

Introduction à la sécurité (services, mécanismes, algorithmes)

Master2, UPMC - Télécom ParisTech,

UE INF944

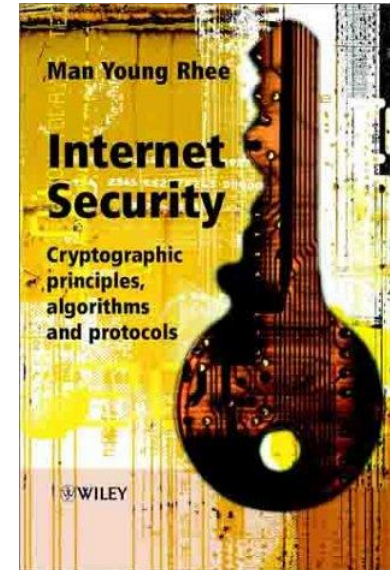
Responsable : Rida Khatoun

Maître de conférences, Télécom-ParisTech

rida.khatoun@telecom-paristech.fr

Objectifs du cours : rappels

1. Objectifs de la sécurité
2. Architecture de sécurité
3. Algorithmes cryptographiques
 - Chiffrement faible
 - Chiffrement symétrique
 - DES
 - AES
 - Chiffrement asymétrique
 - RSA
 - El -Gamal
4. Fonctions de hachage
5. Stéganographie



Internet Security :
Cryptographic Principles, Algorithms and Protocols
Auteur : Man Young Rhee, 2003

Pourquoi étudier la sécurité ?

- *« The art of war teaches us to rely not on the likelihood of the enemy's not coming, but on our own readiness to receive him; not on the chance of his not attacking, but rather on the fact that we have made our position unassailable »*

The art of war – Sun Tzu*
(6th century BC)

- *« L'art de la guerre nous apprend à ne pas nous fier au calme de l'ennemi, mais à notre promptitude à le recevoir et à nos positions inattaquables »*

L'art de la guerre – Sun Tzu
(VI siècle av. J.-C.)

* « Stratégie militaire de maître Sun », pour le général chinois Sun Tzu, fin du VI^e siècle av. J.- C

Pourquoi étudier la sécurité ?

- Développement rapide des technologies de l'information
 - Dépendance croissante des organismes envers leurs SI
 - SI est utilisé dans des applications variées
- => Moyens de communication doivent être sûrs et fiables...

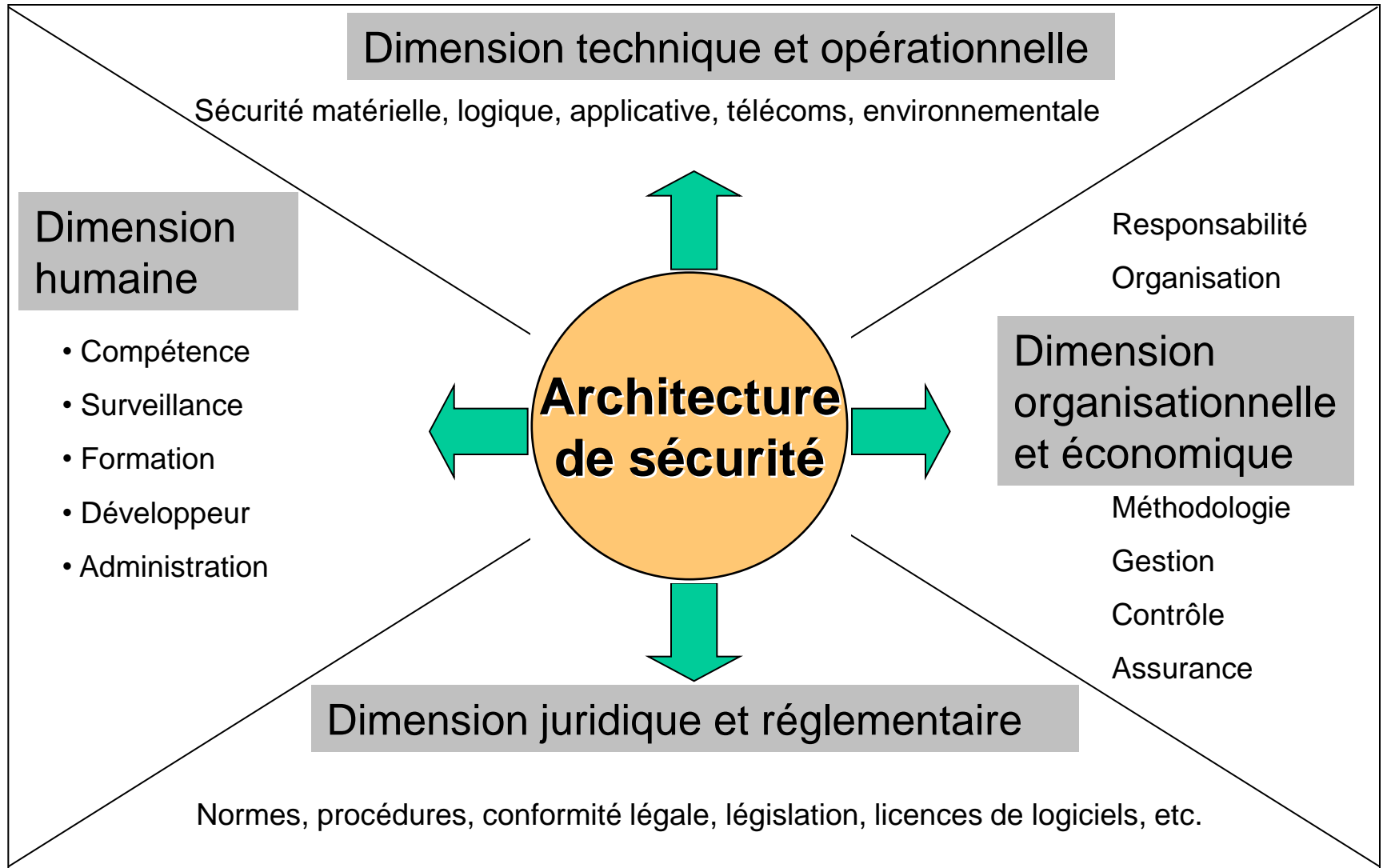
- Définition :

« Structure conceptuelle fixant les dimensions organisationnelles, économiques, techniques, légales et humaines dans lesquelles les solutions de sécurité doivent s'inscrire »

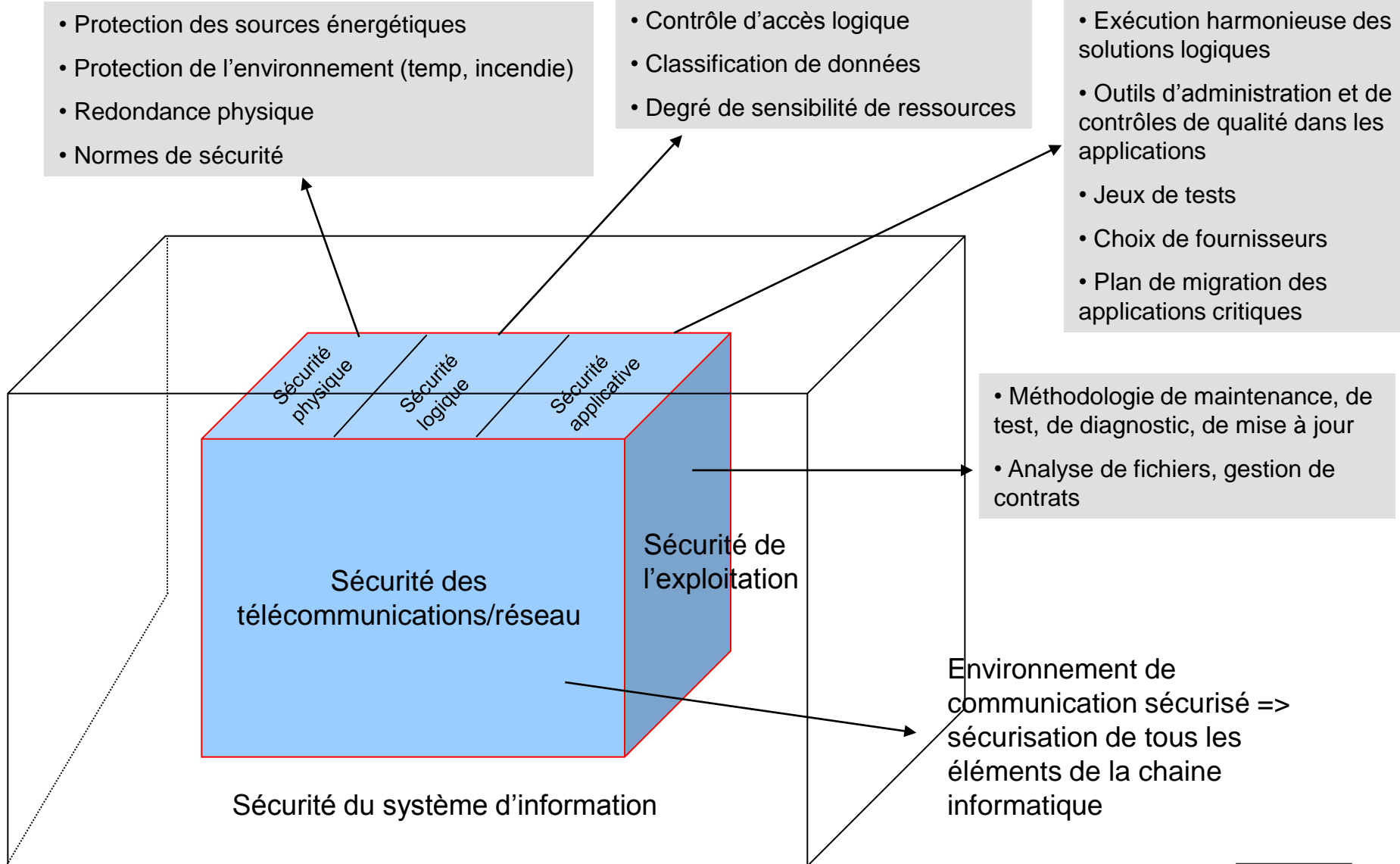
- Objectif

- Identifier les éléments qui la composent : outils, mesures, réglementations
- Traiter les problèmes de manière systématique
- Renforcer la cohérence et la complémentarité des solutions

Architecture de sécurité

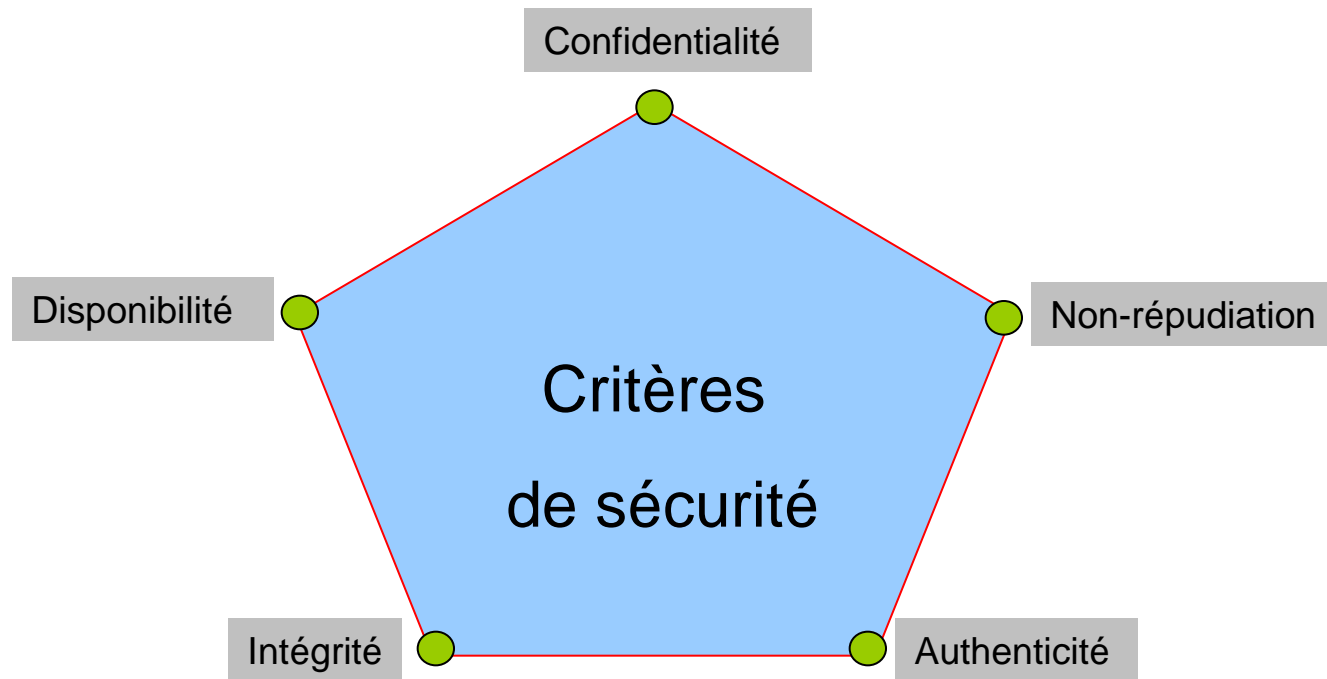


Architecture de sécurité



Critères fondamentaux de sécurité

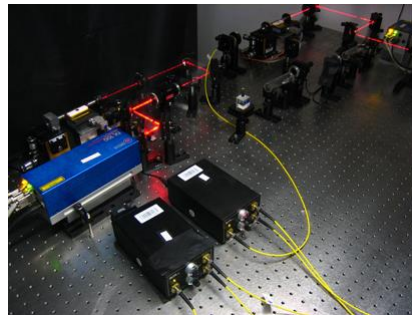
- Les solutions de la sécurité doivent contribuer à satisfaire les critères suivants



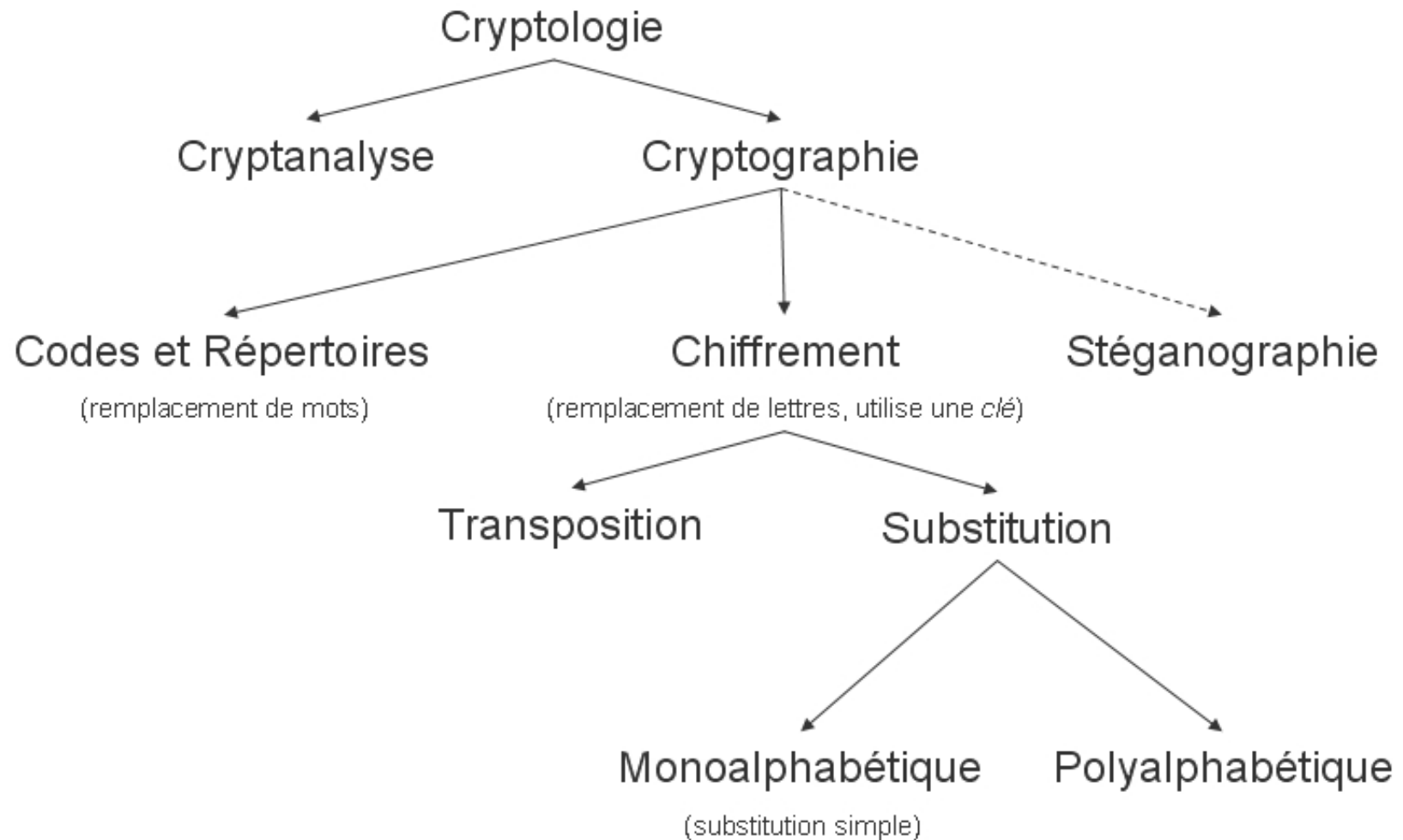
Critères fondamentaux de sécurité

- La confidentialité
 - est le maintien du secret des informations
 - elle assurée par la cryptographie
- L'Intégrité
 - permet de certifier que les données n'ont pas été modifiées ou altérées
 - avec les techniques actuelles, cette fonction est réalisée par la signature numérique (HMAC, MD5, SHA-1, HAVAL)
- L'authentification
 - permet de vérifier l'identité annoncée et de s'assurer de la non-usurpation de l'identité d'une entité
 - elle est assurée par les mécanismes de contrôle d'accès (mots de passe, biométrie, kerberos)
- La non-répudiation
 - est le fait de ne pas pouvoir nier ou rejeter qu'un événement a eu lieu
 - elle est assurée par la traçabilité et les journaux d'audit fichiers *log*
- La disponibilité d'une ressource est la probabilité de pouvoir mener correctement à terme un service, une requête ou une session de travail

- C'est quoi la cryptographie ?
 - Science qui consiste à écrire l'information en la rendant inintelligible à ceux ne possédant pas les capacités de la déchiffrer
 - Information : voix, textes, données, images
 - Bases
 - Mathématiques
 - Physiques !!



