Plan

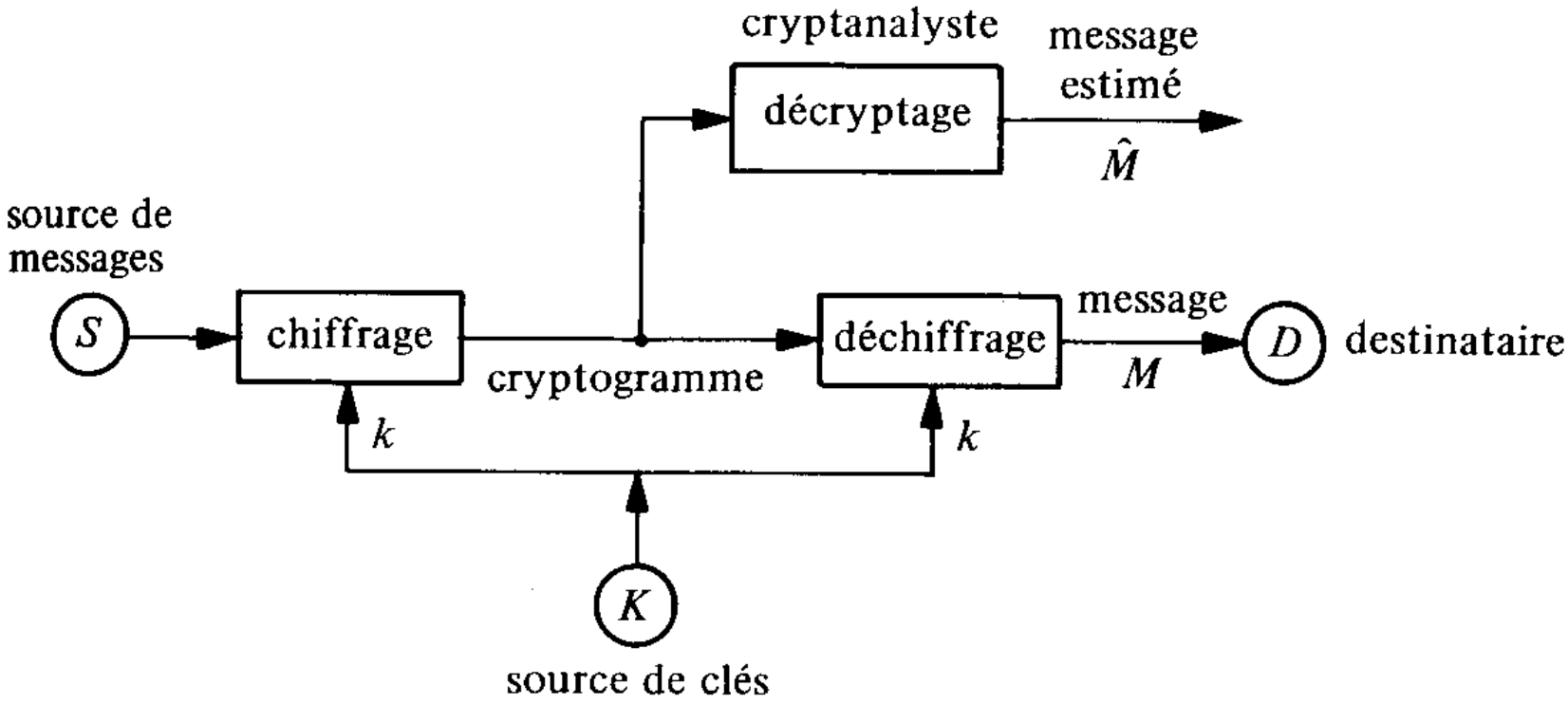
- 1. Introduction
- 2. Sources discrètes & Entropie
- 3. Canaux discrets & Capacité
- 4. Codage de source
- 5. Codage de canal
- 6. Cryptographie
- 7. Conclusion

6. Cryptographie

- **Objectifs**
  - ✓ Garantir la **confidentialité** des données
  - ✓ Garantir l'**intégrité** des données
  - ✓ Garantir l'**identité** des correspondants
    - ⇨ Non répudiation des transactions

