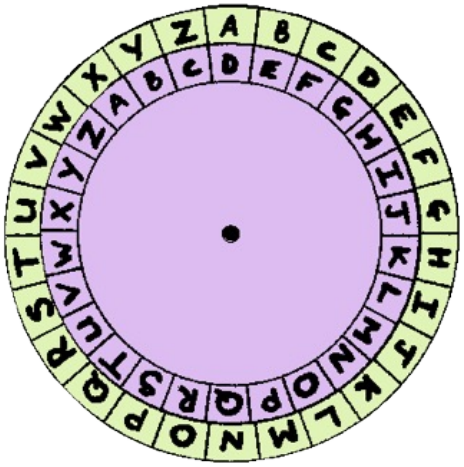
WHAT W	TAWWH
AS THE	T AESH
WEATHE	TAWEEH
R LIKE	ILRE K
ON FRI	F OINR
DAY	YD D

- Message chiffré
  - “TAWWH T AESH TAWEEH ILRE K F OINR YD D ”

Le disque de César - substitution

- Chiffrement par substitution





- Généralisation:
  - Clé = déplacement choisi

Recherche par force brute

clé	message	clé	message	clé	message
0	XMZVH	17	GVIEQ	8	PERNZ
25	YNAWI	16	HWJFR	7	QFSOA
24	ZOBXJ	15	IXKGS	6	RGTPB
23	APCYK	14	JYLHT	5	SHUQC
22	BQDZL	13	KZMIU	4	TIVRD
21	CREAM	12	LANJV	3	UJWSE
20	DSFBN	11	MBOKW	2	VKXTF
19	ETGCO	10	NCPLX	1	WLYUG
18	FUHDP	9	ODQMY		

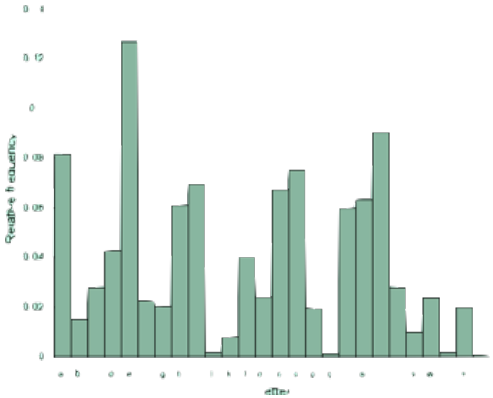
Chiffrement par substitution

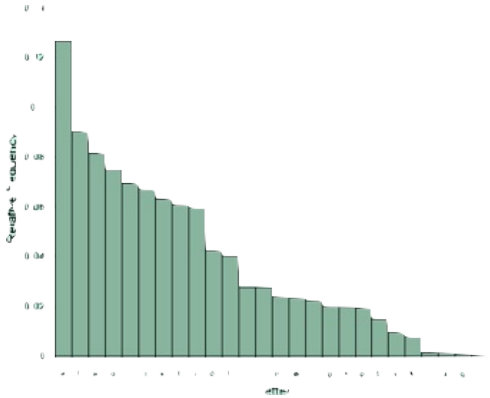
- Substitution quelconque

A	*B*	*C*	*D*	*E*	*F*	*G*	*H*	*I*	*J*	*K*	*L*	*M*
D	**I**	**Q**	**M**	**T**	**B**	**Z**	**S**	**Y**	**K**	**V**	**O**	**F**

N	*O*	*P*	*Q*	*R*	*S*	*T*	*U*	*V*	*W*	*X*	*Y*	*Z*
E	**R**	**J**	**A**	**U**	**W**	**P**	**X**	**H**	**L**	**C**	**N**	**G**

- 403'291'461'126'605'635'584'000'000 clés (26!)





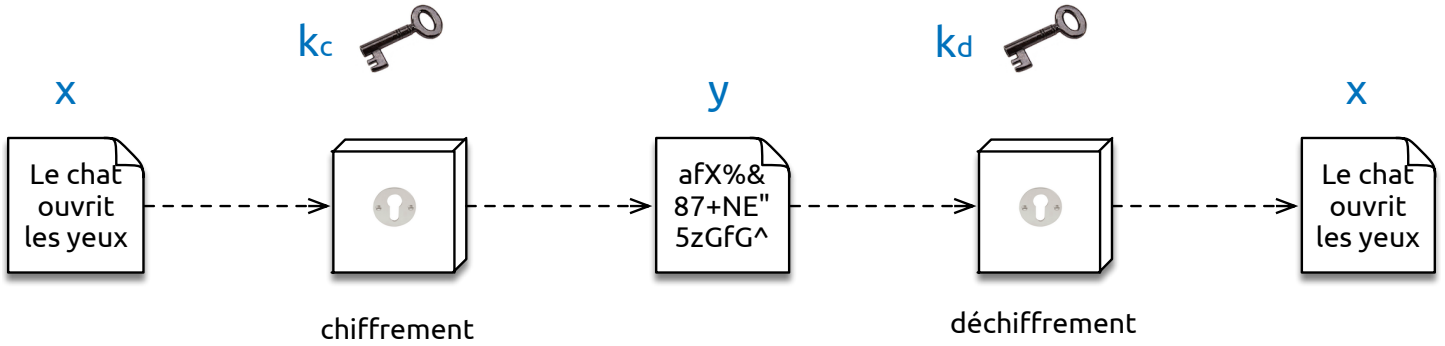
Arithmétique modulaire

- La plupart des systèmes de chiffrement sont
  - Discrets (nombres entiers)
  - Finis (non infini)

- On utilise alors l'arithmétique modulaire
- Autres exemples
  - Horloge
  - Preuve par neuf

- Opération modulo
  - Soient ***a***, ***r***, ***m*** des entiers, avec ***m>0***
  - Si ***(r-a)*** est divisible par ***m***, ***a modulo m = r***.
- ***m*** est dit le modulo
- ***r*** est dit le reste

Le disque de César en arith modulaire



$$y = e_k(x) \qquad x = d_k(y)$$

$$y = e(x, k) \qquad x = d(y, k)$$

$k, x, y \in \{ 0, 1, \ldots, 25 \}$

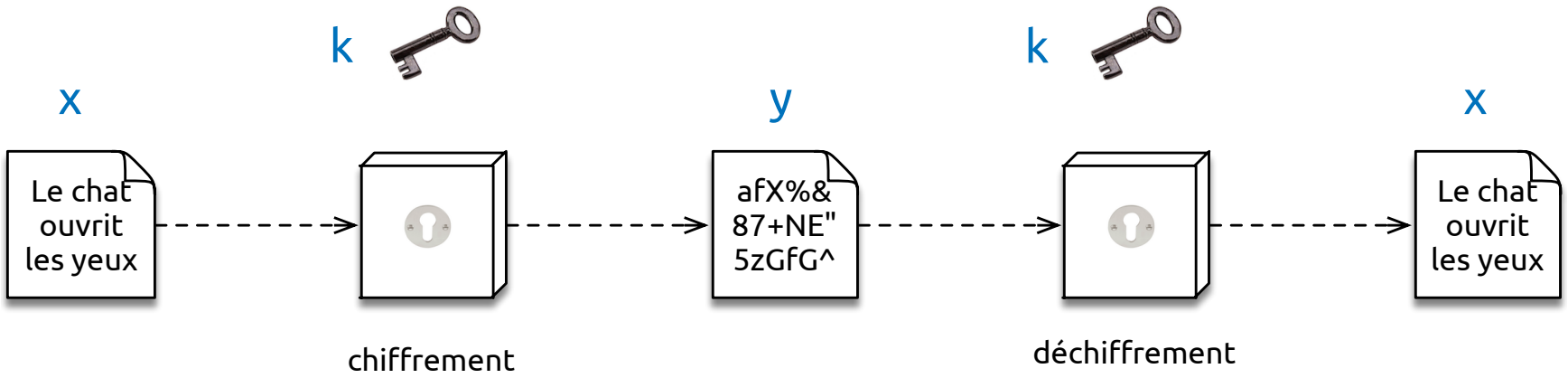
Chiffrement : $y = e(x, k) = (x + k) \bmod 26$