Vocabulaire



Histoire de la cryptographie

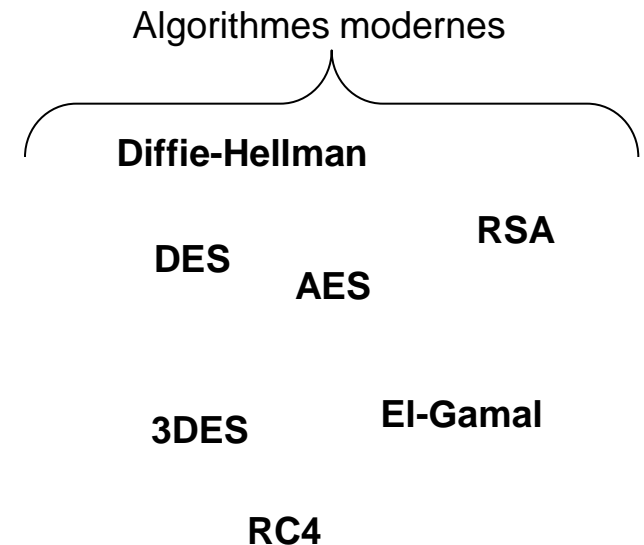
- Débuts de la cryptographie
- Mécanisation de la cryptographie
- Cryptographie contemporaine



Blaise de Vigenère



Une machine ENIGMA



- Algorithmes de chiffrement faibles
 - Chiffrement de *César*
 - Jules César : général et écrivain romain 100 av. J.-C
 - Cryptographie la plus ancienne et la plus simple
 - Chiffrement de *Vigenère*
 - Blaise de Vigenère (1523-1596), français
 - Notion de clef
 - Autres

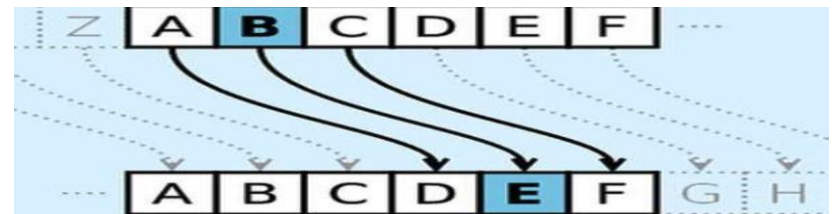
Les débuts de la cryptographie

- **Chiffrement de César**

- Substitution très simple pour transmettre des messages militaires
- Cryptographie la plus ancienne et la plus simple

- **Principe :**

- Chiffrement basé sur la substitution mono-alphabétique de lettres
- Chaque lettre est remplacée ("substitution") par une seule autre ("mono-alphabétique"), selon un certain décalage dans l'alphabet
- EX : décalage de 3 lettres



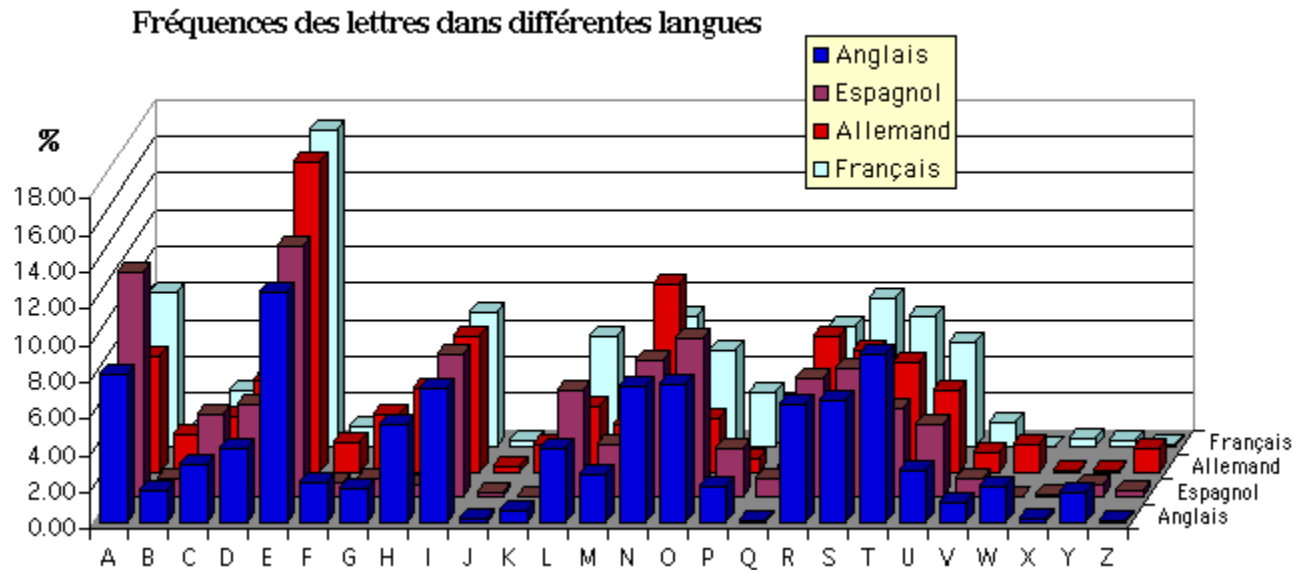
Les débuts de la cryptographie

- Chiffrement de César

- Lettre numérotée de 0 à 25 (A = 0, B = 1, etc.)
- Coder l'expression « J'adore les maths ! »
 - 'J' a le numéro : 9
 - Décalage de 4
 - $9 + 4 = 13$, ce qui correspond à N, donc 'J' devient 'N'
 - Même chose pour les autres lettres
 - Phrase initiale « **J'adore les maths** »
 - Phrase chiffrée « **N'EHSVI PIW QEXLW** »
- Si la valeur > 26
 - modulo, c'est le reste de la division
 - Exemple: $5 \bmod 3 = 2$, $10 \bmod 3 = 1$

Les débuts de la cryptographie

- Limites du chiffrement de César
 - Vulnérable à l'analyse des fréquences
 - Attaques 26 lettres dans l'alphabet => 26 décalages possibles



SOURCE : www.apprendre-en-ligne.net/crypto/stat/

Les débuts de la cryptographie

BQPSNRSJXJNJXLDPCLDLPQBE_QRKJXHKKPSJ
PJIKSPUNBDKIQRBKPQPBQPZITEJQDQBTSEKPEL
NIUNPHNKPBKPKCKSSQWKPSLXJPSNVVXSQCCK
DJPBLDWPXBPSNVVXJPGKPJKDXIPZLCEJKPGK
SPSJQJXSJXHNKSPGPLZZNIIKDZKPGKSPGXVVK
IKDJKSPBKJJIKS

Comment peut-on décoder ce texte ?

Les débuts de la cryptographie

- Chiffrement de *Vigenère*
 - Amélioration du chiffrement de César en utilisant la notion de clefs
 - Substitution polyalphabétique
 - Exemple
 - Texte : université
 - Clef : master
 - Cipher : «GNAOIIIEILX»
 - $C = (M + K) \text{ modulo } 26$
 - La même lettre sera chiffrée de différentes manières
- Cassé par le test de *Kasiski*

Les débuts de la cryptographie

- Example

- Texte : université
- Clef : master
- CIPHER : «GNAOIIILX»
- $C = (M + K) \text{ modulo } 26$

G N A O I I E I L X

		Lettre 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
C l é u t i l i s é e	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

Les débuts de la cryptographie

- Chiffrement de Vigenère : Test de Kasiski
 - Cryptogramme

XAUNMEESYIEDTLLFGSNBWQUFXPQTYORUTYIIN**UMQI**EULSMFAFXGUTYBXXAGBHMIFIIM**UMQI**DEKRIFRIRZQUHIENOO**OI**
GRMLYETYOVQRYSEXEOKIYPY**OIGR**FBWPIYRBQURJIYEM**JIGRY**KXYACPPQSPBVESIRZQRUFREDY**JIGRY**KXBLOPJARNPU
GEFBWMILXMZSMZYXPNBPUMYZMEEFBUGENLRDEPBXONQEZTMBWOFIIPAHPPQBFLGDEMFWFAHQ

- Test pour trouver la taille de la clef
 - **UMQI** se retrouve après 30 caractères
 - **OIGR** se retrouve après 25 caractères
 - **JIGRY** se retrouve après 30 caractères
- La longueur de la clé doit être un diviseur de 30 et de 25 : il est possible qu'il s'agisse de 5

Séquence	Distance	Diviseurs de la distance					
UMQI	30	2	3	5	6	10	15
OIGR	25	-	-	5	-	-	-
JIGRY	30	2	3	5	6	10	15

Mécanisation de la cryptographie

- Début de la mécanisation de la cryptographie
 - Entre les deux guerres mondiales
 - Mécaniser la cryptographie
 - Outils mécaniques
 - Cylindres chiffants
 - Machines électromécaniques
- Substitutions polyalphabétiques
 - Rotors et des contacts électriques
 - Clé de longueur gigantesque
- Machine Enigma
 - Machine à chiffrer et déchiffrer utilisée par l'armée allemande (1930 - 1944)
 - Automatise le chiffrement par substitution



Mécanisation de la cryptographie

- Quelques systèmes électro-mécaniques
 - Purple (Japon)
 - Nema (Suisse)
 - Sigaba (USA)
 - Typex (Angleterre)
 - Lacida (Pologne)
 - Hagelin M-209 (USA)

Nema



<http://www.cryptomuseum.com>



Fialka



Transvertex

La cryptographie contemporaine

- Auguste Kerckhoffs*

- «La cryptographie militaire», article publié dans le Journal des sciences militaires, en 1883
 - Référence de cryptographie
 - Ensemble de règles pour assurer la confidentialité
- Toute méthode de chiffrement est connue de l'ennemi
- La sécurité du système ne dépend que du choix des clefs qui doivent être simples et modifiables



Kerckhoffs

- Clef

- Il s'agit du paramètre impliqué et autorisant des opérations de chiffrement et/ou déchiffrement

** : cryptologue militaire néerlandais (1835 - 1903)



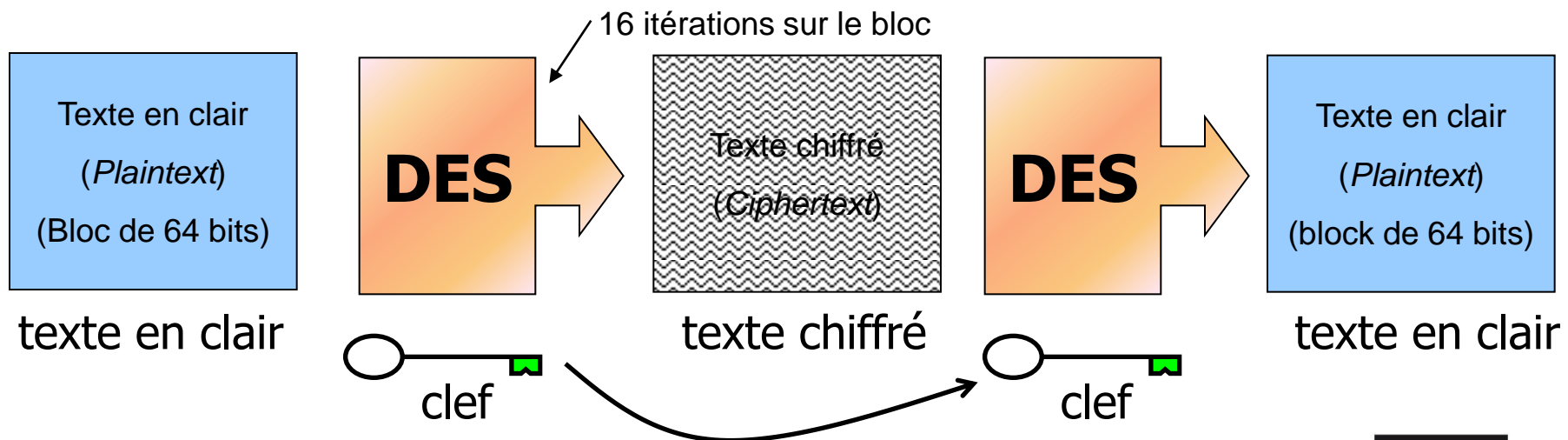
Chiffrement symétrique

- **Cryptosystème à clé symétrique**
 - Clés identiques : $K_E = K_D = K$,
 - Clé doit rester secrète
 - Algorithmes répandus DES, AES, 3DES, ...
 - Clé choisie aléatoirement dans l'espace des clés
 - Algorithmes basés sur des opérations de transposition et de substitution des bits du texte clair en fonction de la clé
 - Taille des clés : variable
 - DES, 56 bits
 - AES peut aller jusqu'à 256
 - Avantage principal : rapidité
 - Désavantage : Distribution des clés

Chiffrement à clef symétrique : DES

- Data Encryption Standard (DES)
 - Adopté par le NIST* en 1977
 - Chiffrement par bloc de 64 bits (CBC)
 - Clef de 56 bits
 - Largement répandu pour des applications financières

**National Institute of Standards and Technology* : agence du Département du Commerce aux États-Unis



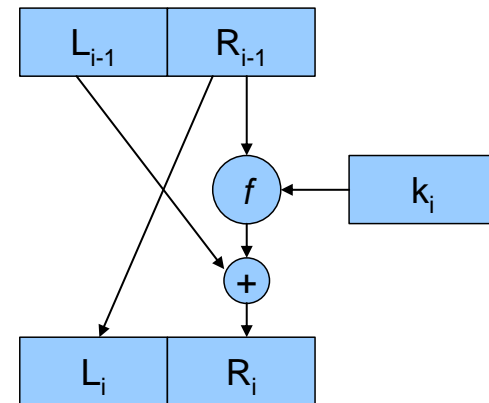
Chiffrement à clef symétrique : DES

- DES se déroule en trois étapes

x est un bloc de 64 bits

- Permutation initiale (IP) appliquée à x pour obtenir une chaîne $IP(x) = L_0R_0$
- On effectue 16 tours de chiffrement (rondes)

$$\begin{cases} L_i = R_{i-1} \\ R_i = L_{i-1} (+) f(R_{i-1}, K_i) \end{cases}$$



- On effectue une permutation inverse IP^{-1} à $R_{16}L_{16}$

Chiffrement à clef symétrique : DES

- Diversification de la clef dans DES :
 - K de 64 bits est réordonné dans PC-1 qui supprime les bits de parités (en 8, 16,...,64)
 - LS_i : rotation circulaire vers la gauche d'une ou deux positions selon la valeur de i
 - PC2 : autre permutation de bits

Table 3.1 Permuted choice 1 (PC-1)

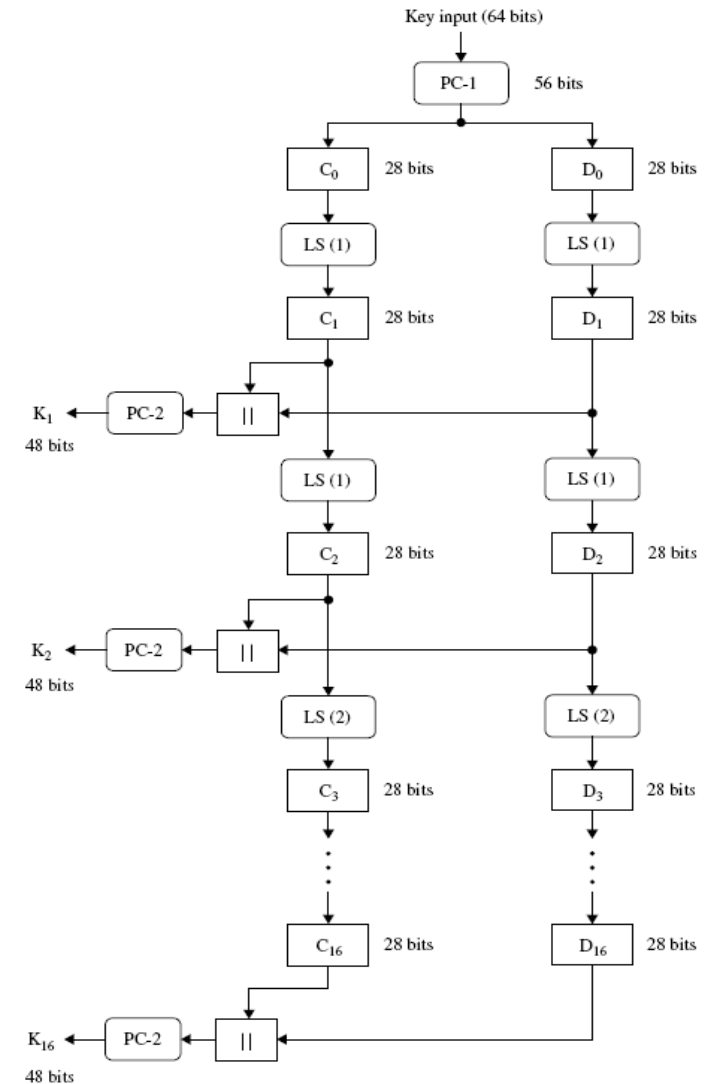
57	49	41	33	25	17	9	1	58	50	42	34	26	18
10	2	59	51	43	35	27	19	11	3	60	52	44	36
63	55	47	39	31	23	15	7	62	54	46	38	30	22
14	6	61	53	45	37	29	21	13	5	28	20	12	4