- **Applications**
  - ✓Militaires
  - ✓Mots de passe
  - ✓Sécurité réseaux
  - ✓Téléphonie
  - ✓Commerce électronique
  - ✓@Business

- **Vocabulaire**

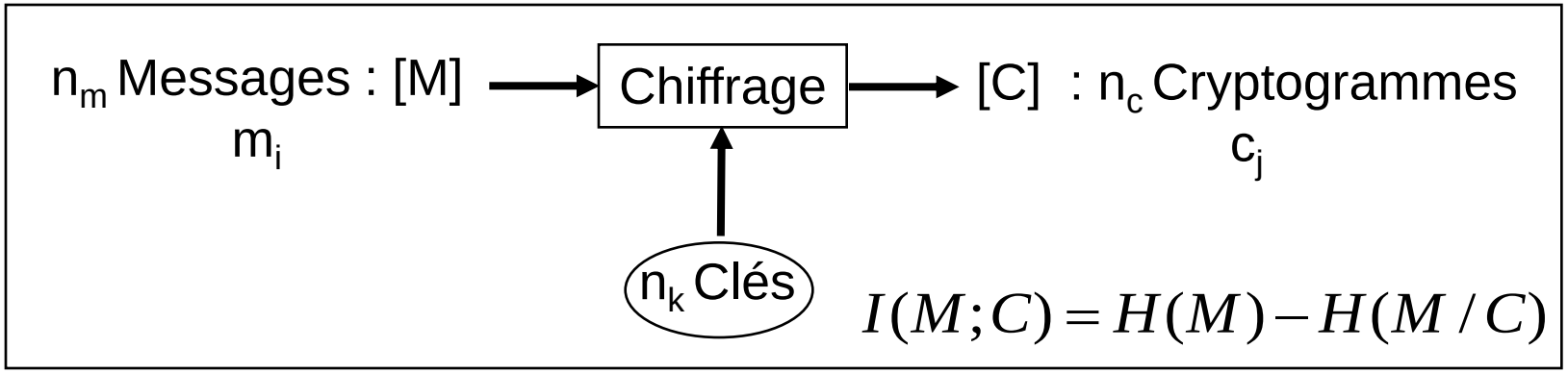


✓**Cryptographie** : techniques de chiffrage

✓**Cryptologie** : cryptographie & cryptanalyse

- **Vue de la théorie de l'information**

  ↳ **Chiffrage = Canal très perturbé**



✓Secret parfait ssi : $H(M/C) = H(M)$ soit $I(M;C) = 0$

- Clé unique permet m_i ⇨ c_j soit $n_m = n_c = n_k$
- Toutes les clés sont équiprobables

Chiffrage efficace

ssi

(Coût + temps) de décryptage >> Valeur de l'info

- **Les grandes approches**

  - ✓ **Approches classiques**

    - ✓**Chiffrage par substitution**
      Jules César, l'Abbé Trithème
    - ✓**Chiffrage par transposition**

  - ✓ **Approches modernes**

    - ✓**Chiffrage à clé privée (symétrique)**
      DES, IDEA,
    - ✓**Chiffrage à clé publique (asymétrique)**
      RSA, PGP

• Chiffrage par substitution

⇨ Chaque lettre (ou groupe de lettres) est remplacée par une lettre (ou un groupe de lettres)

• Abbé Trithème (1499)

Dans son royaume à perpétuité,
En Paradis à perpétuité,
Ainsi qu'en toute éternité;
Dans la gloire à perpétuité,
Mais dans son règne;
Sempiternel, toujours dans la félicité,
Tant dans la lumière que dans la béatitude,
Et toujours dans la gloire à perpétuité,
Mais dans son règne;
En une infinité encore à perpétuité,
Comme dans la gloire autant que dans les Cieux,
A tout jamais, oui ! à tout jamais à perpétuité;
Dans son royaume et dans la félicité,
Irrévocablement, dans son royaume,
Et sans cesse qu'il soit à perpétuité dans la lumière,
Et encore à perpétuité !