Déchiffrement : $x = d(y, k) = (y - k) \bmod 26$

Chiffrement symétrique (1)

- Technique universelle pour obtenir confidentialité
  - Utile pour données stockées ou communiquées
- Aussi connu comme
  - Chiffrement conventionnel
  - Chiffrement à clé unique (*single-key*)
- Deux prérequis :
  - Un algorithme fort de chiffrement
  - Emetteur et récepteur doivent se mettre d'accord sur la clé
    - Communication sûre préalable
    - Stockage sûr

Chiffrement symétrique (2)



$$y = e(x, k) \qquad x = d(y, k)$$

$$y = e_k(x) \qquad x = d_k(y)$$

- Exemples
  - Le disque de César
  - DES - Data Encryption Standard
  - AES - Advanced Encryption Standard

Attaques au chiffrement symétrique

- Cryptanalyse
  - Doit compter sur
    - La nature de l'algorithme
    - Quelques connaissances sur les caractéristiques générales du texte en clair
    - Quelques exemples de paires texte-crypté
  - Exploite les caractéristiques de l'algorithme pour tenter de déduire un texte en clair spécifique ou la clé utilisée
  - En cas de succès: tous les messages passés et futurs chiffrés avec cette clé sont compromis
- Force brute
  - Essayer toutes les clés possibles sur un texte chiffré jusqu'à ce qu'une traduction intelligible en texte clair soit obtenue
  - Pour réussir, il faut en moyenne la moitié de toutes les clés possibles

Les algorithmes amplement utilisés

- DES - ancien principal standard (années 70)
  - Taille de clé est trop courte pour une sécurité adéquate (56 bits effectifs, cassé en 1997 avec brute force)
- 3DES - astuce pour réutiliser DES
  - Trois instances DES en cascade, des clés distinctes
  - Censé être encore sécurisé, mais lent
- AES - successeur de DES en tant que standard
  - Accepte les clés grandes (128…256 bits)
  - Efficace tant sur le plan logiciel que matériel
  - En gros, il n'y a pas mieux que ça
- Blowfish - option similaire à AES
  - Clés grandes, blocs petits (inefficient)
- Twofish - successeur de Blowfish avec des blocs plus grands

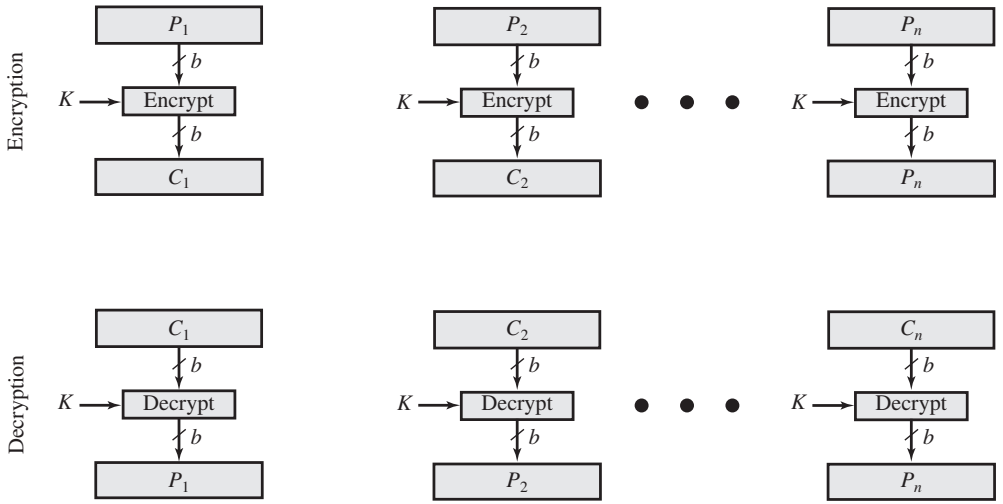
Déchiffrement par force brute

- DES
  - Brute force possible avec un grand nombre de machines (data center)
- AES
  - Loin d'être le cas

Key Size (bits)	Cipher	Number of Alternative Keys	Time Required at 10^9 decryptions/μs	Time Required at 10^{13} decryptions/μs
56	DES	$2^{56} \approx 7.2 \times 10^{16}$	$2^{55}\ \mu s = 1.125$ years	1 hour
128	AES	$2^{128} \approx 3.4 \times 10^{38}$	$2^{127}\ \mu s = 5.3 \times 10^{21}$ years	5.3×10^{17} years
168	Triple DES	$2^{168} \approx 3.7 \times 10^{50}$	$2^{167}\ \mu s = 5.8 \times 10^{33}$ years	5.8×10^{29} years
192	AES	$2^{192} \approx 6.3 \times 10^{57}$	$2^{191}\ \mu s = 9.8 \times 10^{40}$ years	9.8×10^{36} years
256	AES	$2^{256} \approx 1.2 \times 10^{77}$	$2^{255}\ \mu s = 1.8 \times 10^{60}$ years	1.8×10^{56} years