Table 3.2 Schedule for key shifts

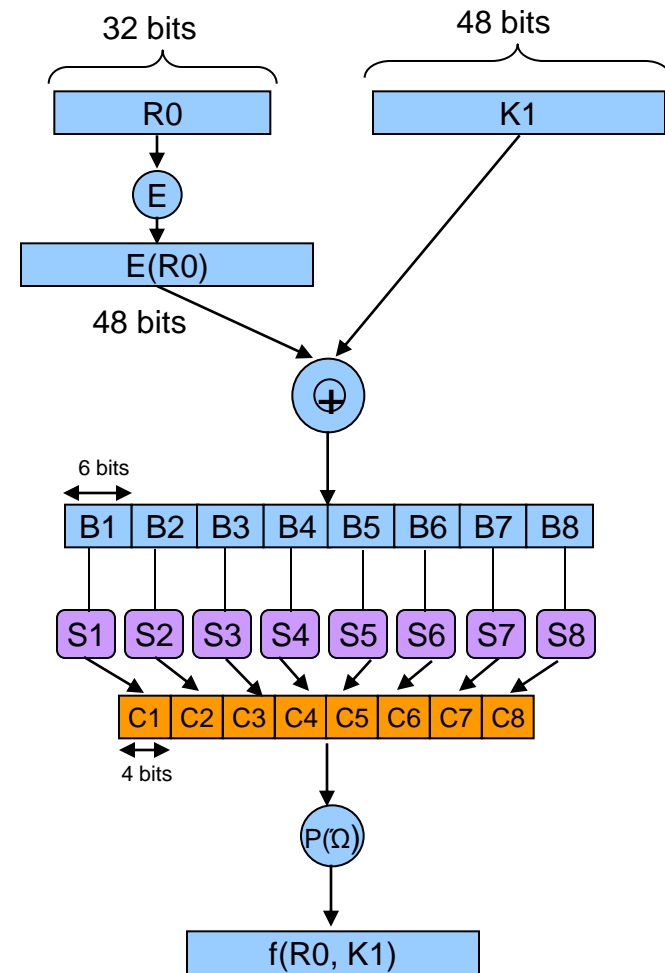
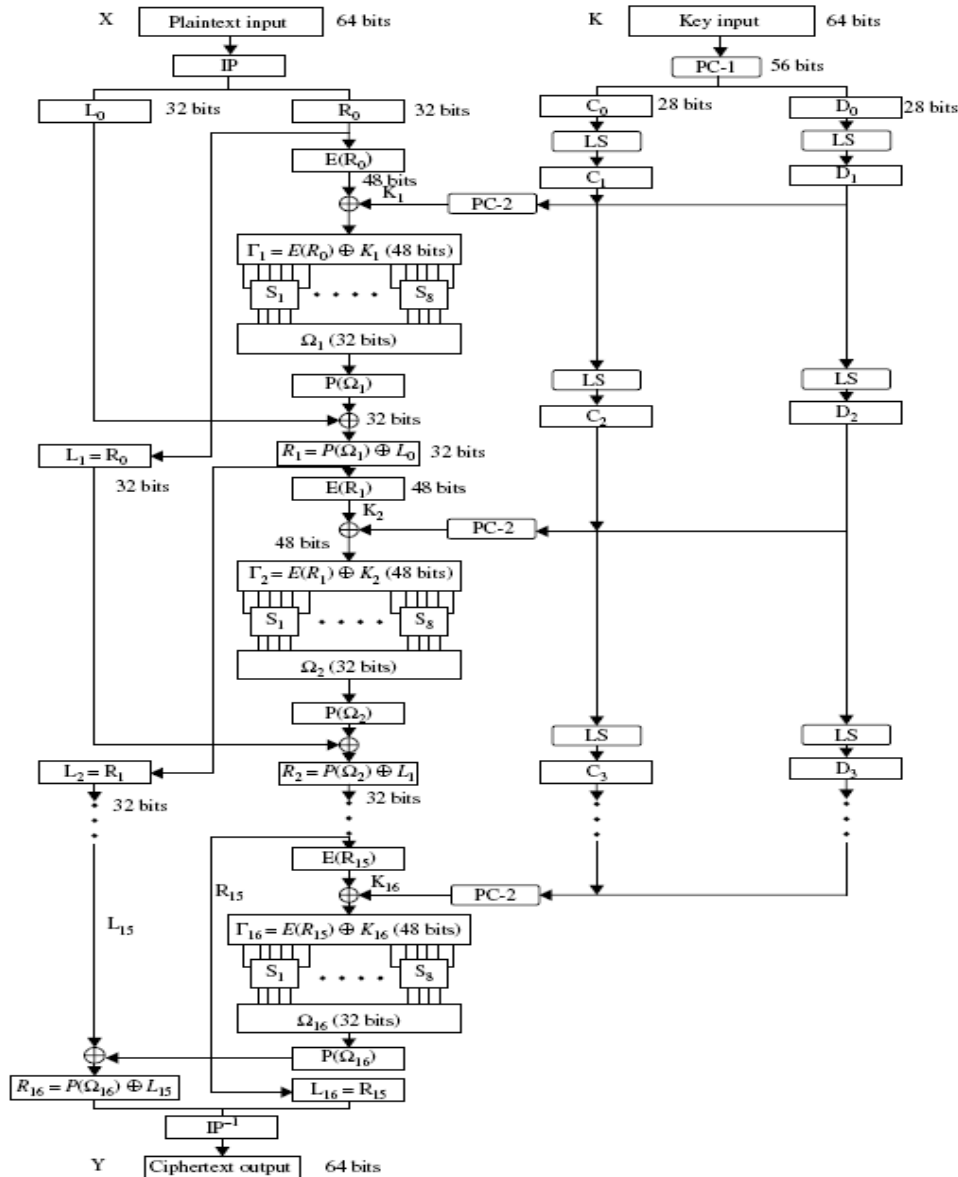
Round number	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16
Number of left shifts	1	1	2	2	2	2	2	2	1	2	2	2	2	2	2	1

Table 3.3 Permuted choice 2 (PC-2)

14	17	11	24	1	5	3	28	15	6	21	10
23	19	12	4	26	8	16	7	27	20	13	2
41	52	31	37	47	55	30	40	51	45	33	48
44	49	39	56	34	53	46	42	50	36	29	32



Chiffrement à clef symétrique : DES



Chiffrement à clef symétrique : DES

Inverse of initial permutation, IP^{-1}

40	8	48	16	56	24	64	32
39	7	47	15	55	23	63	31
38	6	46	14	54	22	62	30
37	5	45	13	53	21	61	29
36	4	44	12	52	20	60	28
35	3	43	11	51	19	59	27
34	2	42	10	50	18	58	26
33	1	41	9	49	17	57	25

Initial permutation (IP)

L_i	58	50	42	34	26	18	10	2
	60	52	44	36	28	20	12	4
	62	54	46	38	30	22	14	6
	64	56	48	40	32	24	16	8
R_i	57	49	41	33	25	17	9	1
	59	51	43	35	27	19	11	3
	61	53	45	37	29	21	13	5
	63	55	47	39	31	23	15	7

Permutation function P

16	7	20	21
29	12	28	17
1	15	23	26
5	18	31	10
2	8	24	14
32	27	3	9
19	13	30	6
22	11	4	25

E bit-selection table

32	1	2	3	4	5
4	5	6	7	8	9
8	9	10	11	12	13
12	13	14	15	16	17
16	17	18	19	20	21
20	21	22	23	24	25
24	25	26	27	28	29
28	29	30	31	32	1

Chiffrement à clef symétrique : DES

- Boîte de substitution S_i
- Ex: si $B5 = 101110$
alors, $S_5^{10}(0111)$
 $\Rightarrow C5 = 8 \text{ hex} = (1000)_b$

		S-boxes															
		0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15
S_1	0	14	4	13	1	2	15	11	8	3	10	6	12	5	9	0	7
	1	0	15	7	4	14	2	13	1	10	6	12	11	9	5	3	8
	2	4	1	14	8	13	6	2	11	15	12	9	7	3	10	5	0
	3	15	12	8	2	4	9	1	7	5	11	3	14	10	0	6	13
S_2	0	15	1	8	14	6	11	3	4	9	7	2	13	12	0	5	10
	1	3	13	4	7	15	2	8	14	12	0	1	10	6	9	11	5
	2	0	14	7	11	10	4	13	1	5	8	12	6	9	3	2	15
	3	13	8	10	1	3	15	4	2	11	6	7	12	0	5	14	9
S_3	0	10	0	9	14	6	3	15	5	1	13	12	7	11	4	2	8
	1	13	7	0	9	3	4	6	10	2	8	5	14	12	11	15	1
	2	13	6	4	9	8	15	3	0	11	1	2	12	5	10	14	7
	3	1	10	13	0	6	9	8	7	4	15	14	3	11	5	2	12
S_4	0	7	13	14	3	0	6	9	10	1	2	8	5	11	12	4	15
	1	13	8	11	5	6	15	0	3	4	7	2	12	1	10	14	9
	2	10	6	9	0	12	11	7	13	15	1	3	14	5	2	8	4
	3	3	15	0	6	10	1	13	8	9	4	5	11	12	7	2	14
S_5	0	2	12	4	1	7	10	11	6	8	5	3	15	13	0	14	9
	1	14	11	2	12	4	7	13	1	5	0	15	10	3	9	8	6
	2	4	2	1	11	10	13	7	8	15	9	12	5	6	3	0	14
	3	11	8	12	7	1	14	2	13	6	15	0	9	10	4	5	3
S_6	0	12	1	10	15	9	2	6	8	0	13	3	4	14	7	5	11
	1	10	15	4	2	7	12	9	5	6	1	13	14	0	11	3	8
	2	9	14	15	5	2	8	12	3	7	0	4	10	1	13	11	6
	3	4	3	2	12	9	5	15	10	11	14	1	7	6	0	8	13
S_7	0	4	11	2	14	15	0	8	13	3	12	9	7	5	10	6	1
	1	13	0	11	7	4	9	1	10	14	3	5	12	2	15	8	6
	2	1	4	11	13	12	3	7	14	10	15	6	8	0	5	9	2
	3	6	11	13	8	1	4	10	7	9	5	0	15	14	2	3	12
S_8	0	13	2	8	4	6	15	11	1	10	9	3	14	5	0	12	7
	1	1	15	13	8	10	3	7	4	12	5	6	11	0	14	9	2
	2	7	11	4	1	9	12	14	2	0	6	10	13	15	3	5	8
	3	2	1	14	7	4	10	8	13	15	12	9	0	3	5	6	11

Chiffrement à clef symétrique : DES

- **Avantages et applications de DES**
 - Facile à comprendre et implémenter
 - Sécurité indépendante de l'algorithme lui-même
 - Rapide
 - Clé relativement petite
 - Résultat statistiquement « plat » après 16 tours : espaces et fréquences indétectables
 - Légère modification du texte provoque changements importants dans le *ciphertext*
- **Applications actuelles**
 - Chiffrer les paiements par carte de crédits (*UEPS*)
 - Protocoles d'authentification comme *Kerberos*

Chiffrement à clef symétrique : AES

- AES (Advanced Encryption Standard)
 - Histoire
 - Inventé par Joan Daemen et Vincent Rijmen
 - Adopté par NIST* en 2000
 - Successeur de DES
 - Standard de chiffrement pour les organisations du gouvernement des Etats-Unis
 - Chiffrement : symétrique (CBC)
 - Bloc : 128 bits organisés sous forme matricielle
 - Clefs : taille 128, 192, 256 bits

* National Institute of Standards and Technology

Chiffrement à clef symétrique : AES

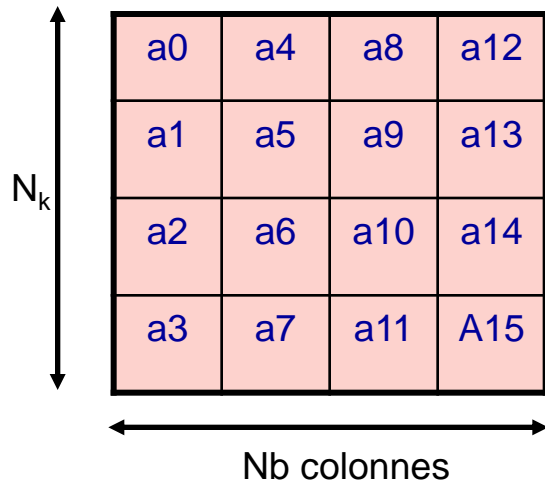
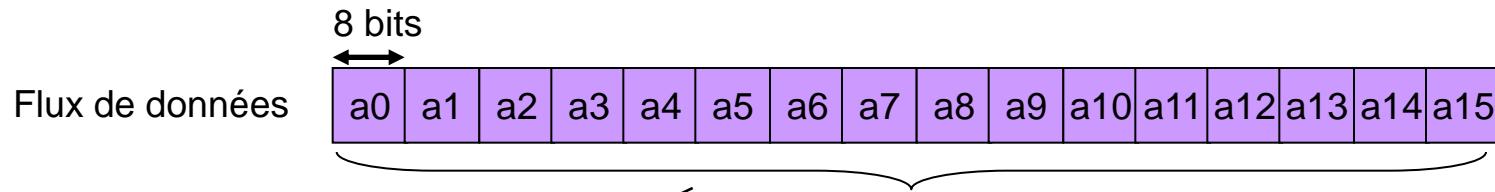
- Propriétés d'AES

- Plusieurs longueurs de clef et de bloc sont possibles : 128, 192, ou 256 bits
- Nombre de cycles ("rondes") varie en fonction de la longueur des blocs et des clés (de 10 à 14)
- Structure générale ne comprend qu'une série de transformations/permutations/sélections
- Beaucoup plus performant que le DES
- Parallélisme peut être implémenté

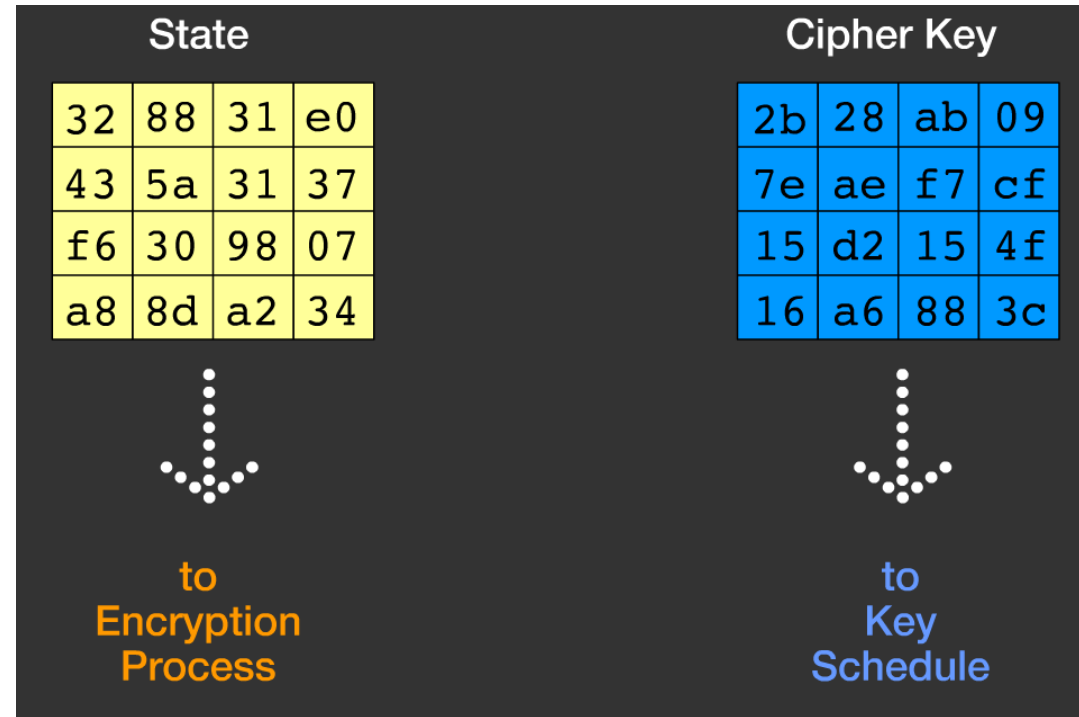
Chiffrement à clef symétrique : AES

- Principe de l'algorithme :
 - Chiffrement AES consiste en
 - Une addition initiale de clef (*AddRoundKey*)
 - $N_r - 1$ tours (rondes) chacun divisé en 4 étapes
 - Quatre étapes d'une ronde (tours)
 - *SubBytes* : substitution non-linéaire où chaque octet est remplacé par un autre choisi d'une table SBox
 - *ShiftRows* : transposition où chaque élément de la matrice est décalé cycliquement à gauche d'un certain nombre de colonnes
 - *MixColumns* : effectue un produit matriciel
 - *AddRoundKey* : addition de chaque octet avec l'octet correspondant dans une clé de tour obtenue par diversification

Chiffrement à clef symétrique : AES



Représentation matricielle d'un bloc de 16 octets



hexadecimal notation:

Ex: 32 = 00110010 (1 byte)
3hex 2hex

Chiffrement à clef symétrique : AES

Flux de données

Ex : $32 \text{ xor } 2b = 19$ en hex

19	a0	9a	e9
3d	f4	c6	f8
e3	e2	8d	48
be	2b	2a	08

32	88	31	e0
43	5a	31	37
f6	30	98	07
a8	8d	a2	34

AddRoundKey

Cipher Key			
2b	28	ab	09
7e	ae	f7	cf
15	d2	15	4f
16	a6	88	3c

initial
round

1-SubBytes

2-ShiftRows

3-MixColumns

4-AddRoundKey

Round key 0

9
rounds

SubBytes

ShiftRows

AddRoundKey

Round key 10

final
round

Chiffrement à clef symétrique : AES

- SubBytes (State)