A = dans les cieux
B = à tout jamais
C = un monde sans fin
D = en une infinité
E = à perpétuité
F = sempiternel
G = durable
H = sans cesse
I-J = irrévocablement
K = éternellement
L = dans la gloire
M = dans la lumière
N = en paradis
O = toujours
P = dans la divinité
Q = dans la déité
R = dans la félicité
S = dans son règne
T = dans son royaume
U-V-W = dans la béatitude
X = dans la magnificience
Y = au trône
Z = en toute éternité

- **Chiffrage par transposition**

  ⇨Change l'ordre des lettres sans les substituer

- Exemple

B	R	I	Q	U	E	S
1	5	3	4	7	2	6
t	r	a	n	s	f	é
r	e	z	u	n	m	i
l	l	i	a	r	d	d
e	f	r	a	n	c	s
à	m	o	n	c	o	m
p	t	e	s	u	i	s
s	e	n	u	m	é	r
o	t	é	z	é	r	o
z	é	r	o	s	e	p
t	a	b	c	d	e	f

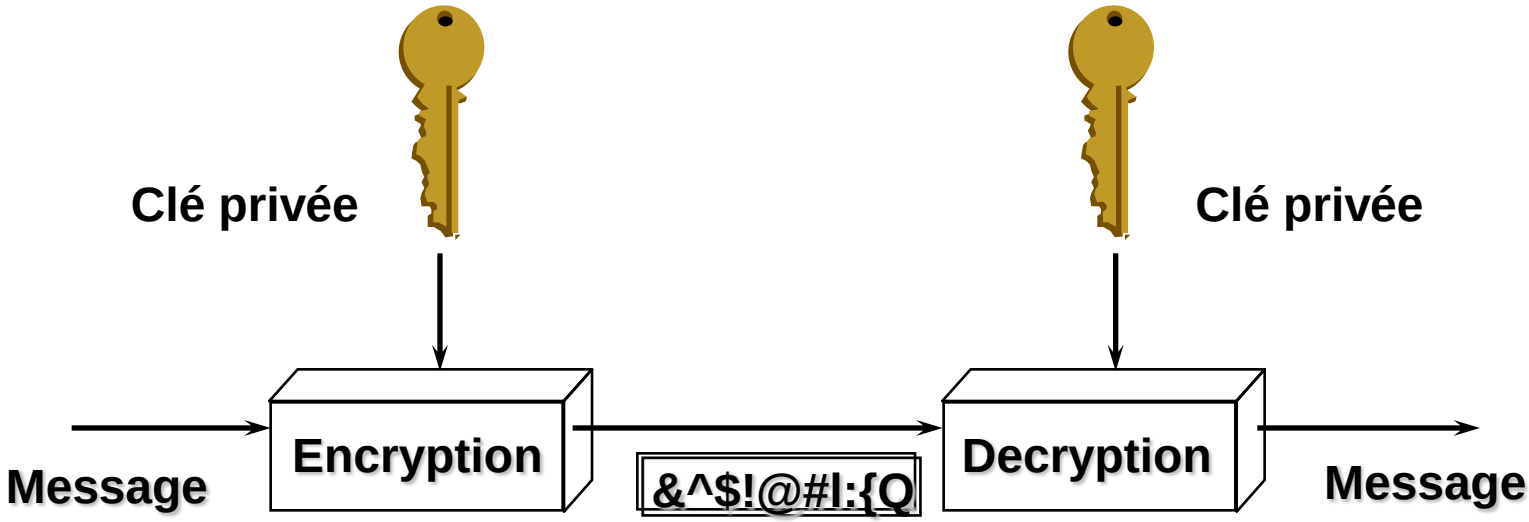
texte en clair

tranférezunmilliarddefrancsàmon
comptesuissenumérotézérozérosept

texte chiffré

TRLEAPSOZTFMDCOIEREEAZIROENERB
NUAANSUZOCRELFMTETEAEIDSMSROPF
SNRNCUMESD

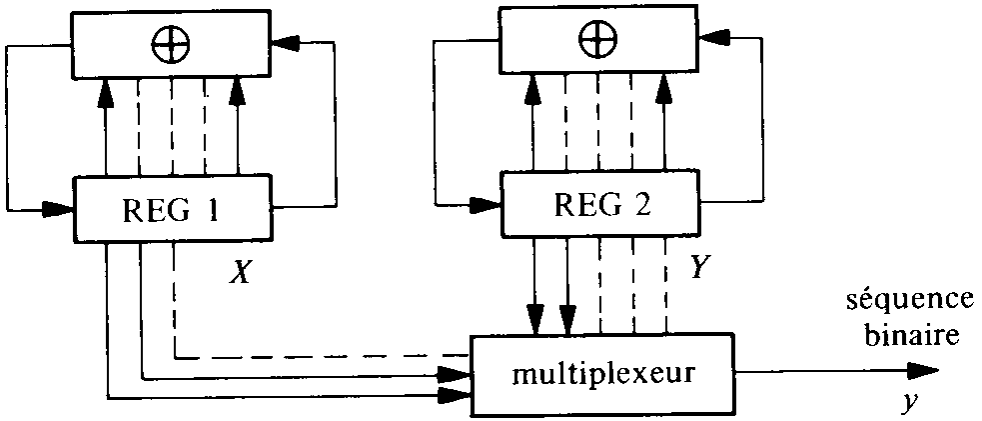
• Chiffrage à clé privée



- ✓ Encryption and decryption use same key
- ✓ Encryption and decryption use same mathematical function
- ✓ Fast
- ✓ Example: Data Encryption Standard (DES, IDEA ,RC2, ...)

• Challenges with symmetric encryption

- ✓ Key length matters
- ✓ Keys must often be changed
- ✓ Shared keys must be generated and distributed securely
  - Ramdomized Key generator