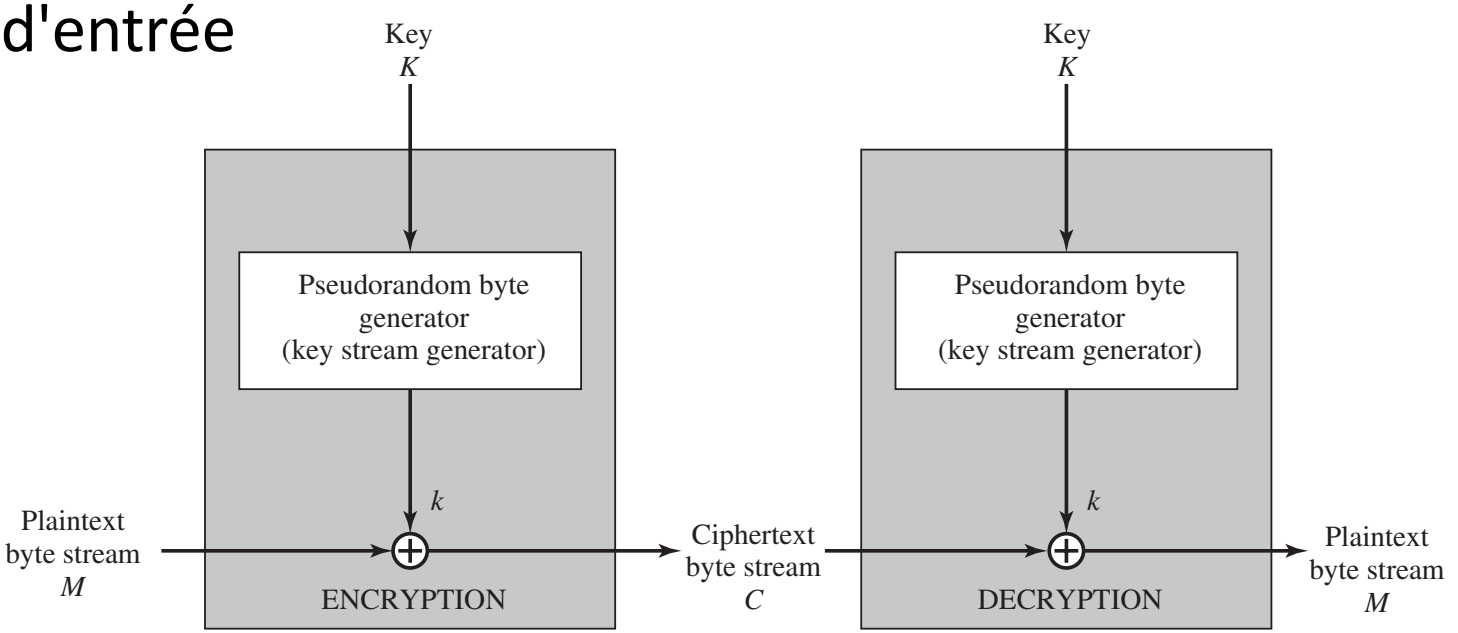
Chiffrement par bloc

- Traite un bloc d’octets à la fois
- Produit un bloc de sortie pour chaque bloc d'entrée
- Peut réutiliser des clés
- Utilisation plus fréquente



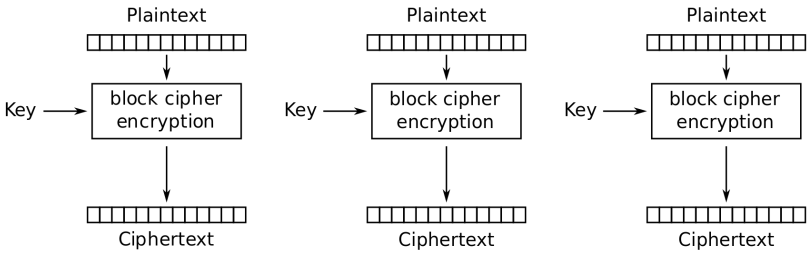
Chiffrement en flot de données

- Traite les octets de l'entrée en continu
- Produit en sortie un octet à la fois
- En général plus rapides, moins de code
- Le flux pseudo-aléatoire est imprévisible sans connaissance de la clé d'entrée

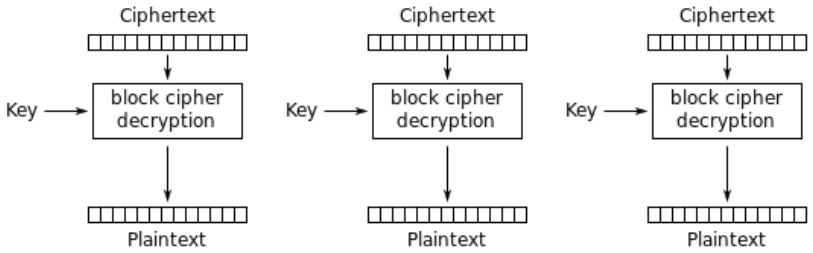


Modes d'opération

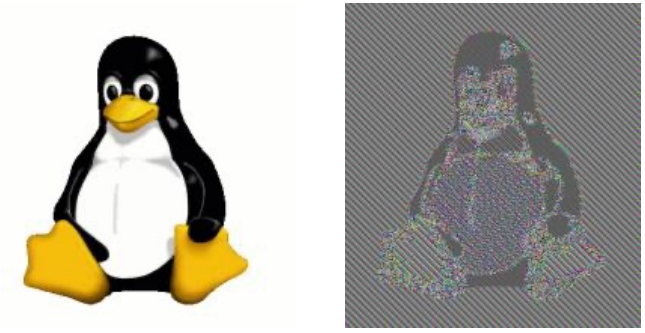
- Chiffrement seul: un texte en clair donne toujours le même texte chiffré



Electronic Codebook (ECB) mode encryption



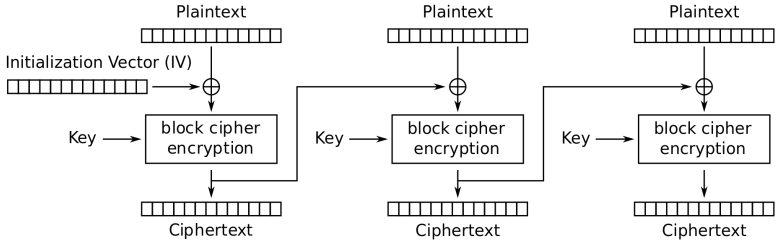
Electronic Codebook (ECB) mode decryption



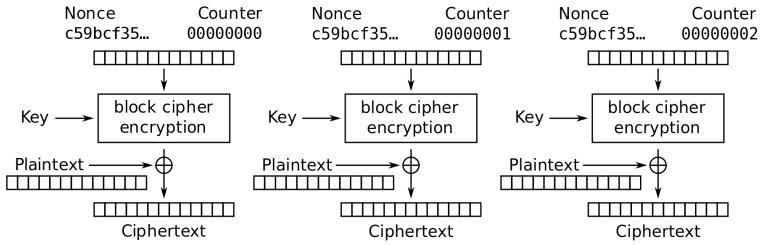
Le résultat n'est pas aléatoire

Modes d'opération

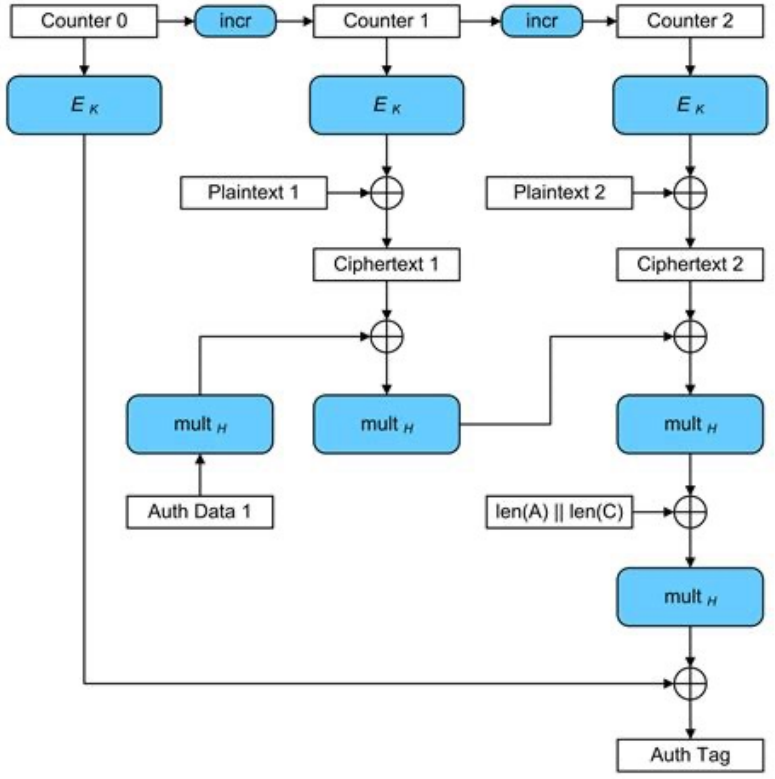
- ECB, CBC, OFB, CFB, CTR, **GCM**, CCM, EAX, OCB, …