19	a0	9a	e9
3d	f4	c6	f8
e3	e2	8d	48
be	2b	2a	08

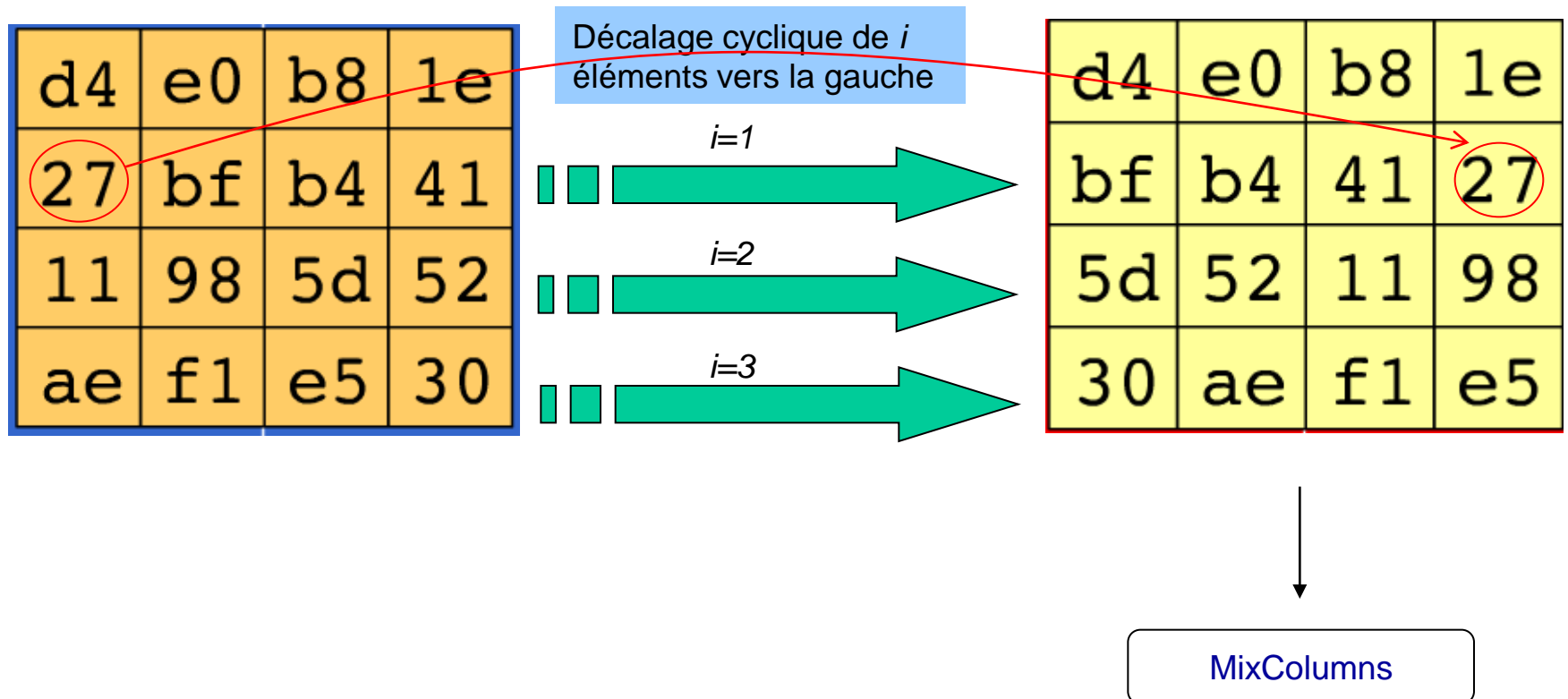
d4	e0	b8	1e
27	bf	b4	41
11	98	5d	52
ae	f1	e5	30

		y															
		0	1	2	3	4	5	6	7	8	9	a	b	c	d	e	f
x	0	63	7c	77	7b	f2	6b	6f	c5	30	01	67	2b	fe	d7	ab	76
	1	ca	82	e9	7d	fa	59	47	f0	ad	d4	a2	af	9c	a4	72	c0
	2	b7	fd	93	26	36	3f	f7	cc	34	a5	e5	f1	71	d8	31	15
	3	04	c7	23	c3	18	96	05	9a	07	12	80	e2	eb	27	b2	75
	4	09	83	2c	1a	1b	6e	5a	a0	52	3b	d6	b3	29	e3	2f	84
	5	53	d1	00	ed	20	fc	b1	5b	6a	cb	be	39	4a	4c	58	cf
	6	d0	ef	aa	fb	43	4d	33	85	45	f9	02	7f	50	3c	9f	a8
	7	51	a3	40	8f	92	9d	38	f5	bc	b6	da	21	10	ff	f3	d2
	8	cd	0c	13	ec	5f	97	44	17	c4	a7	7e	3d	64	5d	19	73
	9	60	81	4f	dc	22	2a	90	88	46	ee	b8	14	de	5e	0b	db
	a	e0	32	3a	0a	49	06	24	5c	c2	d3	ac	62	91	95	e4	79
	b	e7	c8	37	6d	8d	d5	4e	a9	6c	56	f4	ea	65	7a	ae	08
	c	ba	78	25	2e	1c	a6	b4	c6	e8	dd	74	1f	4b	db	8b	8a
	d	70	3e	b5	66	48	03	f6	0e	61	35	57	b9	86	c1	1d	9e
	e	e1	f8	98	11	69	d9	8e	94	9b	1e	87	e9	ce	55	28	df
	f	8c	a1	89	0d	bf	e6	42	68	41	99	2d	0f	b0	54	bb	16

AES SBox

Chiffrement à clef symétrique : AES

- ShiftRows (State)

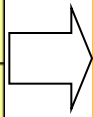


Chiffrement à clef symétrique : AES

- MixColumns (State)

multiplication de polynômes modulo un polynôme irréductible.

d4	e0	b8	1e
bf	b4	41	27
5d	52	11	98
30	ae	f1	e5



e0	b8	1e
b4	41	27
52	11	98
ae	f1	e5

02	03	01	01
01	02	03	01
01	01	02	03
03	01	01	02

*

d4
bf
5d
30

=

04
66
81
e5

MixColumns →

04	e0	48	28
66	cb	f8	06
81	19	d3	26
e5	9a	7a	4c

Chiffrement à clef symétrique : AES

- Arithmétique des polynômes binaires

- Un corps binaire \mathbb{F}_2 est l'ensemble $\{0; 1\}$ munit des lois d'addition et de multiplication suivante

- Addition

$$(x^5 + x^3 + x^2 + 1) + (x^7 + x^5 + x + 1) = x^7 + x^3 + x^2 + x$$

$$(00101101) \oplus (10100011) = (10001110)$$

$$(2d) \oplus (a3) = (8e)$$

- Multiplication

$$(01110011) \bullet (10100101)$$

$$(x^6 + x^5 + x^4 + x + 1) \bullet (x^7 + x^5 + x^2 + 1)$$

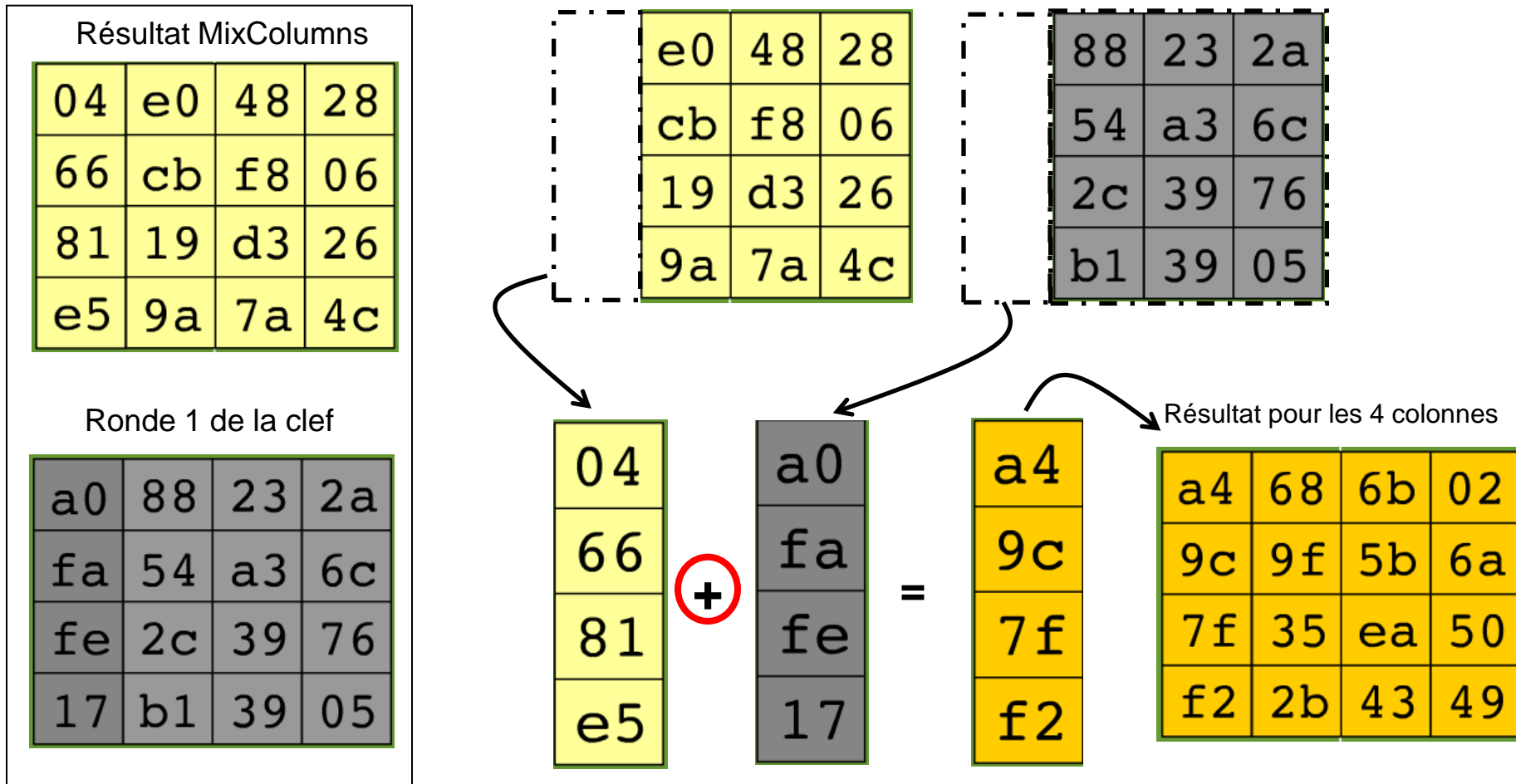
$$= x^{13} + x^{12} + x^{10} + x^9 + x^6 + x^4 + x^3 + x^2 + x + 1$$

- Un polynôme binaire $A(X)$ est une somme formelle en une indéterminée X avec des coefficients dans \mathbb{F}_2

$$A(X) = a_0 + a_1X + a_2X^2 + \dots + a_nX^n$$

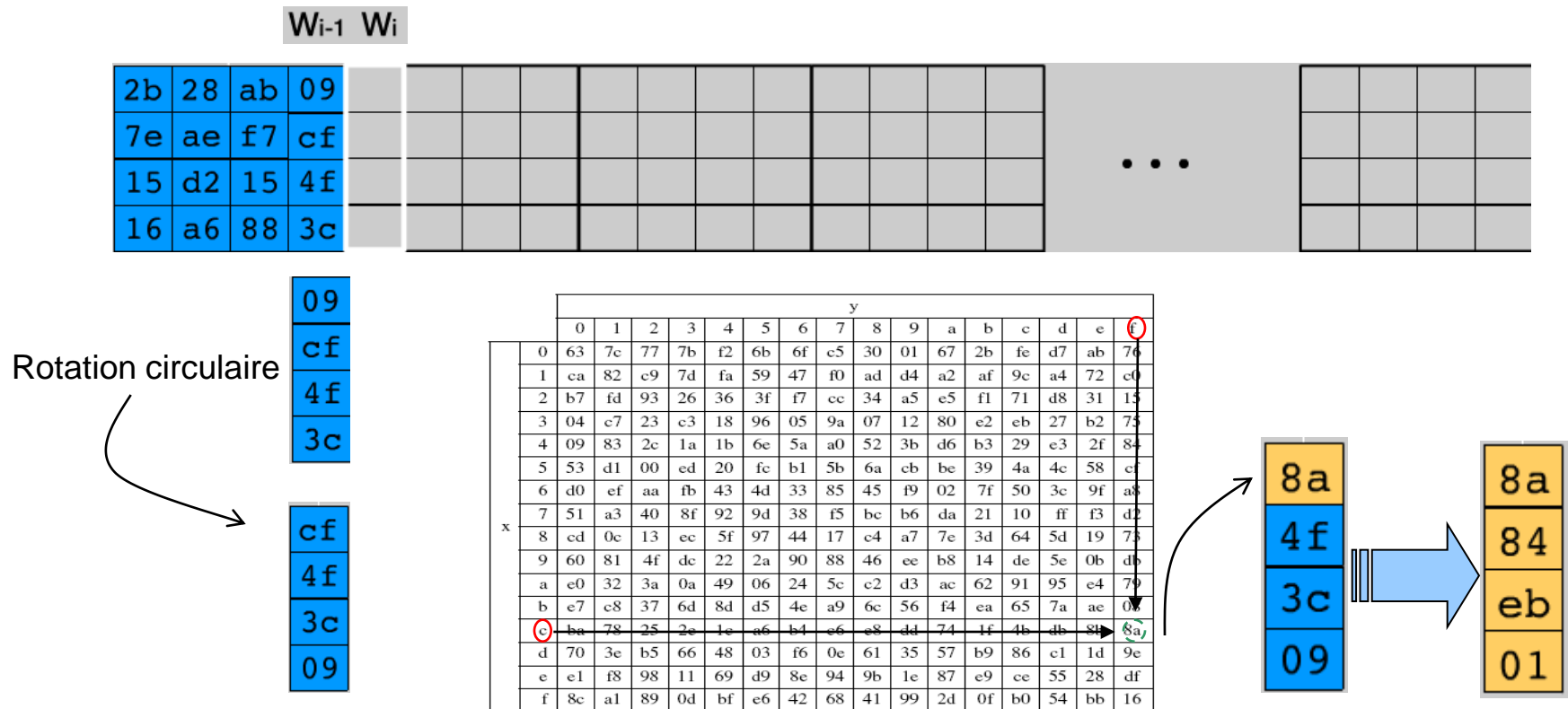
Chiffrement à clef symétrique : AES

- AddRoundKey (State, Ki)

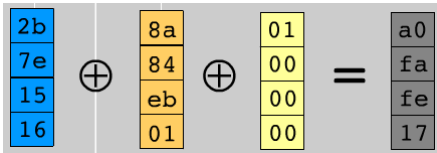
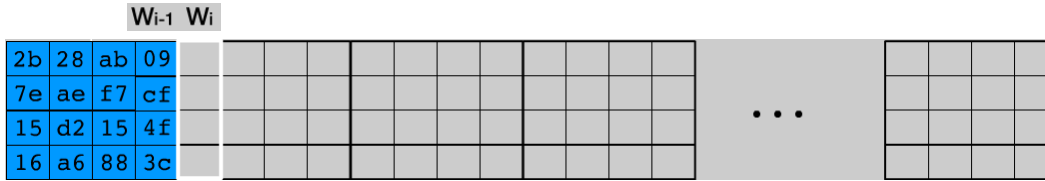


Chiffrement à clef symétrique : AES

- Diversification de la clef (*KeyExpansion*)
 - Permet de diversifier la clef K de $4 \cdot N_k$ dans une clef étendue W de $4N_b(N_r+1)$ octets

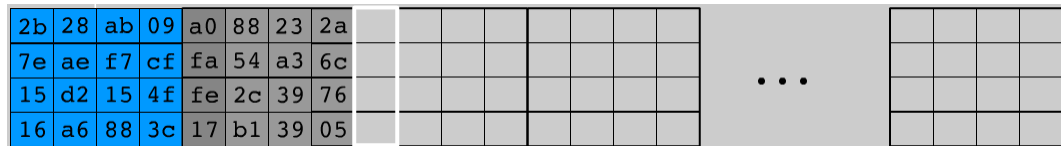
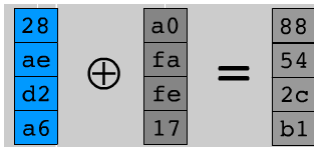
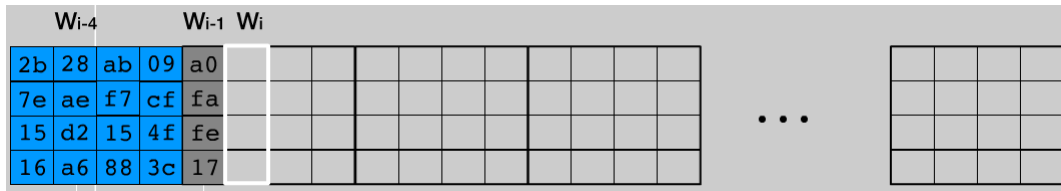


Chiffrement à clef symétrique : AES



01	02	04	08	10	20	40	80	1b	36
00	00	00	00	00	00	00	00	00	00
00	00	00	00	00	00	00	00	00	00
00	00	00	00	00	00	00	00	00	00

Tableau de constante de tours Rcon[i]



Rotation

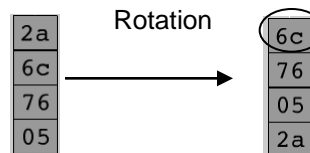


Tableau Sbox

50
38
6b
e5

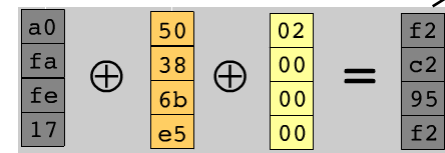
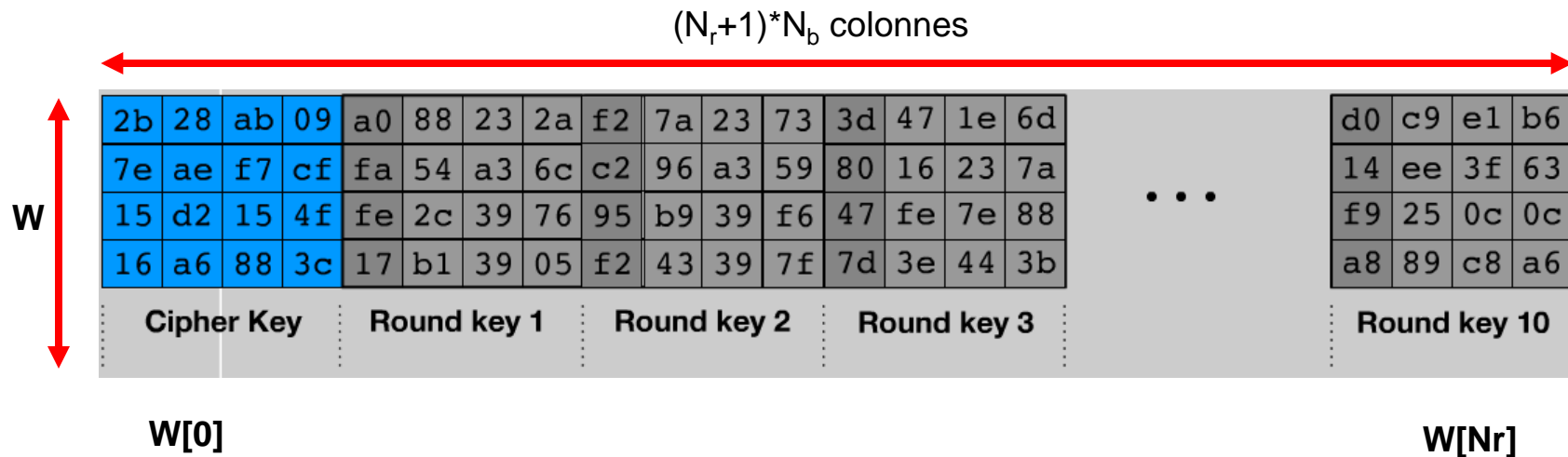


Tableau Rcon[i]

Chiffrement à clef symétrique : AES

- Clef étendue de 10 tours



Chiffrement à clef symétrique : AES

- Avantages et spécificités

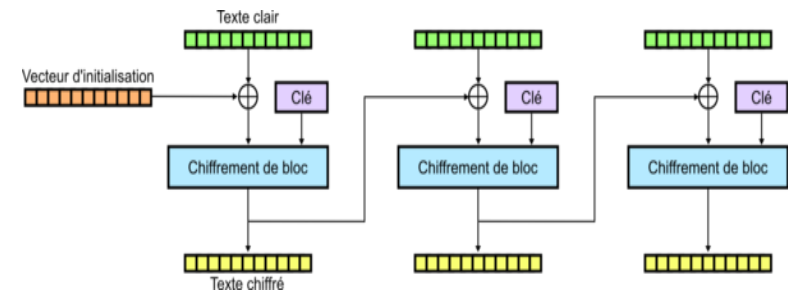
- Grande résistance à toutes les attaques connues
- Très grande rapidité (chiffrement/déchiffrement)
- Véritable structure mathématique
- Clé de 256 bits largement suffisant pour les applications commerciales
- 80 % des acteurs du marché utilisent AES

- Attaques ?