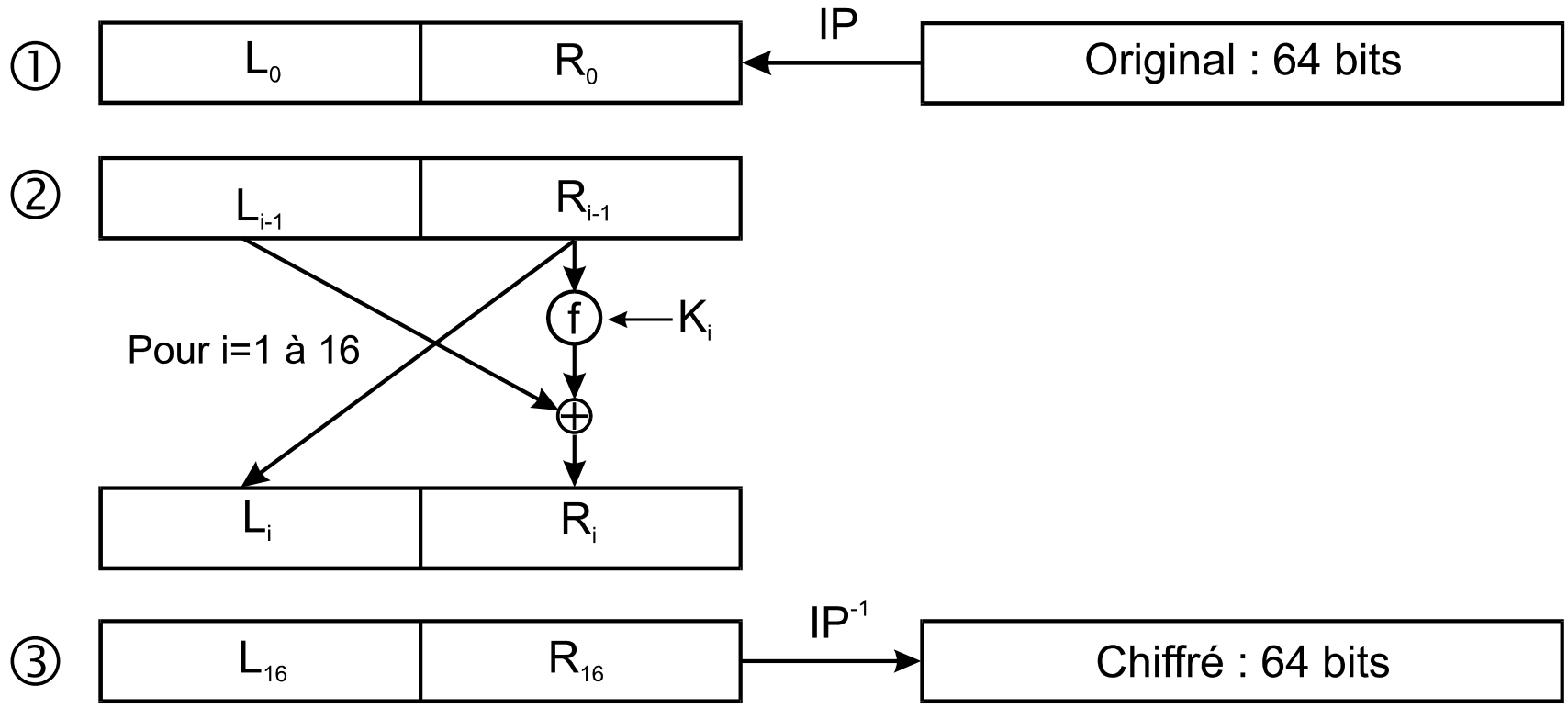


- **DES (Data Encryption Standard / IBM 1977)**

⇨ Un ensemble de permutations / substitutions

- Mot de 64 bits
- Clé de 56 bits
- 16 rondes

✓Principe



- **DES (Data Encryption Standard / IBM 1977)**

IP

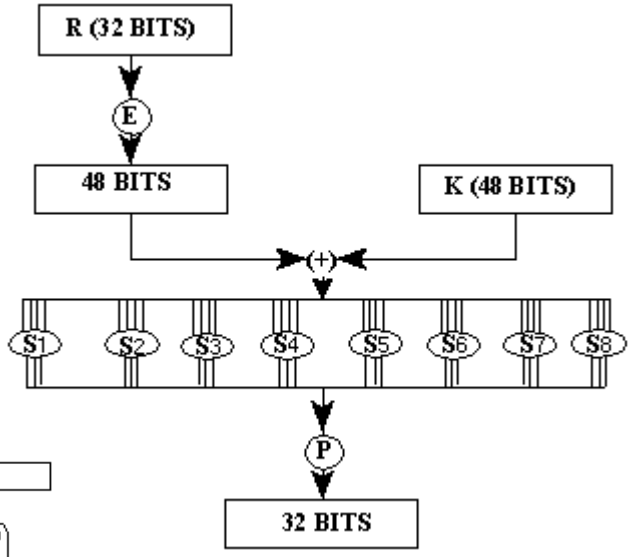
58 50 42 34 26 18 10 2
60 52 44 36 28 20 12 4
62 54 46 38 30 22 14 6
64 56 48 40 32 24 16 8
57 49 41 33 25 17 9 1
59 51 43 35 27 19 11 3
61 53 45 37 29 21 13 5
63 55 47 39 31 23 15 7