Cipher Block Chaining (CBC) mode encryption



Counter (CTR) mode encryption



Figures: Wikipedia

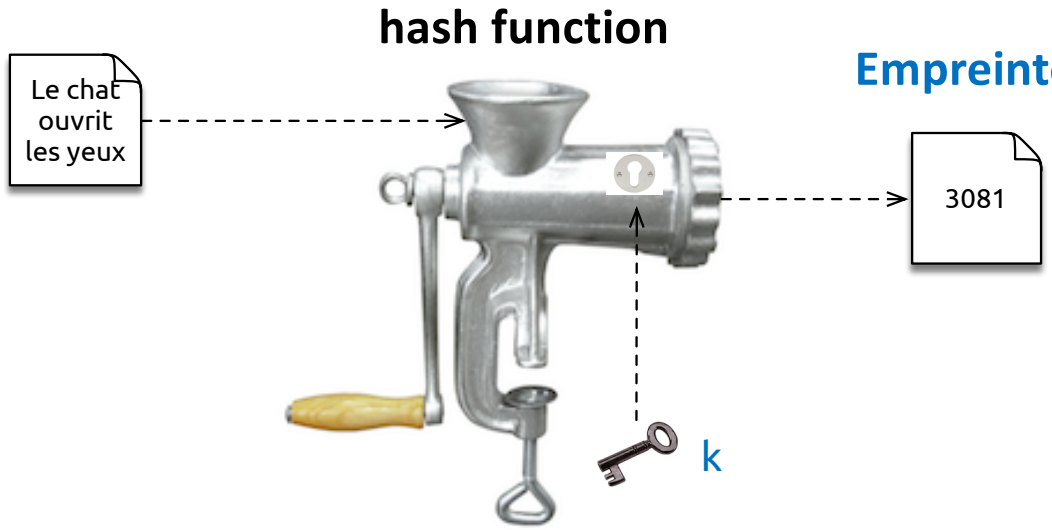

15
min

Authentification de messages

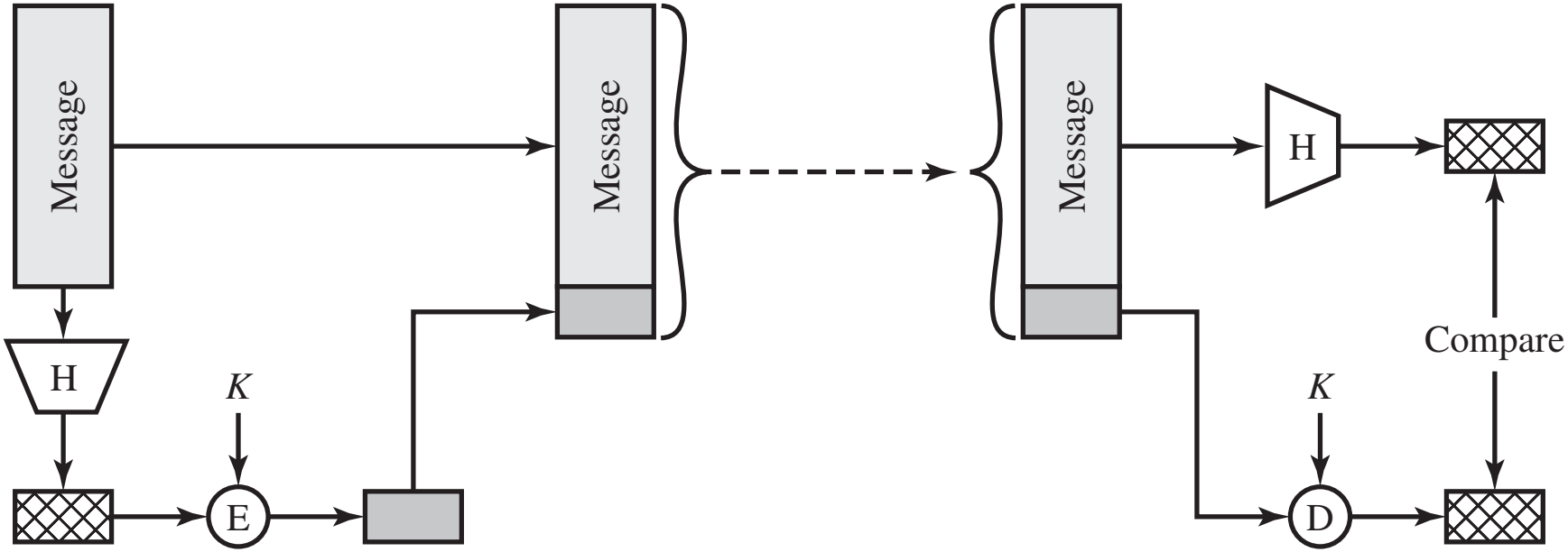
- Protection contre des attaques actives
- Permet de vérifier que
  - Un message reçu est authentique
  - Son contenu n'a pas été modifié
  - La source est authentique
  - Message arrive en temps opportun et dans le bon ordre
- Avec le chiffrement conventionnel
  - L'expéditeur et le destinataire partagent une clé