- Pour l'instant, AES n'a pas été cassé
- Pas de failles avec une clef de chiffrement 128 bits
- Principales failles (niveau du logiciel et partage de clés)

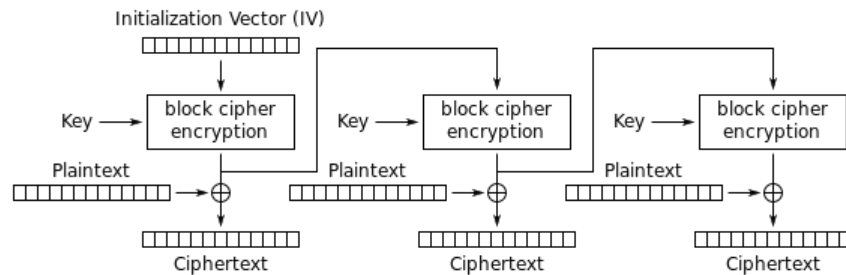
Modes opératoires de chiffrement symétrique

- Quatre modes de chiffrement par bloc (64 bits)
 - ECB : Electronic CodeBook
 - Chiffrer un bloc indépendamment des autres blocs
 - Parallélisme utilisé / peu utilisé
 - CBC : Cipher Block Chaining
 - Dépendance entre les blocs successifs
 - Complexité dans le processus de chiffrement
 - Pas de parallélisme / Très utilisé
 - CFB : Cipher FeedBack
 - Chiffrement par flux
 - Taille variable de blocs
 - OFB : Output FeedBack
 - Beaucoup de problèmes de sécurité
 - Peu conseillé (chiffrement qu'en XOR)
- Algorithmes utilisant ces modes
 - DES
 - AES

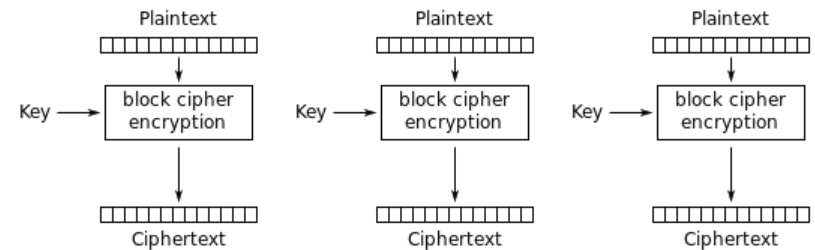


Modes opératoires de chiffrement symétrique

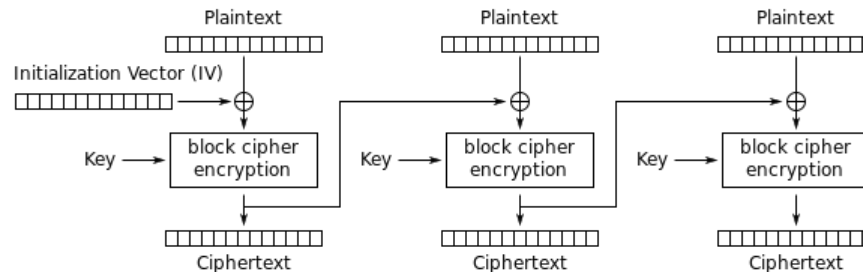
- Mode opératoire par blocs



Output Feedback (OFB) mode encryption



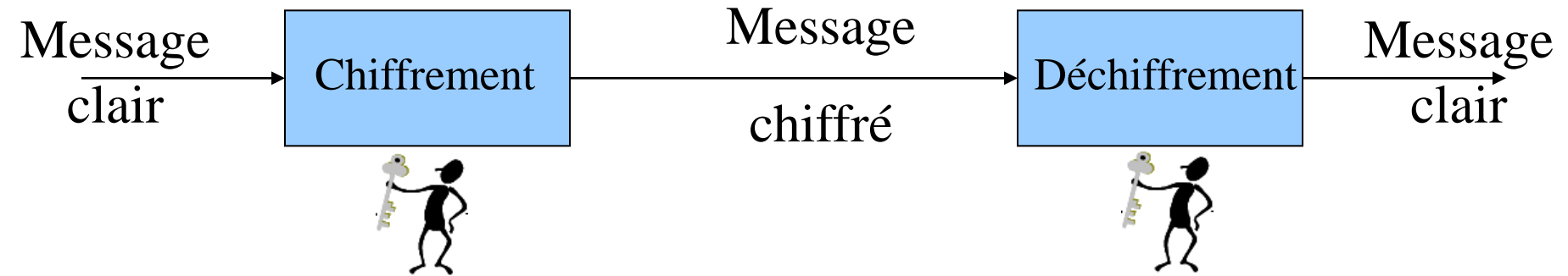
Electronic Codebook (ECB) mode encryption



Cipher Block Chaining (CBC) mode encryption

Algorithme symétrique

A → B



- Une seule clef pour le chiffrement/déchiffrement
- Exemple : DES, 3DES, AES, RC4
- Comment les deux parties partagent-elles une clef ?

- **Echange de clés**
 - Aspect important dans la création d'une connexion sécurisée
- **Algorithme de Diffie-Hellman**
 - Partage de clés même si le canal de communication n'est pas sécurisé
 - Clé utilisée pour chiffrer les données avec l'algorithme choisi par A et B

Echange de la clé secrète : Algorithme Diffie-Hellman



Alice



Mise en accord publique sur 2 nombres premiers g et p

Génère une clef secrète A
(nombre premier)

Calcule son élément public

$$A' = g^A \bmod p$$

Envoie A' à Bob

Calcule $K = (B')^A \bmod P$

Génère une clef secrète B
(nombre premier)

Calcule son élément public

$$B' = g^B \bmod p$$

Envoie B' à Alice

Calcule $K = (A')^B \bmod P$



Attaquant : aucune information sur K
à partir de A' et B'

Echange de la clé secrète : Algorithme Diffie-Hellman



Alice



clef secrète $A=5$
 $A' = g^A \bmod p = 11^5 \bmod 13$
 $A' = 161051 \bmod 13$
Envoie $A' = 7$ à Bob

Calcule $K = (B')^A \bmod p$
alors $K = (2)^5 \bmod 13$
 $K = 32 \bmod 13$
 $K=6$

$g=11$ et $p=13$

$A'=7$

$B'=2$

clef secrète $B=19$
 $B' = g^B \bmod p = 11^{19} \bmod 13$
 $B' = 61159090448414546291 \bmod 13$
Envoie $B'=2$ à Alice
Calcule $K = (A')^B \bmod p = (7)^{19} \bmod 13$
 $K = 11398895185373143 \bmod 13$
 $K=6$

clef secrète pour un algorithme
symétrique choisi (chiffrement et
déchiffrement)



$K = ?$

$(A'=7, B'=2, g=11, p=13)$

Je ne connais pas A et B !!

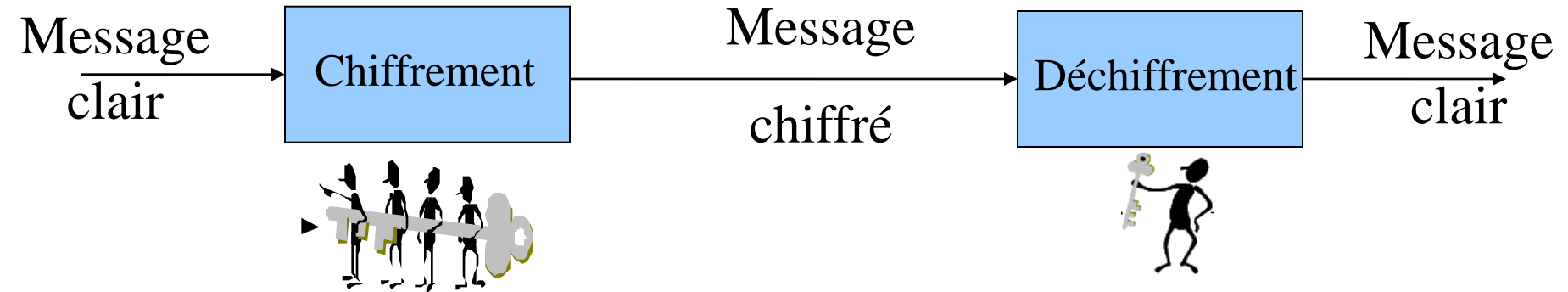
DH est sensible à l'attaque MITM !!!



Chiffrement asymétrique et signature numérique

Cryptosystème à clé publique

A → B



- Deux clés : clé publique / clé privée
- Exemple : RSA (Rivest-Shamir-Adleman)
- Utilisation en 3 catégories
 - Chiffrement / déchiffrement : confidentialité
 - Signature numérique : authentification
 - Échange de clés (pour le chiffrement symétrique)

Chiffrement Asymétrique RSA

- RSA

- Développé en 1977 par Ron Rivest, Adi Shamir et Len Adleman
- Algorithme asymétrique de cryptographie à clé publique
- Plusieurs services de sécurité

- But

- Transmettre un message codé entre 2 entités
- Seul le récepteur “officiel” puisse le décrypter

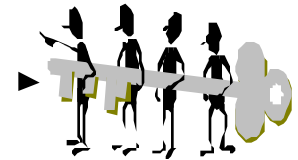
- Principe

- Basé sur la difficulté de factoriser
 - Un nombre très grand quand ce nombre est le produit de deux nombres premiers très grands eux aussi

Chiffrement Asymétrique RSA

- M : message à chiffrer (*Plaintext*)
- C : message chiffré (*Ciphertext*)
- n : produit de deux nombres premiers
- Algorithme RSA
 - Clé publique : couple (e, n)
 - Clé privée : d
- Pour chiffrer le message M , on calcule :
 - $C = M^e \text{ modulo } n$
- Pour déchiffrer C on calcule :
 - $M = C^d \text{ modulo } n$

Clef publique (e, n)

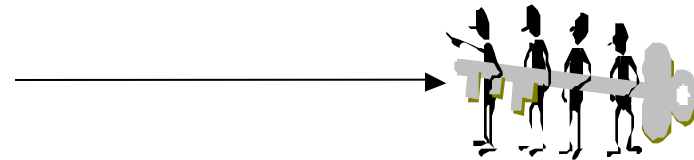
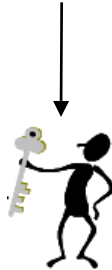


Clef privée d



Chiffrement Asymétrique RSA

- M : message à chiffrer (*Plaintext*)
- C : message chiffré (*Ciphertext*)
- Pour chiffrer le message M :
 - On choisit deux grands entiers naturels premiers p et q et on calcule leur produit $n = p \cdot q$
 - On choisit un entier e premier avec $(p-1) \cdot (q-1)$
 - $C = M^e \text{ modulo } n$
- Pour déchiffrer C on calcule :
 - On calcule $e \cdot d \text{ mod } ((p-1)(q-1)) = 1$
 - $M = C^d \text{ modulo } n$
- Clé publique est le couple (e, n)
- Clé privée : d



Chiffrement Asymétrique RSA : Exemple

- Choisir au hasard 2 nombres premiers
 - Ex : $p = 13$ et $q = 17$
- Calculer $n = p.q = 13 \cdot 17 = 221$
- On pose $j = (p-1).(q-1) = 12 \cdot 16 = 192$
- Sélectionne e
 - e et j soient premiers entre eux avec $1 < e < j$
 - « Deux entiers a et b sont premiers entre eux, s'ils n'ont aucun facteur en commun »
 - On choisit $e = 5$
 - Clé publique : (221, 5)
- On calcule d tel que :
 - $e.d = 1 \bmod j \Rightarrow 5.d = 1 \bmod 192$
 - clé privée $d = 77$

Théorème de Bezout

Chiffrement Asymétrique RSA : Exemple

- Clé publique $(e,n) = (5,221)$
- Clé privée $d = 77$
- M est le message à chiffrer : « bonjour »
- B= 98, o= 111, n= 110, j= 106, u= 117, r= 114
- Chiffrement
 - $C = M^e \text{ modulo } n$
 - $C1=98^5 \text{ mod } 221 = 115$
 - $C2=76$, $C3=145$, $C4=123$, $C5=76$, $C6=104$, $C7=173$
 - $C=sL\ae\{Lhi$

Plaintext	b	o	n	j	o	u	r
Code	98	111	110	106	111	117	114
Ciphertext	s	L	æ	{	L	h	i
Code	115	76	145	123	76	104	173

Chiffrement Asymétrique RSA : Exemple

- Déchiffrement

- $M = C^d \text{ modulo } n$

- $M1 = 115^{77} \text{ mod } 221 = 98 \dots\dots\dots b$
 - $M2 = 76^{77} \text{ mod } 221 = 111 \dots\dots\dots o$
 - $M3 = 145^{77} \text{ mod } 221 = 110 \dots\dots\dots n$
 - $M4 = 123^{77} \text{ mod } 221 = 106 \dots\dots\dots j$
 - $M5 = 76^{77} \text{ mod } 221 = 111 \dots\dots\dots o$
 - $M6 = 104^{77} \text{ mod } 221 = 117 \dots\dots\dots u$
 - $M7 = 173^{77} \text{ mod } 221 = 114 \dots\dots\dots r$

Plaintext	b	o	n	j	o	u	r
Code	98	111	110	106	111	117	114
Ciphertext	s	L	æ	{	L	h	i
Code	115	76	145	123	76	104	173

Chiffrement Asymétrique RSA : cryptanalyse

- La seule technique connue pour briser RSA consiste à calculer l'exposant de déchiffrement.
 - $d = e^{-1} \bmod (p-1)(q-1)$ où $pq=n$.
 - Mais, il faut factoriser n !!!
 - Très difficile
 - Exemple de factorisation
 - $N =$
310741824049004372135075003588856793003734602284272754572016194882320644051808150455634682967172328678
2437916272838033415471073108501919548529007337724822783525742386454014691736602477652346609
 - $P =$
16347336458092538484431338838650908598417836700330 92312181110852389333100104508151212118167511579
 - $Q =$
1900871281664822113126851573935413975471896789968515493666638539088027103802104498957191261465571

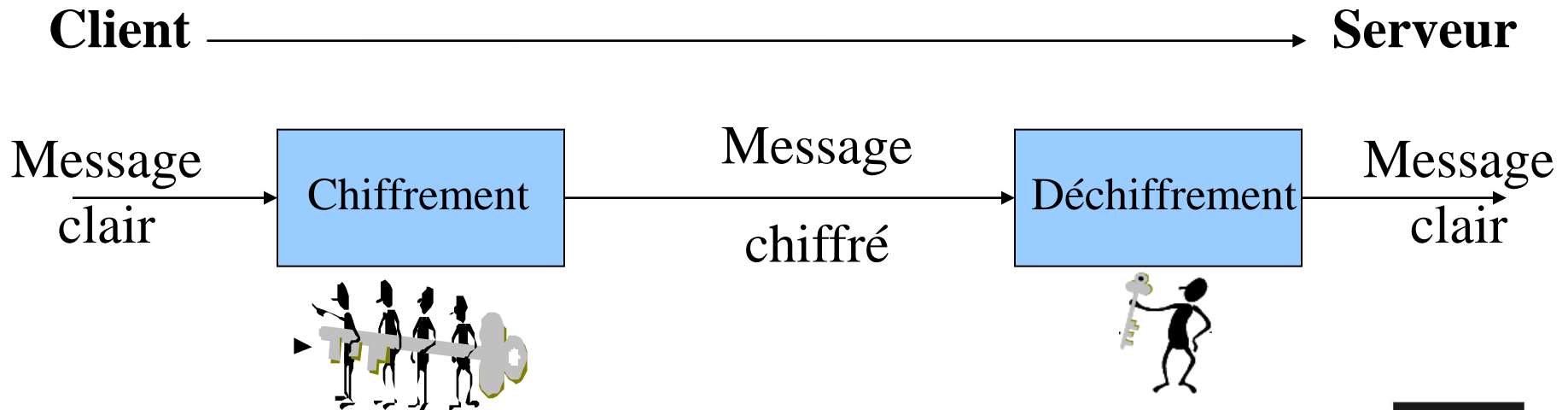
Chiffrement Asymétrique RSA : recommandations

- Ne jamais utiliser de valeur n trop petite
- Ne pas utiliser de clé secrète trop courte ($<$ racine n)
- N'utiliser que des clés fortes ($p - 1$ et $q - 1$ ont un grand facteur premier)
- Ne pas chiffrer de blocs trop courts
- Ne pas utiliser un n communs à plusieurs clés

Chiffrement Asymétrique ElGamal

- **Algorithme ElGamal**

- Publié par Tahar El Gamal en 1987
- Sa sécurité dépend de la difficulté de calculer les logarithmes discrets ($3^k \equiv 5 \pmod{7} \Rightarrow K=?$)
- Utilisé pour le chiffrement et la signature électronique.
- Utilisé par le logiciel libre GNU Privacy Guard, et PGP (Pretty Good Privacy)



Chiffrement Asymétrique ElGamal

- Exemple

- $p=11$, $g=6$, $x=8$
- $y=6^8 \pmod{11}=4$
- Public : 4, 6, 11
- Private : $x=8$

Public key:

p (a prime number)
 $g, x < p$ (two random numbers)
 $y \equiv g^x \pmod{p}$
 y, g and p : public key

Private key:

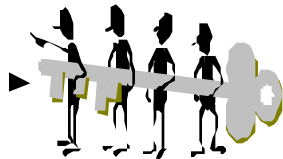
$x < p$

Enciphering:

k : a random number such that $\gcd(k, p-1) = 1$
 $r \equiv g^k \pmod{p}$
 $s \equiv (y^k \pmod{p}) (m \pmod{p-1})$

Deciphering:

$m \equiv s/r^x \pmod{p}, 0 \leq m \leq p-1$



Clef publique : P, g et y



Clef privée : x

Chiffrement Asymétrique ElGamal



Alice

Message à chiffrer $m = 5$

Générer $k=7$ random

$$r = g^k \bmod p$$

$$s = y^k \bmod p * m \bmod (p-1)$$

Envoie r et s au serveur

$$r = 6^7 \bmod 11 = 8$$

$$s = 4^7 \bmod 11 * 5 \bmod 10 = 25$$

$$(r, s) : (8, 25)$$

Mise en accord publique sur
 $p=11$, $g=6$ et $y=4$



$X=8$

Recevoir $r=8$ et $s=25$

$$m = s / r^x \bmod (p)$$

$$r^x \bmod 11 = 8^8 \bmod 11$$

$$16777216 \bmod 11 = 5$$

$$m = 25/5 = 5$$



Pirate : aucune information sur x et k

Chiffrement Asymétrique ElGamal

- Avantages

- Difficile à casser

- Basé sur les logarithmes discrets

- Algorithme non déterministe

- Deux chiffrements du même message M donneront deux messages chiffrés différents

- Inconvénients

- La taille de *ciphertext* est 2 fois plus longue que le *plaintext*

- El Gamal est 2 fois plus lent que le RSA

Chiffrement / signature

- Chiffrement RSA

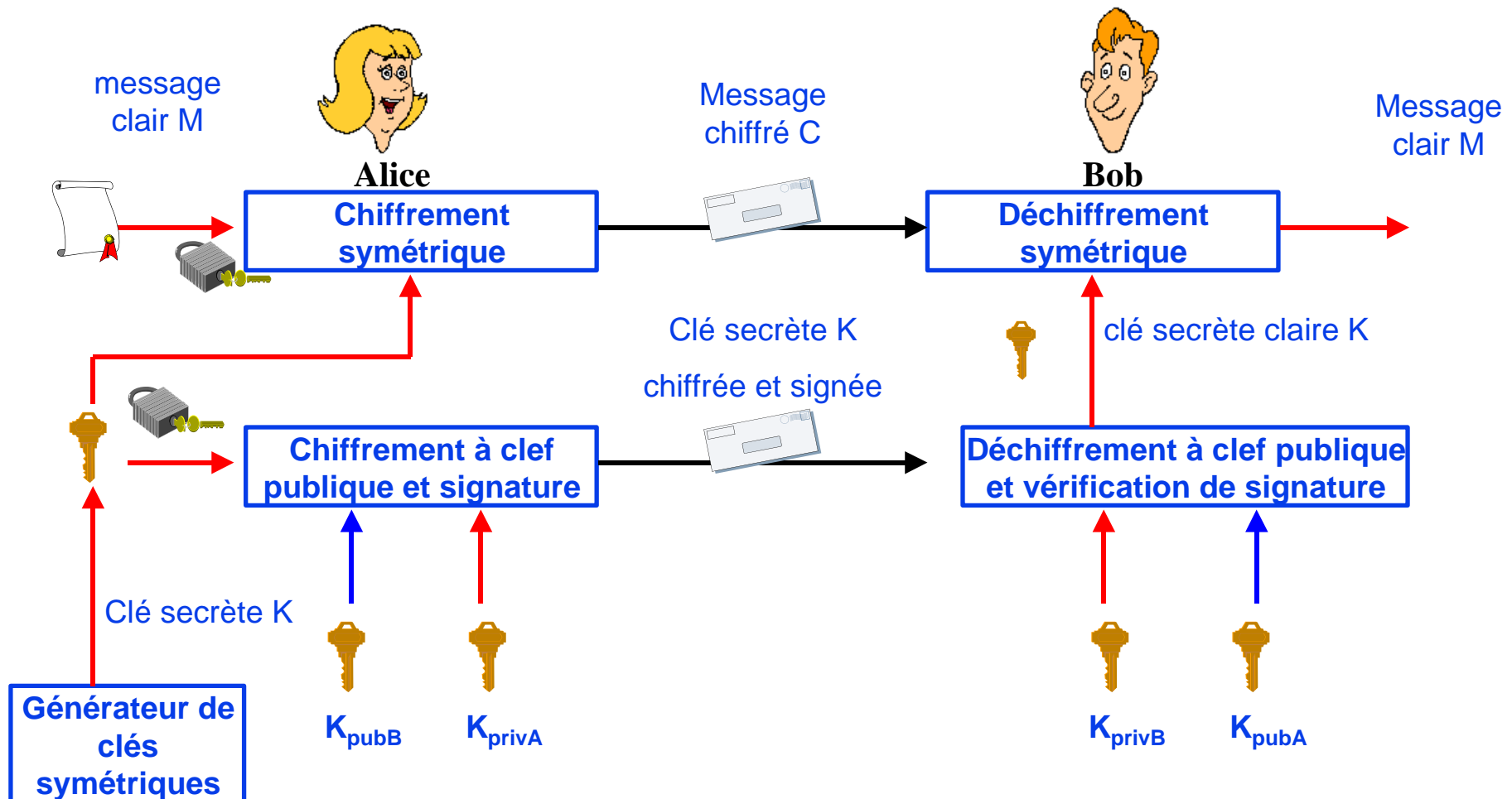
- Clé publique pour chiffrer
- Clé privée pour déchiffrer
- Ex: soit $p=13$, $q=17$, $e=5$ et $M=98$
 - $K_{pb}=(192, 5)$ et $K_{pr}=77$
 - $C = M^e \text{ modulo } n \Rightarrow C=115$
 - $M = C^d \text{ modulo } n \Rightarrow M=98$

- Signature

- Clé publique pour vérifier
- Clé privée pour signer (chiffrer !)
- Ex :
 - $C = M^d \text{ modulo } n = 98^{77} \text{ mod } 221 = 115$
 - $M = C^e \text{ modulo } n = 115^5 \text{ mod } 221 = 98$

Chiffrement / signature

- Transport sécurisé de clé symétrique en asymétrique





Fonctions de hachage

Fonction de hachage

- **Caractéristiques**

- Troisième grande famille d'algorithmes utilisés en cryptographie
- Message de longueur quelconque transformé en un message de longueur fixe inférieure à celle de départ
- Message réduit porte le nom de "Haché" ou de "Condensé«

- **Usage**

- Condensé utilisé comme empreinte digitale du message original
- Assure l'intégrité de données

- **Fonctions les plus connues**

- MD5 , SHA-1, SHA-256, Whirlpool

* Non prédictibles : les entrées et les sorties sont indépendantes

** considérée cassée lorsqu'il existe un algorithme permettant de trouver une collision

Fonction de hachage

- Caractéristiques

- Fonction unidirectionnelle

- A partir de $H(M)$ il est impossible de retrouver M

- Fonction sans collisions

- A partir de $H(M)$ et M il est impossible de trouver $M' \neq M$ tel que $H(M') = H(M)$

- Exemples

- Fonction de hachage MD5 : empreinte numérique de 128 bits

- $\text{md5}(\text{"Bonjour"}) = \text{ebc58ab2cb4848d04ec23d83f7ddf985}$

- $\text{md5}(\text{"Gendarmerie"}) = \text{5d4a85c5186d9883d453fa7ffec63f2a}$

- $\text{md5}(\text{"La gendarmerie"}) = \text{a1e53f21f46f8f9e889f0712196e9b48}$

Fonction de hachage MD5

- Proposé par *Ronald Rivest* à MIT en 1991, RFC 1321
- Entrée : Message $L \times 512$ bits, sortie : empreinte de taille 128 bits
- Vue d'ensemble
 - Traiter le message par blocs de 512 bits
 - 4 rondes de 16 opérations fonction du bloc (512), des buffers (A, B, C, D) et de fonctions primitives
 - Résultat (4×32 bits) de chaque ronde est utilisé pour l'initialisation des registres suivants
 - Résultat final est obtenu en additionnant A,B,C,D
- Buffers Initialisés à
 - A = 01 23 45 67
 - B = 89 ab cd ef
 - C = fe dc ba 98
 - D = 76 54 32 10
- 4 fonctions non linéaires

$$F(X, Y, Z) = (X \cdot Y) + (\bar{X} \cdot Z)$$

$$G(X, Y, Z) = (X \cdot Z) + (Y \cdot \bar{Z})$$

$$H(X, Y, Z) = X \oplus Y \oplus Z$$

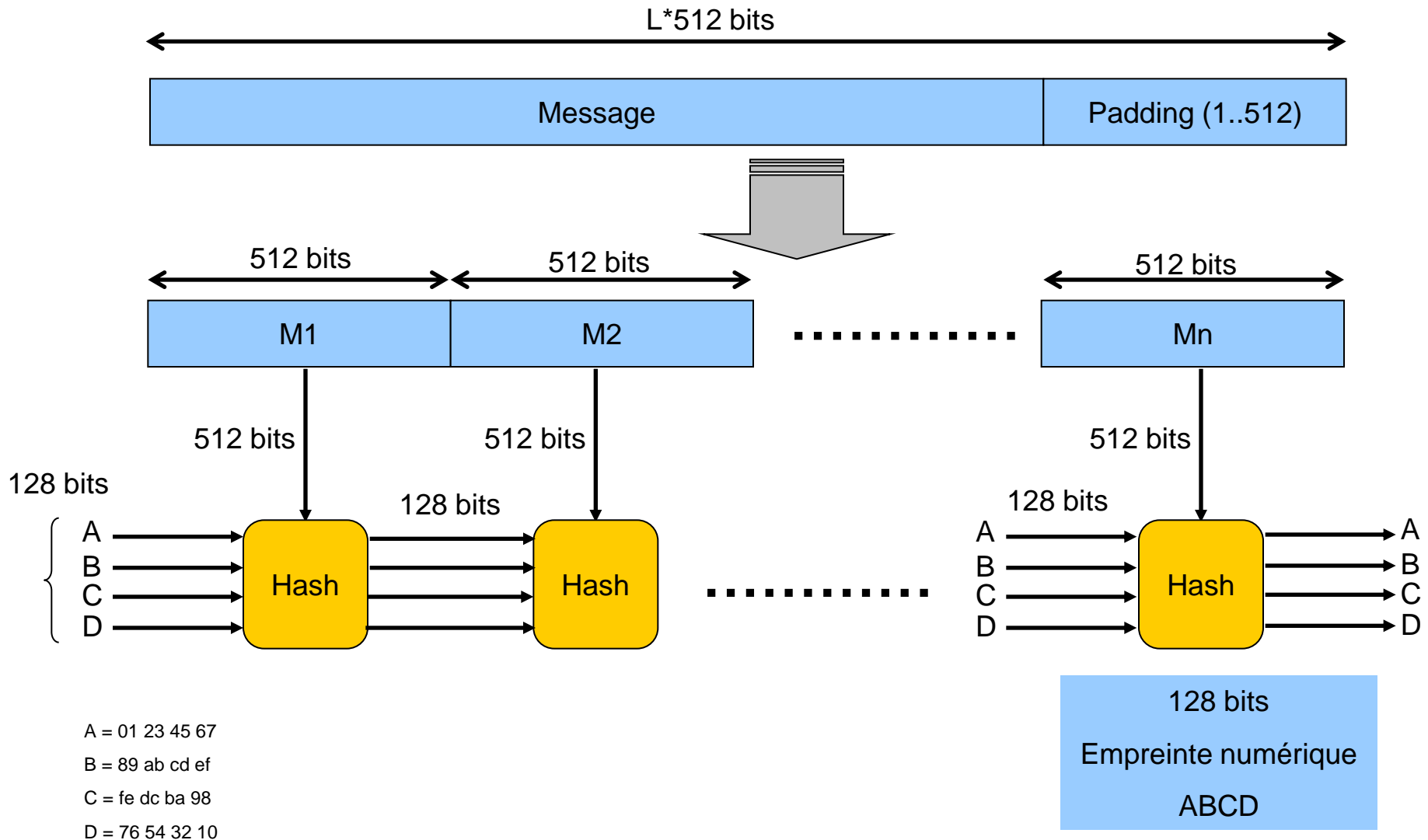
$$I(X, Y, Z) = Y \oplus (X + \bar{Z})$$

Entrée : 3 variables de 32 bits chacune

Sortie : 32 bits

• AND + OR \oplus XOR

Fonction de hachage MD5



Fonction de hachage MD5

- Transformations FF, GG, HH, II

- FF(a, b, c, d, M[k], s, i) :

- $$a = b + ((a + F(b, c, d) + M[k] + T[i] \lll s)$$

- GG(a, b, c, d, M[k], s, i) :

- $$a = b + ((a + G(b, c, d) + M[k] + T[i] \lll s)$$

- HH(a, b, c, d, M[k], s, i) :

- $$a = b + ((a + H(b, c, d) + M[k] + T[i] \lll s)$$

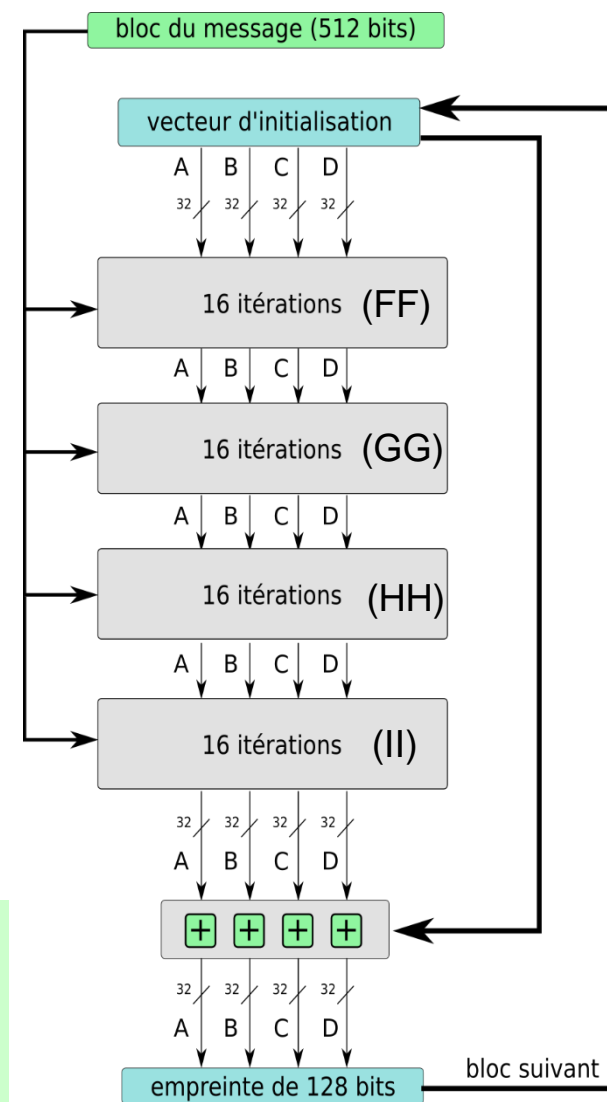
- II(a, b, c, d, M[k], s, i) :

- $$a = b + ((a + I(b, c, d) + M[k] + T[i] \lll s)$$

• T[i] : $i = 1, 2, \dots, 64$, valeur obtenu par la fonction sinus, $T[1] = 2^{32} \cdot \text{Abs}(\sin[i])$, avec i en radian. Ex: $T[1] = 4294967296 \cdot 0.8414 = \text{d76aa478}$ en hexa

• s: décalage à gauche de s bits

• M[k] : $0 \leq k \leq 15$, $k^{\text{ième}}$ sous-bloc du message



Fonction de hachage MD5

- Exemple :
 - 152 bits de données : 7a138b25 24af17c3 17b439a1 2f51c5a8 8051cb36
 - Padded message (512bits) = Original message(152bits) + Padding(360bits).
 - A = 67452301, B = efcdab89, C = 98badcfe, D = 10325476
 - Tour 1:
 - $FF[a, b, c, d, M[0], 7, 1]: a = b + ((a + F(b, c, d) + M[k] + T[l] \lll s), a=b+U$
 - $a = 67452301$
 - $b = efcdab89$
 - $M[0]=7a138b25$
 - $T[0]=d76aa478$
 - $F(b,c,d)= b.c + b.d = 98badcfe$
 - Alors $U= efcdab89 + (67452301+98badcfe+ 7a138b25 + d76aa478 \lll 7)$
 - $a=b + U: efcdab89 + bf17ce28 = aee579b1$
 - Il faut faire encore 15 autres itérations de FF pour obtenir A, B, C et D de la première tour
 - Répéter l'opération avec GG, HH et II pour obtenir la signature

Fonction de hachage MD5

- Bilan sur les fonctions de hachage

Fonction	Empreinte	Résistance aux collisions
MD5	128 bits	Cassée en 2005
SHA-1	160 bits	Cassée en 2005
SHA-256	256 bits	Sûr
Whirlpool	512 bits	Sûr

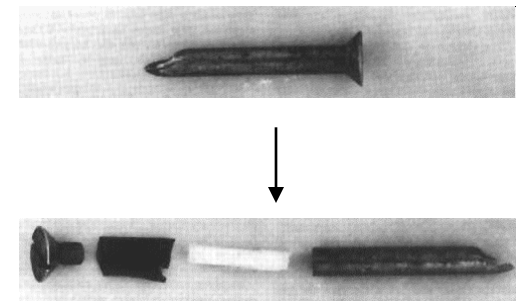
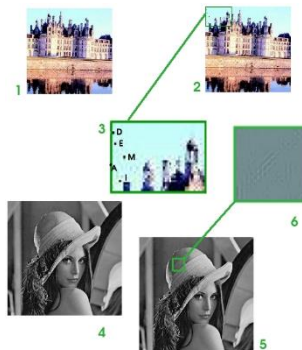
- Une fonction de hachage suffit-elle pour faire une signature électronique ? Non :
 - possède la propriété « si message change, la signature change »,
 - mais ne permet pas de s'assurer de l'identité du signataire

Stéganographie

La stéganographie : qu'est-ce que c'est ?