Code d'authentification de messages *Message Authentification Code (MAC)*

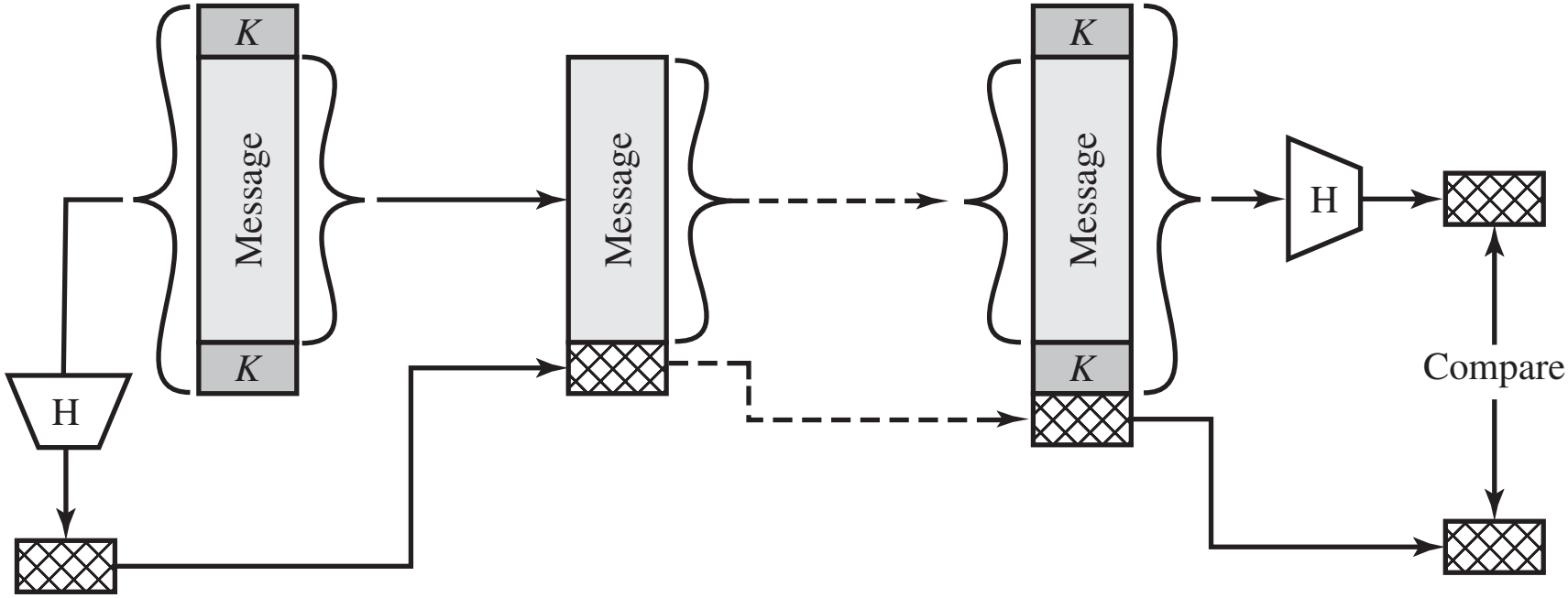
- Fonction d'hachage
  - Calcul à partir d'une donnée d'entrée de taille quelconque
  - **Empreinte** : résultat de taille fixe (petite comparé à la moyenne des données d'entrée)
  - Impossible de reconstruire la donnée à partir du résultat
  - Si deux donnés donnent le même résultat : collision
- MAC: une clé symétrique change le résultat



Authentification avec chiffrement



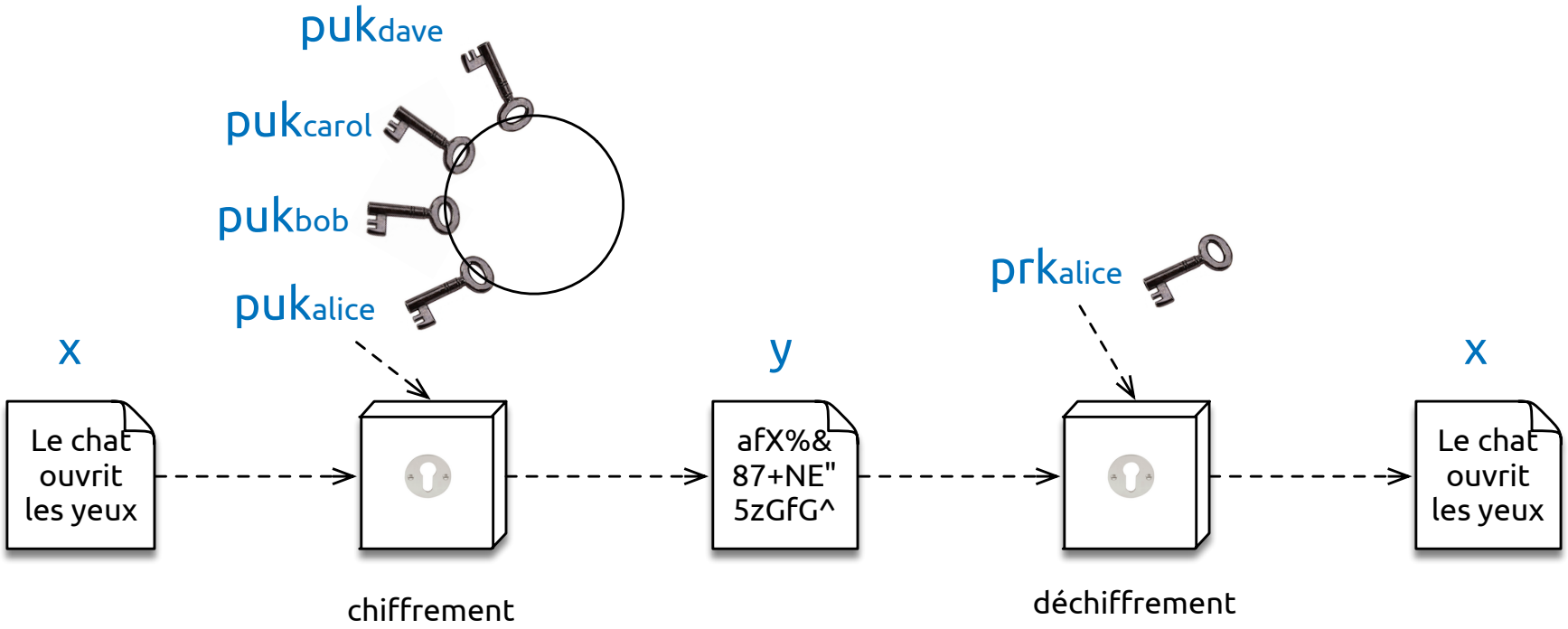
Authentification avec une valeur secrète