- Stéganographie

- Art de dissimuler des données dans d'autres données
- Support : fichier texte, image, audio, vidéo, système de fichier, code source
- Ne rend pas un message inintelligible
- Utilisé pour garder secret le fait même de communiquer
- Existe depuis longtemps (avant l'invention de l'ordinateur)
- Plusieurs techniques
 - Utiliser un sous-ensemble de lettres ou de mots dans un messages plus long
 - Utiliser l'encre sympathique
 - Utiliser un pixel précis dans une séquence d'images vidéo...



La stéganographie : qu'est-ce que c'est ?

- Exemple

Antoine et Bob sont deux ingénieurs dirigés par Caroline. Antoine écrit le texte du tableau qui semble louer les qualités de son chef. Fortuitement, le document tombe entre les mains de Caroline qui est tout d'abord flattée de ce portrait.

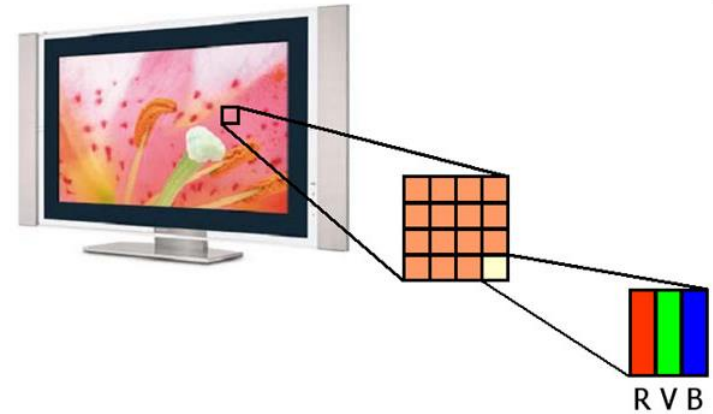
Cacher une information dans une information

Bob ne lit pas tout le texte,
mais seulement les lignes impaires.

Mon chef, est toujours en train de
travailler à son bureau avec assiduité et diligence, sans jamais
perdre son temps en jasant avec ses collègues. Jamais il ne
refuse de passer du temps pour aider les autres et pourtant, il
finit ses projets à temps. Très souvent, il rallonge
ses heures pour terminer son travail, parfois même en sautant
les pauses café. C'est une personne qui n'a absolument aucune
vanité en dépit de ses accomplissements remarquables et de sa grande
compétence en informatique. C'est le genre d'employé de qui on
parle avec grande estime et respect, le genre de personne dont on ne
peut se passer. Je crois fermement qu'il est prêt pour la
promotion qu'il demande, considérant tout ce qu'il nous ap-
porte. L'entreprise en sortira grandie.

La stéganographie : qu'est-ce que c'est ?

- Dissimulation d'information dans une image
 - Documents "porteurs" sont généralement des images (BMP, GIF, videos, ...) ou des sons (WAV, ...)
 - Information sensibles à cacher
- Structure d'image
 - Composée de pixels
 - Un pixel est constitué de 3 octets
 - un octet pour la composante rouge
 - un octet pour la composante verte
 - un octet pour la composante bleue.
 - RVB (Rouge Vert Bleu) -> $256 \times 256 \times 256 = 16777216$ couleurs différentes, ce qui est largement plus que ne peut distinguer l'œil humain
 - Image de 800×600 pixels = $800 \times 600 \times 3 = 1440000$ octets
 - On peut stocker une autre image ou un texte dans les bits de chaque octet de couleur



La stéganographie : qu'est-ce que c'est ?

- Cacher l'information dans l'image :
 - Utiliser un bit à chaque octet RVB qui compose chaque pixel de l'image
 - En retirant 1 bit, on dégrade l'image, mais ce n'est pas visible à l'œil nu...
 - on peut donc récupérer ce bit à chaque fois et l'utiliser pour stocker les données que l'on souhaite.
 - Exemple
 - Image 800x600 pixels permet de stocker une information de 180Koctets ($800 \times 600 \times 3/8$)
 - Exemple : stocker un document Word à l'intérieur de l'image...
 - Possibilité de dissimuler des informations dans d'autres formats d'images, des fichiers sonores, des vidéos, du flash, etc.

La stéganographie : qu'est-ce que c'est ?

- Effet visuel de la modification des bits de poids faibles



La stéganographie : qu'est-ce que c'est ?

- Cacher une image dans une autre image !
 - Variations de couleurs entre les deux photos sont totalement invisibles à l'œil nu
 - Image de droite cache bien un message !



La stéganographie : qu'est-ce que c'est ?

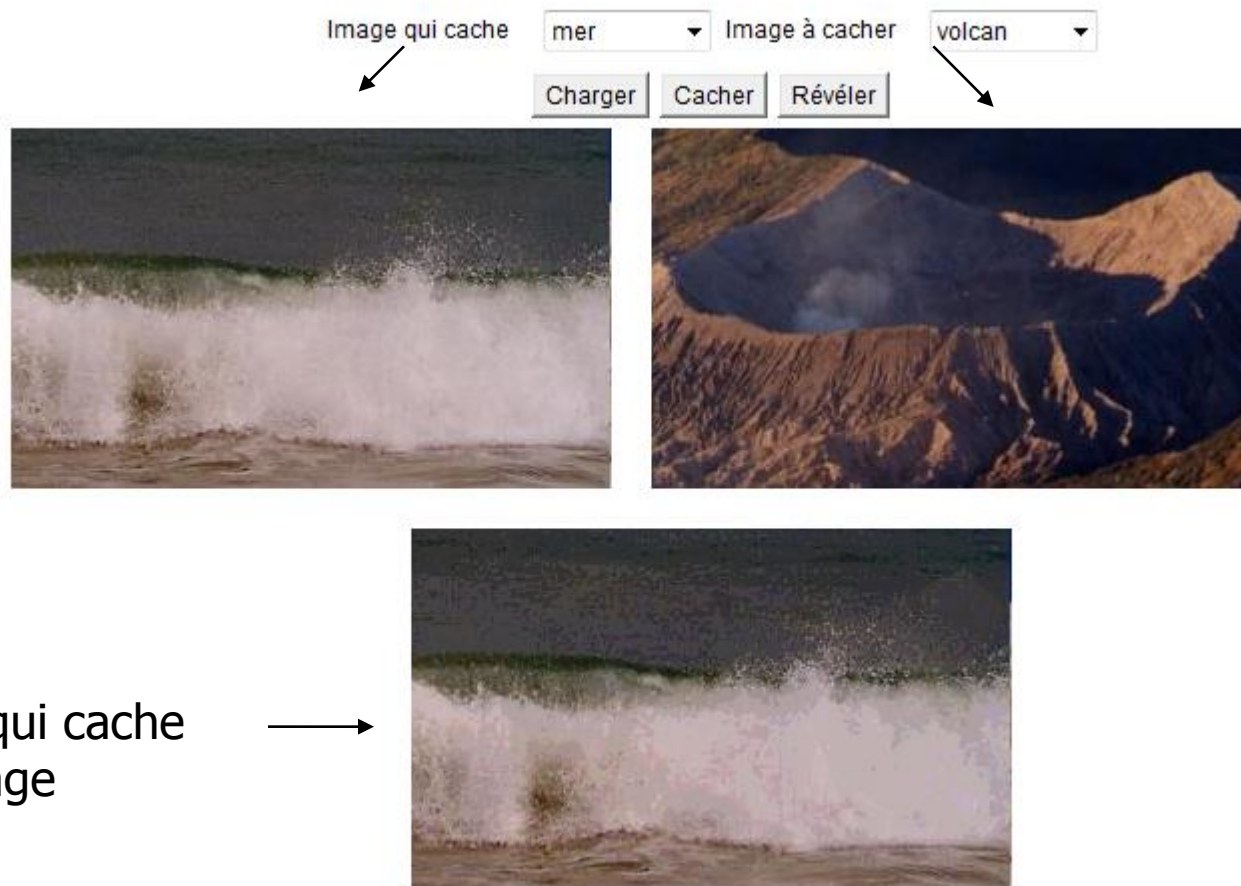
- Cacher une image dans une autre image !
 - Pour chaque pixel de la première image, et pour chaque couleur R,G,B de cette image, on remplace les 4 bits de poids faible par les 4 bits de poids fort correspondants dans la seconde image
 - Exemples :

Image 1	R1=01001110 G1=01101111 B1=11111111
Image 2	R1=01110011 G1=01110110 B1=10101010
Image qui cache	R1=01000111 G1=01100111 B1=11111010
Image 1 retrouvée	R1=01000000 G1=01100000 B1=11110000
Image 2 retrouvée	R1=01110000 G1=01110000 B1=10100000

Image initiale	R1=01001110 G1=01101111 B1=11111111 R2=01110011 G2=01110110 B2=10101010
Message	101100011011
Image qui cache le message	R1=01001110 G1=01101111 B1=11111100 R2=01110001 G2=01110110 B2=10101011

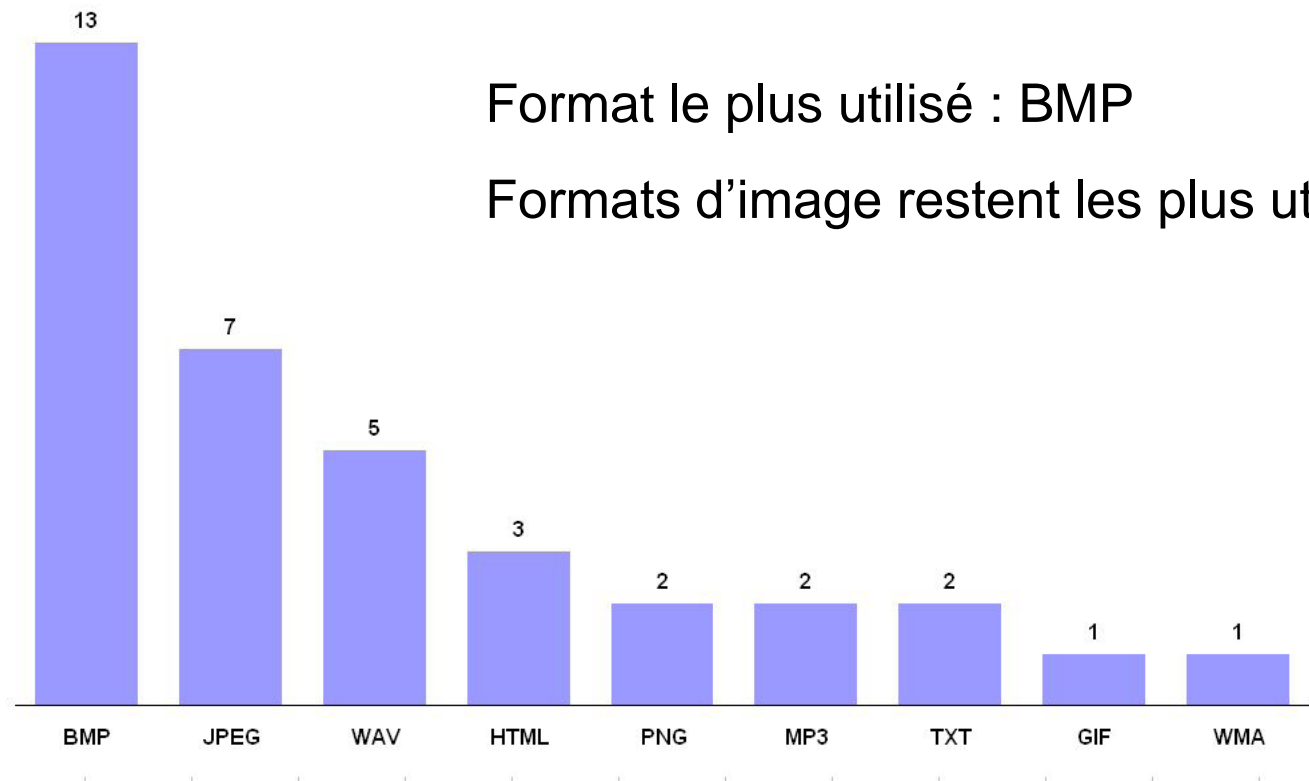
La stéganographie : qu'est-ce que c'est ?

- Cacher une image dans une autre image !



La stéganographie : qu'est-ce que c'est ?

- Formats de fichier dans la stéganographie



La stéganographie : qu'est-ce que c'est ?

- Utilisation de la stéganographie
 - Cacher des informations secrètes
 - Watermarking
 - Fortement utilisé dans l'industrie
 - Cacher un copyright dans une image => prouver l'originalité de l'image
- Détection de la stéganographie
 - Recherche d'information : steganalysis
 - Difficulté de la détection : comment l'information est cachée ?
 - Analyse mathématique et/ou statistique
 - Outil : stegdetect

La stéganographie : qu'est-ce que c'est ?

- Inconvénients

- Enorme overhead pour cacher peu d'informations
- Dissimulation dépendant de la nature de l'image
 - Information dissimulée dans une image BMP est détruite si l'image est convertie en JPG
 - Information cachée est fortement altérée par le compactage

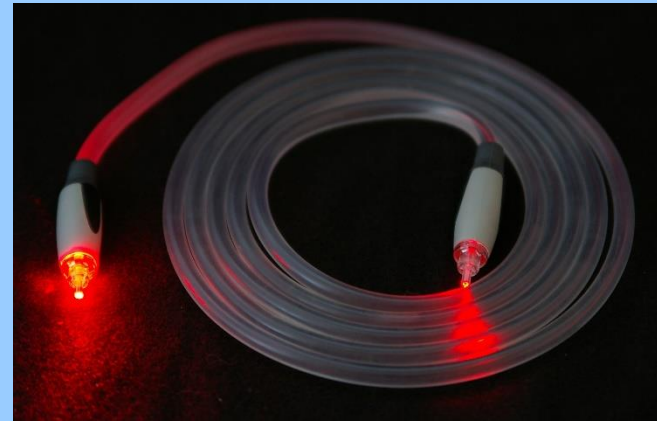
La stéganographie : qu'est-ce que c'est ?

- Nombreux logiciels de stéganographie sont disponibles
 - Windows
 - Steganos Privacy Suite 12
 - NeoByteSolution Invisible Secrets
 - WbStego4Open
 - Hermetic Systems Hermetic Stego
 - Linux
 - OutGuess 0.2
 - StegHide
 - WbStego4Open

Cryptographie quantique

Cryptographie quantique

- Cryptographie classique se base sur les mathématiques pour échanger une clé secrète
 - Factorisation des nombres premiers
 - Logarithmes discrets
 - mais...est-ce que le chiffre parfaitement sûr existe ?
- Cryptographie quantique
 - Sécurité garantie non par des théorèmes mathématiques, mais par les principes fondamentaux de la physique quantique



Cryptographie quantique

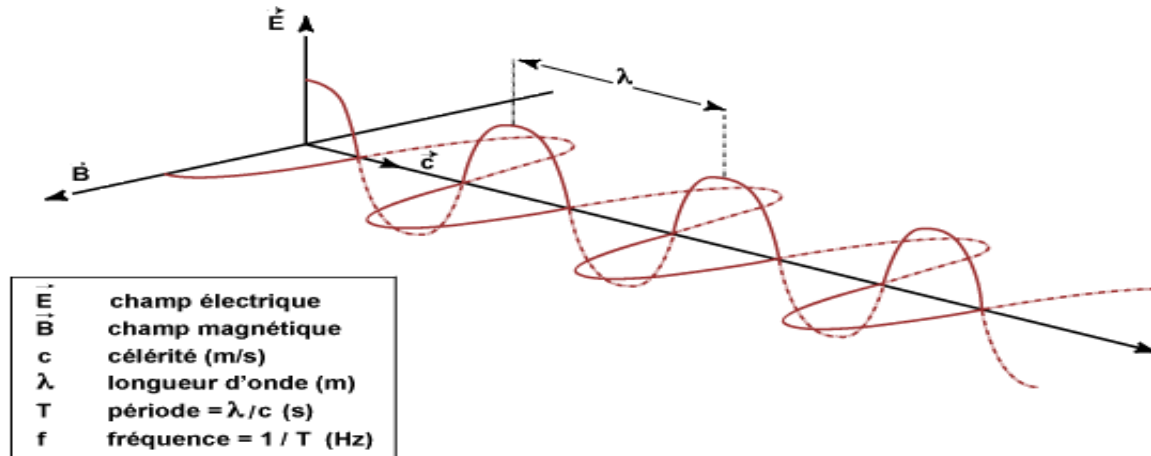
- **Rappels physiques**

- **James Maxwell (1865) : Onde**

- La lumière est un faisceau d'ondes électromagnétiques se déplaçant à une vitesse c de 300.000 km/s

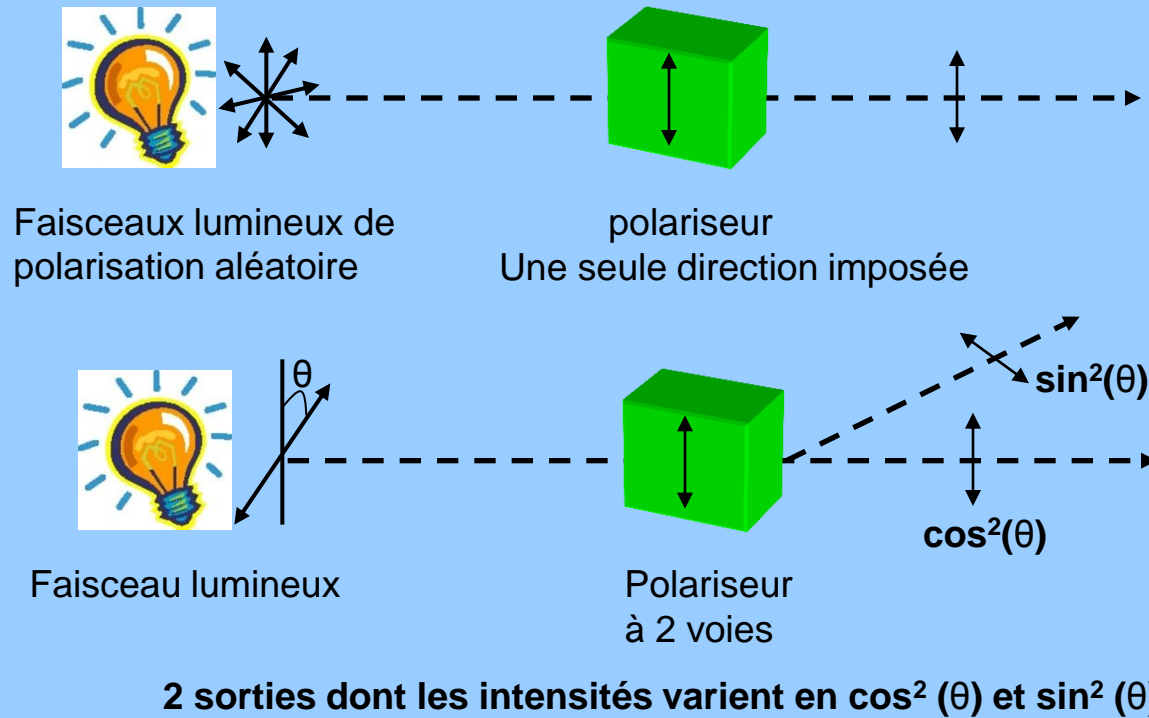
- **Albert Einstein (1926) : Particule**

- La lumière est considérée comme un ensemble de corpuscules appelées photons
 - Le photon est une particule immatérielle et sans masse
 - Energie d'un photo : $E=h \cdot \nu=h \cdot c/\lambda$
 - h : constante de Planck ($h= 6,62 \times 10^{-34}$ J.s)
 - ν : fréquence de la lumière émise
 - λ : longueur d'onde



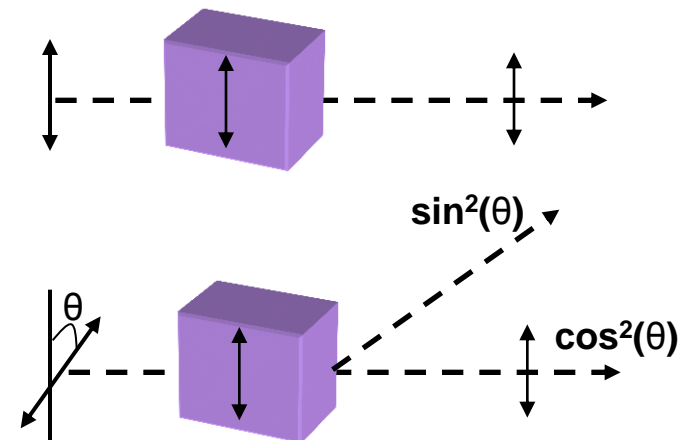
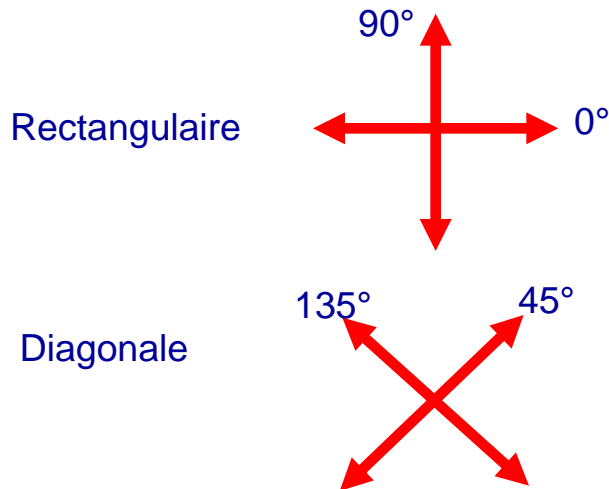
- Polarisation de la lumière

- Polarisation : direction de vibration transverse à la propagation (imposée par un polariseur)



Cryptographie quantique

- Photon
 - grain d'énergie lumineuse $E = h.v \approx 2.10^{-19} \text{ J}$
 - photon polarisé : on impose une direction à son champ électrique
 - État de polarisation d'un seul photon ?
 - Un photon ne peut pas être partagé (un *grain*)
 - Polarisation rectangulaire (0° ou 90°) ou diagonale (45° ou 135°)
- Propriétés quantiques d'un photon polarisé
 - Un photon peut être polarisé selon un axe quelconque
 - Un photon polarisé selon un axe d'angle ' α ' passant dans un filtre polarisant d'axe ' β ' possède une chance égale à $\cos^2(\beta - \alpha)$ de passer le filtre polarisant
 - Même phase ($\alpha = \beta$), $\cos^2(0) = 1 \Rightarrow$ le photon passe
 - Différence de phase $\beta - \alpha = 90$, $\cos^2(90) = 0 \Rightarrow$ le photon ne passe pas
 - Différence de phase $\beta - \alpha = 45$ ou 135 , $\cos^2(45) = 1/2$, une probabilité de 50 % que le photon passe



Utilisation de la cryptographie quantique

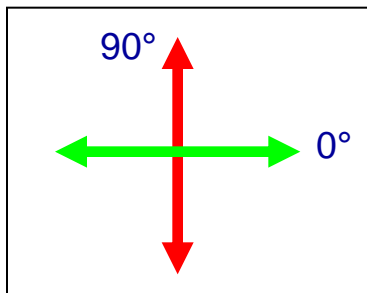
- **Distribution quantique de clefs (QKD)**
 - Pourquoi QKD ?
 - Pour échanger des clefs secrètes et
 - éviter toute écoute clandestine
 - Quels sont les acteurs ? Grands systèmes, grands réseaux bancaires, gouvernements,..
 - Quels sont les équipements utilisés ?
 - Source de photons, détecteurs, dispositifs de modulation
 - Commutateurs optiques contrôlés par des logiciels spécifiques
 - Comment protège-t-on le canal ? toute tentative d'interception sera détecté parce que quand le nombre de photons interceptés augmente, l'erreur augmente



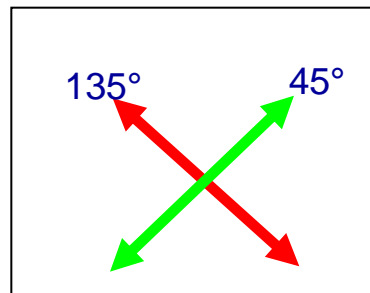
Cryptographie quantique

– Protocole BB84

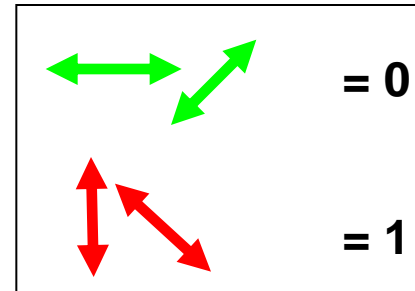
- Proposé par Charles Bennet et Gilles Brassard en 1984
- Protocole quantique de distribution de clé secrètes basé sur le principe d'Heisenberg
- Pour présenter un bit d'information 0 ou 1, QKD BB84 utilise un *photon polarisé*
- Les états de polarisation de photon appartiennent à deux bases conjuguées
 - Base rectangulaire : $\{0: |H, \pi/2: |V\}$, H : Horizontal, V : Vertical
 - Base diagonale : $\{\pi/4: |A, 3\pi/4: |D \}$, A : anti-diagonal, D : diagonal



Base rectangulaire

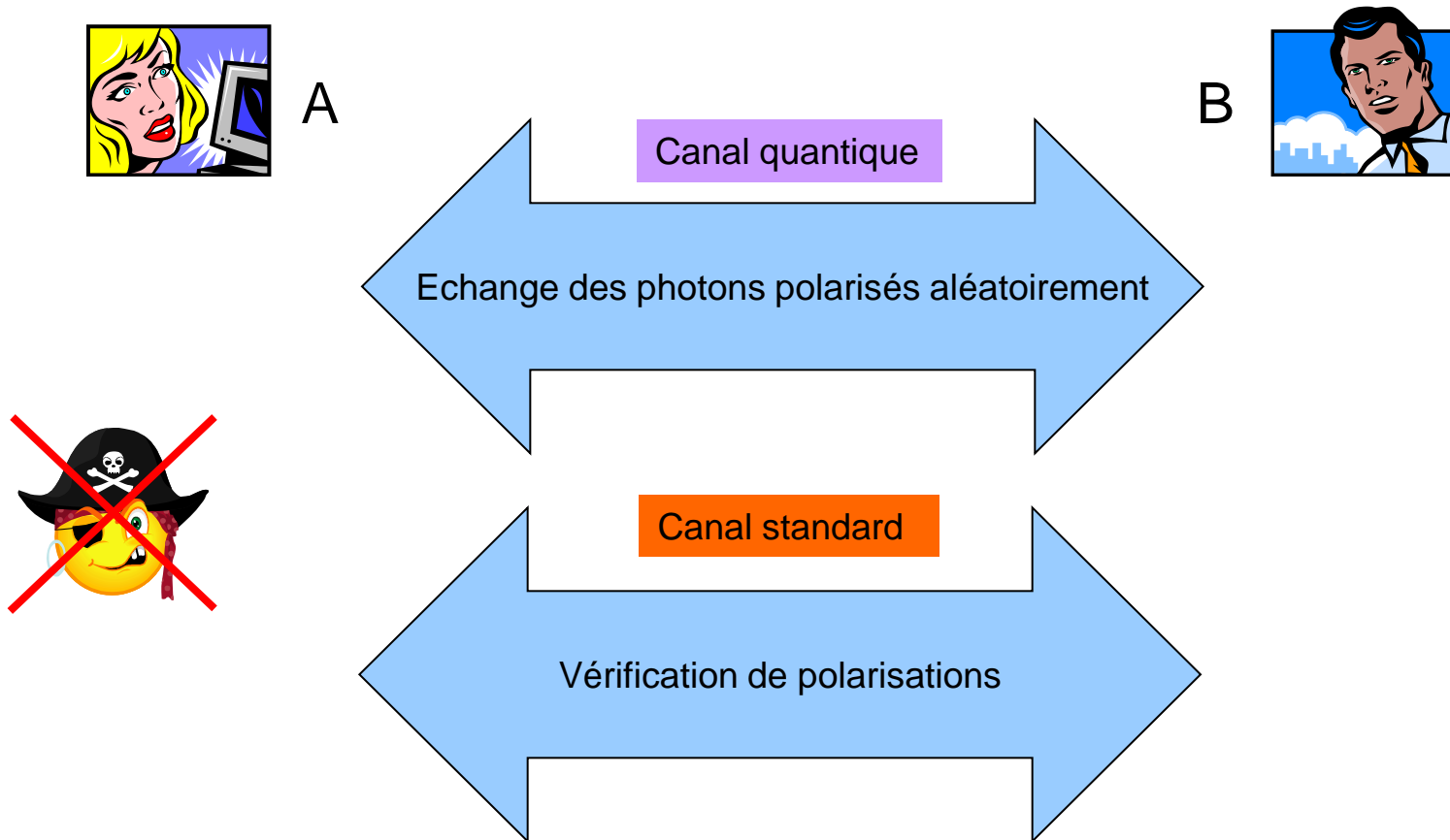


Base diagonale



<= Convention

Cryptographie quantique



clef parfaitement sûre : aléatoire, utilisée une seule fois, lois quantiques

Protocole BB84

- Etape 1 du protocole :



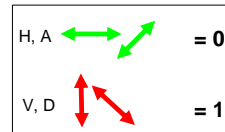
Alice

Alice génère et envoie à Bob une suite de photons polarisés dont la polarisation est aléatoirement choisie



Bob

Transmission quantique															
Bits aléatoires d'Alice	0	1	1	0	1	1	0	0	1	0	1	1	0	0	1
Bases aléatoires d'Alice															
L'état de Photon	A	V	D	H	V	V	H	H	D	A	V	D	A	A	V
Les bases Aléatoires de Bob															
Les bits interprétés par Bob	1	-	1	-	1	0	0	0	-	1	1	1	-	0	1



Protocole BB84

- Etape 2 du protocole














Alice

Alice génère et envoie à Bob une suite de photons polarisés dont la polarisation est aléatoirement choisie



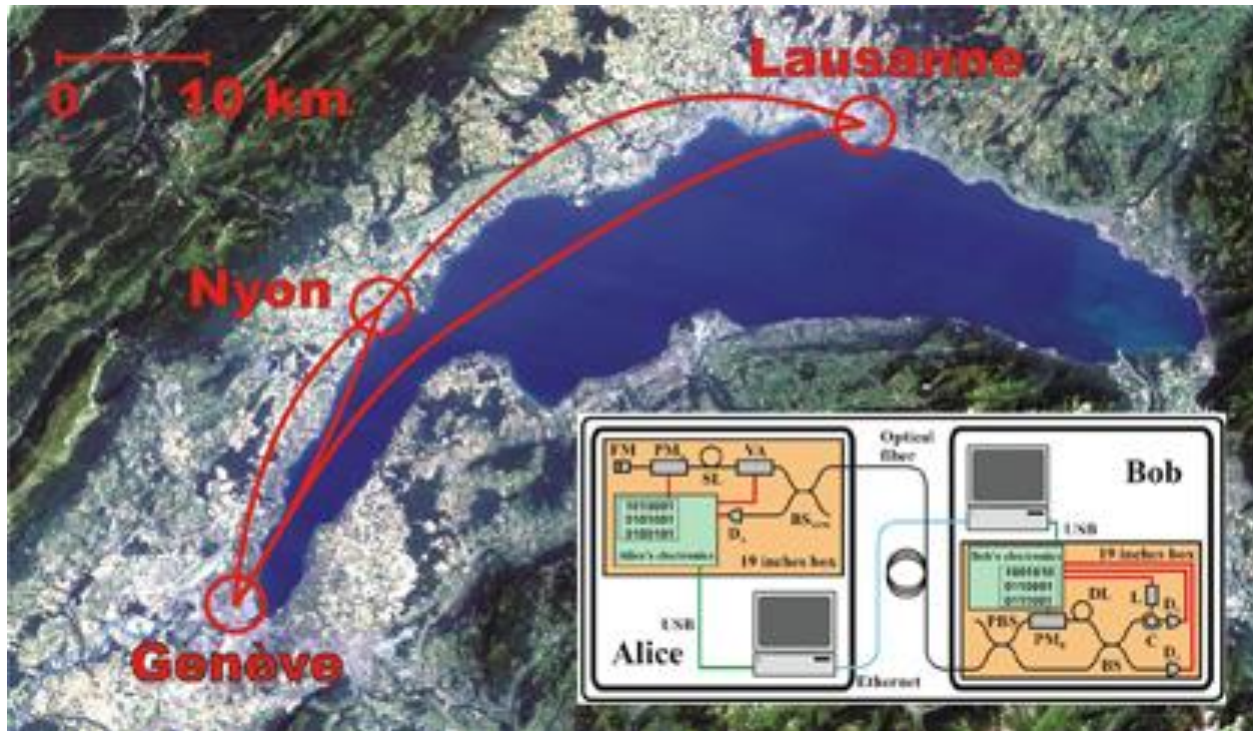
Bob

Transmission par canal classique															
Bits aléatoires d'Alice	0	1	1	0	1	1	0	0	1	0	1	1	0	0	1
Bases aléatoires de Bob															
Les bits interprétés par Bob	1	-	1	-	1	0	0	0	-	1	1	1	-	0	1
Confirmation d'Alice			✓		✓			✓				✓		✓	✓

clef parfaitement sûre : 110101

Applications de la cryptographie quantique

- Distribution quantique de clefs à l'université de Genève



Distance : 67 km débits

- 2007 : première expérience “commerciale” eut lieu à Genève lors des élections fédérales

Applications de la cryptographie quantique

- **Projet européen : SECOQC**
 - Development of a Global Network for **Secure CO**mmunication based on **Q**uantum **C**ryptography
 - Regroupe les meilleurs spécialistes européens en QKD
 - Nouveaux équipements QKD
 - Implémentation complète à Vienne
- **www.secoqc.net**



Conclusion

- Cryptographie quantique
 - Systèmes de distribution quantique de clef fiables et déployables sur des réseaux télécoms
 - Technologie émergente
 - Concepts parfaitement connus
 - Difficultés technologiques à la mettre en œuvre
 - Coût élevé
 - Technologie existe sur le marché (lignes sécurisées sur des distances allant jusqu'au dizaines de km)



Système QKD de la compagnie suisse :IdQuantique



Système QKD de Toshiba