Qualité d'une fonction d'hachage

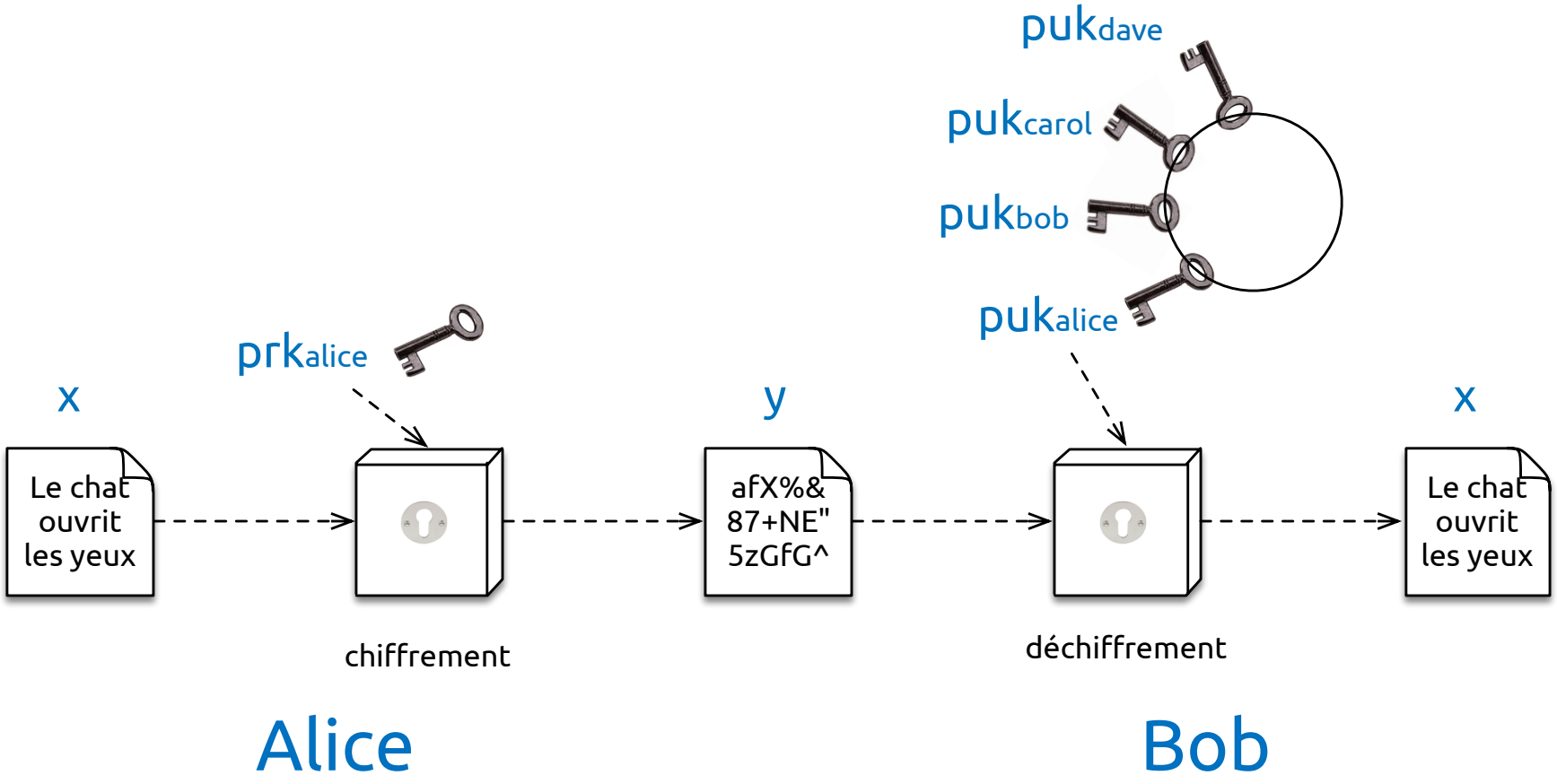
- Opération unidirectionnel
  - Impossible trouver ***x*** tel que ***H(x) = h***
- Résistance aux collisions
  - Impossible trouver ***y ≠ x*** tel que ***H(y) = H(x)***
- Attaques
  - Cryptanalyse : chercher une faiblesse de l'algo
  - Force brute : dépend de la taille du code hash
- Algorithmes
  - MD5 – 128 bits, plus simple, plus rapide, peu sûr
  - SHA-1 – 160 bits, peu sûr
  - SHA-2 – 224, 256, 384, 512 bits, standard actuel

Chiffrement asymétrique

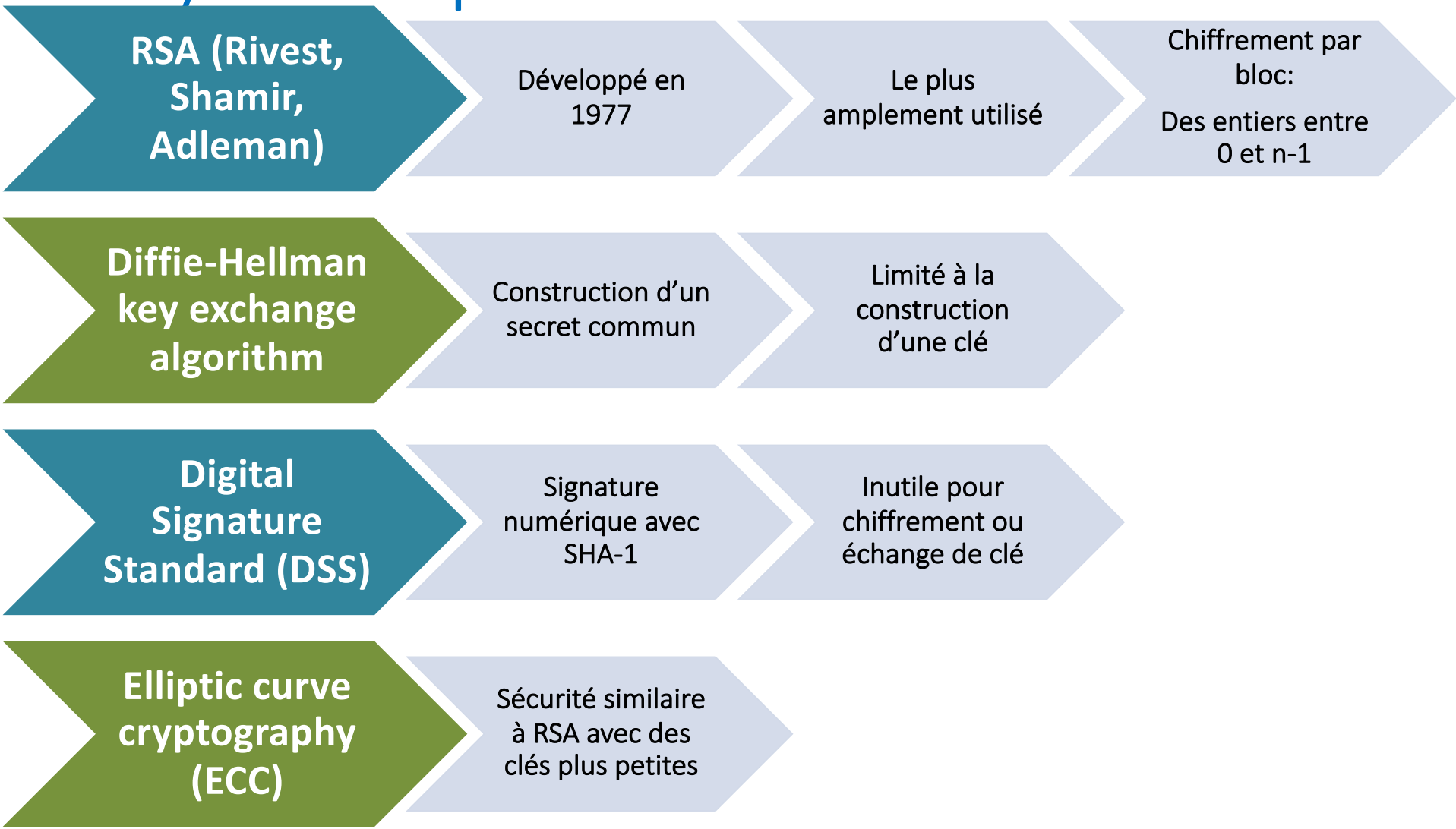


- Chiffrement avec une clé publique (*public-key encryption*)
- Chaque participant a deux clés ***puk*** et ***prk***

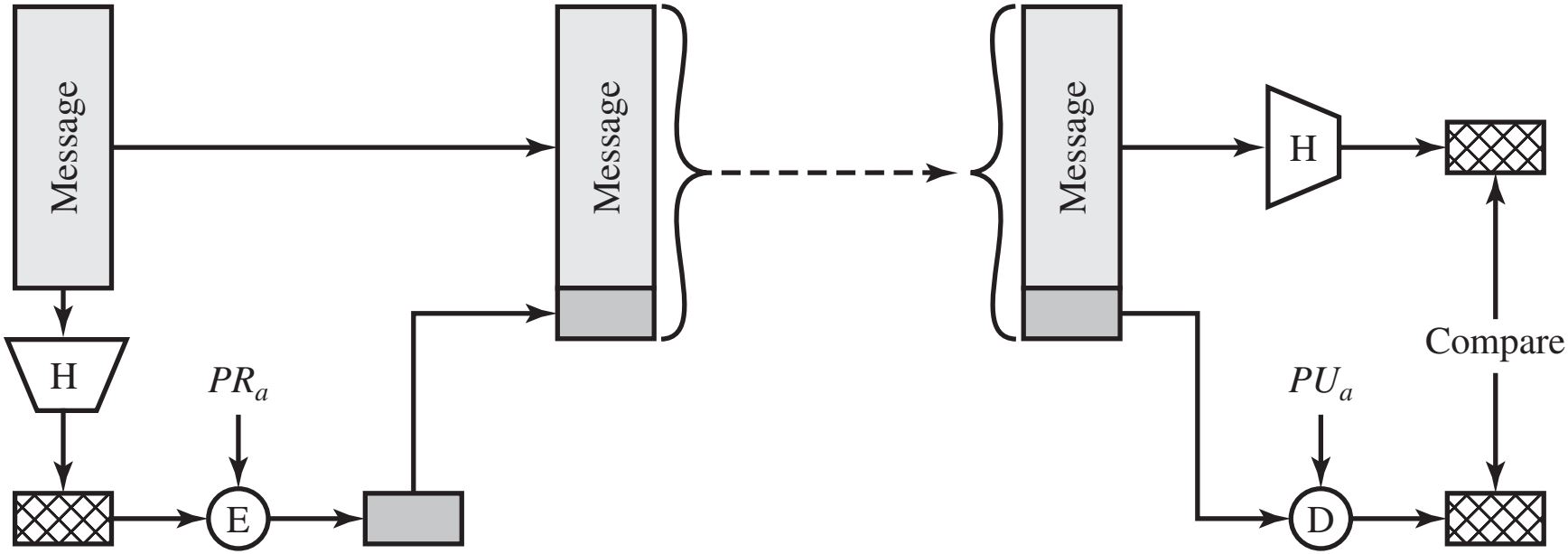
Chiffrement asymétrique (sens inversé)



Algorithmes de chiffrement asymétriques



Signatures numériques



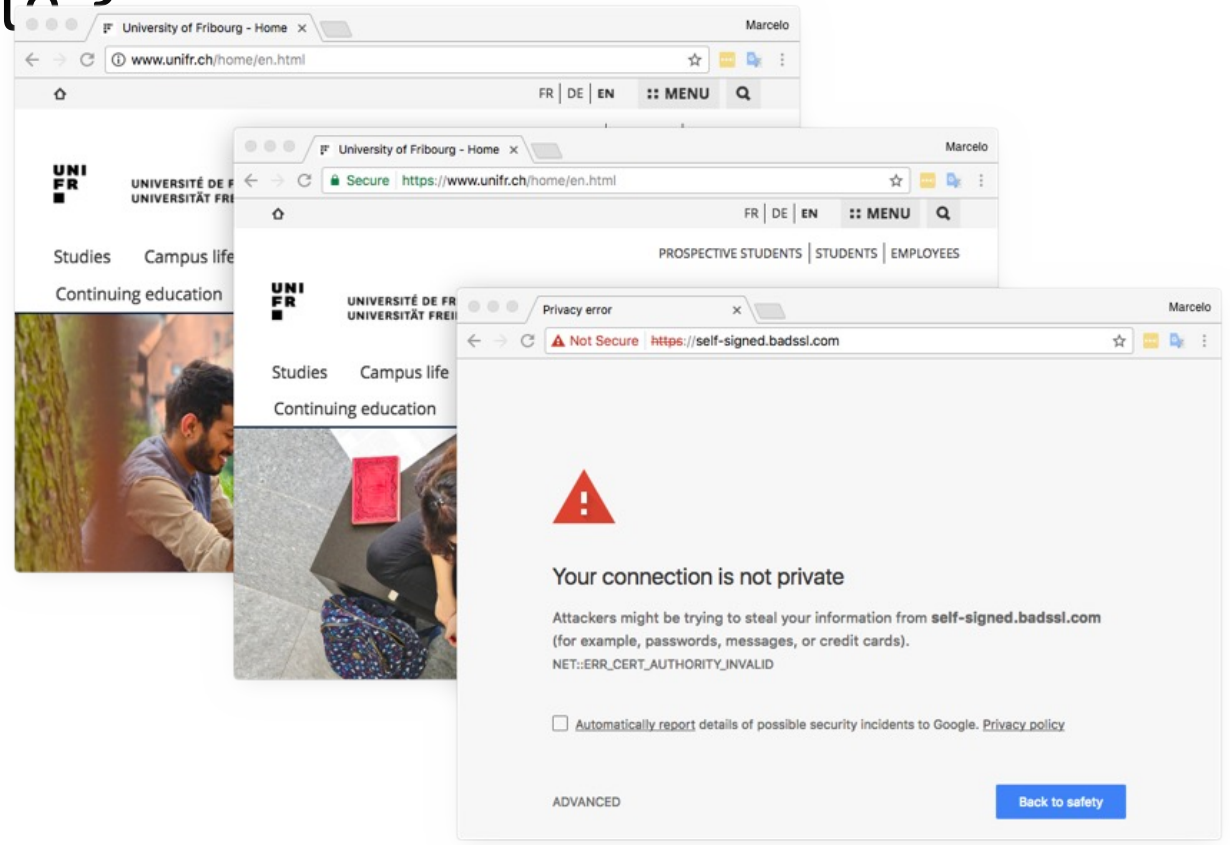
Avantages des signatures numériques

- Seul celui qui a la clé privé aurait pu chiffrer l'empreinte
- Garanties:
  - Authentification
  - Non répudiation

- Inconvénient
  - Assurer l'authenticité des clés publiques
  - Gérer un grand nombre de clés

Besoin de certification

Comment assurer l'identité du serveur auquel on se connecte ?



Certification de l'identité dans le monde physique

- Données sur le doc d'identité
  - Numéro
  - Autorité
  - Validité
  - Identité
  - Description
  - Signature
  - Signature de l'autorité

Certificat numérique

- Un certificat relie une clé à une personne ou à un service
  - Comparable à un passeport
  - Emis par une autorité fiable (exemple: l'état)
- Contient
  - Des informations sur la personne à qui il appartient
  - Informations sur qui l'a émis
  - Une période de validité

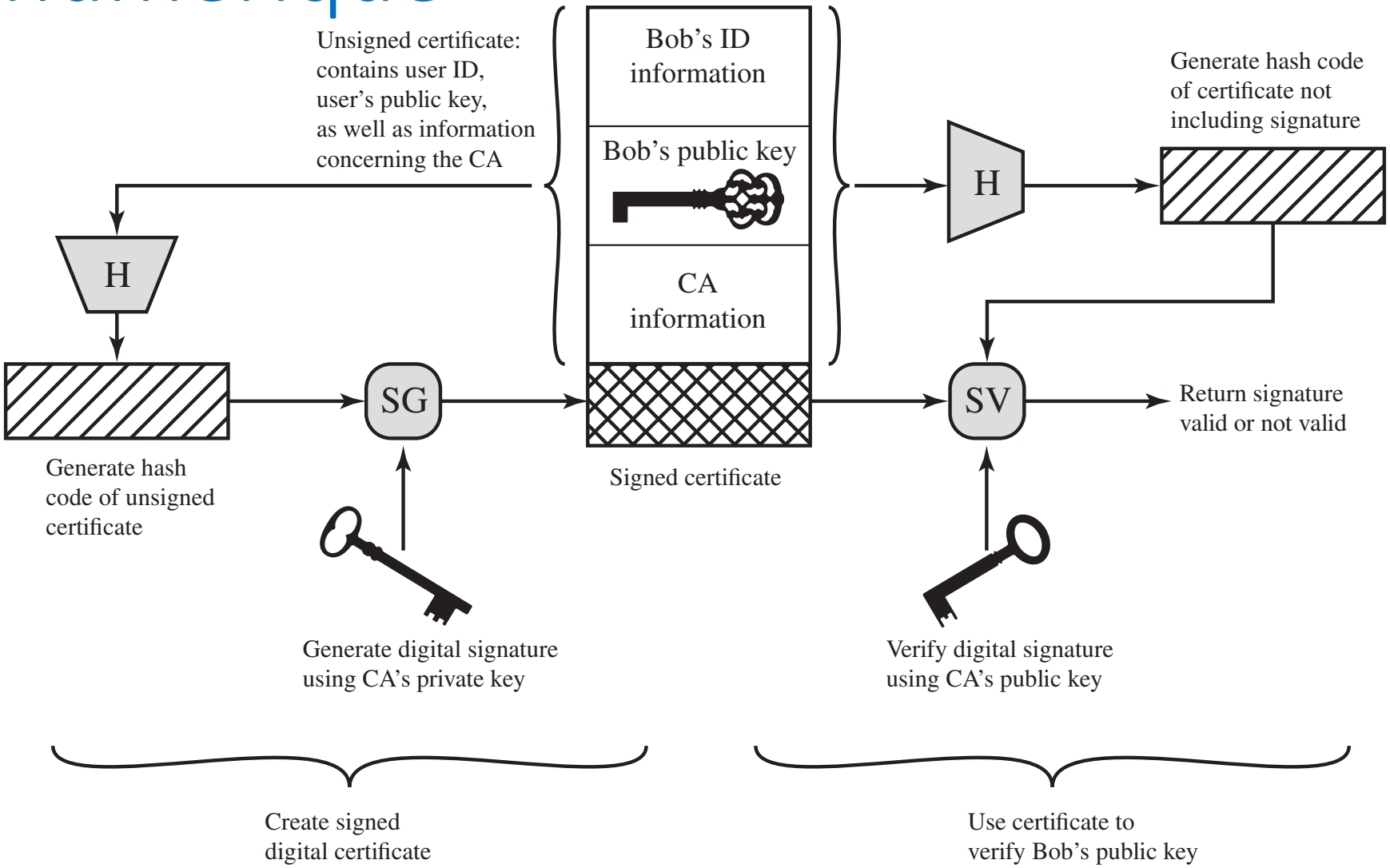
- Le certificat est signé avec la clé de l'émetteur
- Il contient la clé publique du sujet

- Le certificat est géré par un service payant
  - **Certificate Authority**

Exemple de certificat numérique

```
Certificate:
  Data:
    Version: 3 (0x2)
    Serial Number:
       bb:7c:54:9b:75:7b:28:9d
    Signature Algorithm: sha1WithRSAEncryption
    Issuer: C=MY, ST=STATE, O=CA COMPANY NAME, L=CITY, OU=X.509, CN=CA ROOT
    Validity
       Not Before: Apr 15 22:21:10 2008 GMT
       Not After : Mar 10 22:21:10 2011 GMT
    Subject: C=MY, ST=STATE, L=CITY, O=ONE INC, OU=IT, CN=www.example.com
    Subject Public Key Info:
       Public Key Algorithm: rsaEncryption
       RSA Public Key: (1024 bit)
       Modulus (1024 bit):
         00:ae:19:86:44:3c:dd:38:df:e2:41:5f:d8:86:19:69:7e:85:d7:1d:ae:1e:eb:87:b0:5f:fc:f3:db:e3:aa:82:76:d6:42:05:f1:0e:5c:5a:a2:8d:f6:d3:00:37:04:
         96:13:06:16:e6:d1:67:14:69:cd:85:df:a7:b3:ac:a2:6c:33:cd:d6:00:3d:24:99:fa:4b:81:07:0c:b2:5a:fe:06:16:da:34:66:63:78:31:7d:11:5e:63:de:9e:ee:
         76:8b:0c:12:af:fb:f2:28:0a:76:5b:99:20:b8:f7:c0:9c:e8:89:c5:d0:1e:e5:07:c8:bd:38:c8:52:97:cc:76:c9:c8:2b
       Exponent: 65537 (0x10001)
  X509v3 extensions:
    X509v3 Basic Constraints:
       CA:FALSE
  Netscape Comment:
       OpenSSL Generated Certificate
  X509v3 Subject Key Identifier:
       EE:D9:4A:74:03:AC:FB:2C:FD:43:C7:58:6E:2E:6A:88:BA:65:61:CC
  X509v3 Authority Key Identifier:
       keyid:54:0D:DE:E3:37:23:FF:2E:E8:03:0A:2C:52:FE:FC:C0:C8:13:72:80
Signature Algorithm: sha1WithRSAEncryption
   52:3d:bc:bd:3f:50:92:67:a3:d3:6f:37:a9:3f:89:b5:16:5b:9c:0d:32:25:32:91:c7:bf:f6:0d:f8:6d:1c:09:45:2f:3f:b9:18:b7:1c:8d:7c:06:33:ef:ca:e0:92:a3:
   90:3f:7c:4e:16:87:67:ae:7c:2c:1a:43:e5:3a:24:d9:c3:7d:cf:bf:eb:01:9d:c1:f0:bb:0f:15:de:d5:9e:42:9d:f8:7f:0d:5b:af:59:80:d1:aa:cc:db:31:1b:d4:7f:
   f3:f1:71:25:85:c9:8b:78:3e:13:ac:11:51:35:49:8d:c3:9a:bb:9a:89:2c:ef:7f:90:f9:05:b3:65:98:b8:74
```

Utilisation d'un certificat numérique



Communication avec plusieurs interlocuteurs

- Avantage du chiffrement asymétrique:
  - Moyen pour N émetteurs envoyer a 1 destination
    - Chiffrer avec la clé publique
  - Communication N x N: utiliser N clés publiques

- Les broadcasts posent problème
  - Le chiffrement asymétrique est lent
    - Envoyer un message à N destinations: encore plus lent
    - Il faut chiffrer le message N fois
  - Idéalement: chiffrer une seule fois
  - Solution: enveloppes numériques (ex: TV par câble)

Enveloppes numériques