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

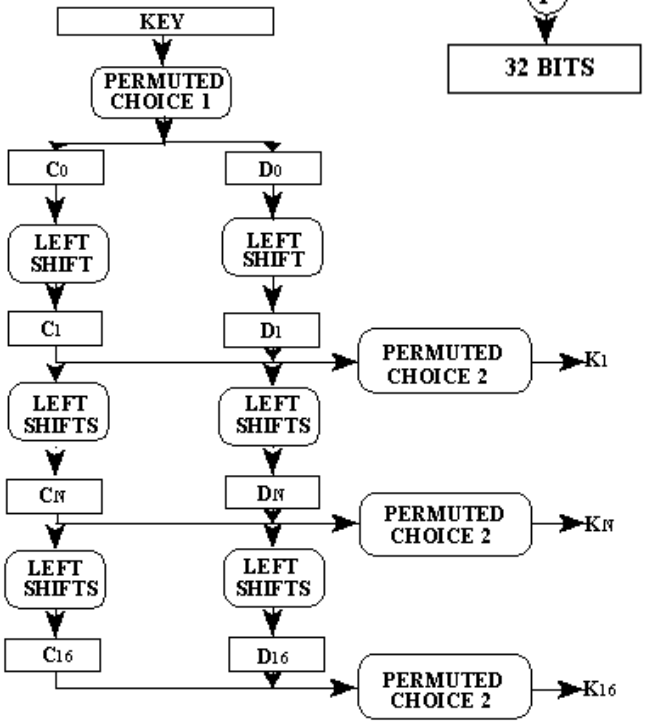
✓Fonction *f*

- Extension à 48 bits (E)
- Xor avec clé secondaire (K_i)
- Réduction (S_j)
- Permutation (PI)



✓Génération des clés secondaires

- Permutation (PC1)
- Décalage (LS)
- Réduction (PC2)



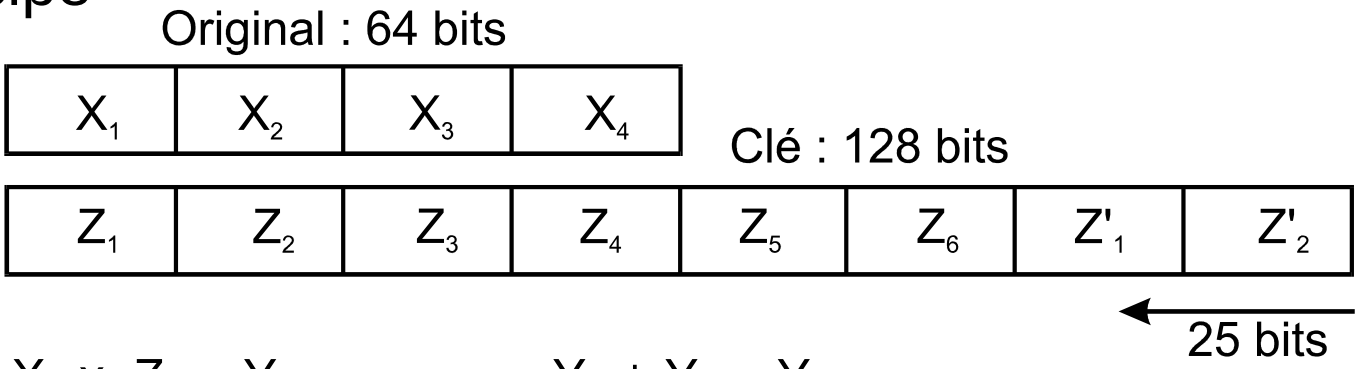
💣 La **clé** à échanger est à garder **secrète**

- **IDEA (International Data Encryption Algorithm / *Lai, Massey* 1991)**

⇨ Une succession d'addition (**+**) , multiplication (**x**), et Xor (⊕)

- Mot de 64 bits
- Clé de 128 bits
- 8 rondes

✓Principe



- $X_1 \times Z_1 = Y_1$
- $X_2 + Z_2 = Y_2$
- $X_3 + Z_3 = Y_3$
- $X_4 \times Z_4 = Y_4$
- $Y_1 \oplus Y_3 = Y_5$
- $Y_2 \oplus Y_4 = Y_6$
- $Y_2 \times Z_5 = Y_7$

⇨

- $Y_6 + Y_7 = Y_8$
- $Y_8 \times Z_6 = Y_9$
- $Y_7 + Y_9 = Y_{10}$
- $Y_1 \oplus Y_9 = X_1'$
- $Y_3 \oplus Y_9 = X_3'$
- $Y_2 \oplus Y_{10} = X_2'$
- $Y_4 \oplus Y_{10} = X_4'$

- $X_1 \times Z_1 = X_1'$
- $X_2 + Z_2 = X_2'$
- $X_3 + Z_3 = X_3'$
- $X_4 \times Z_4 = X_4'$

- **DES / IDEA**

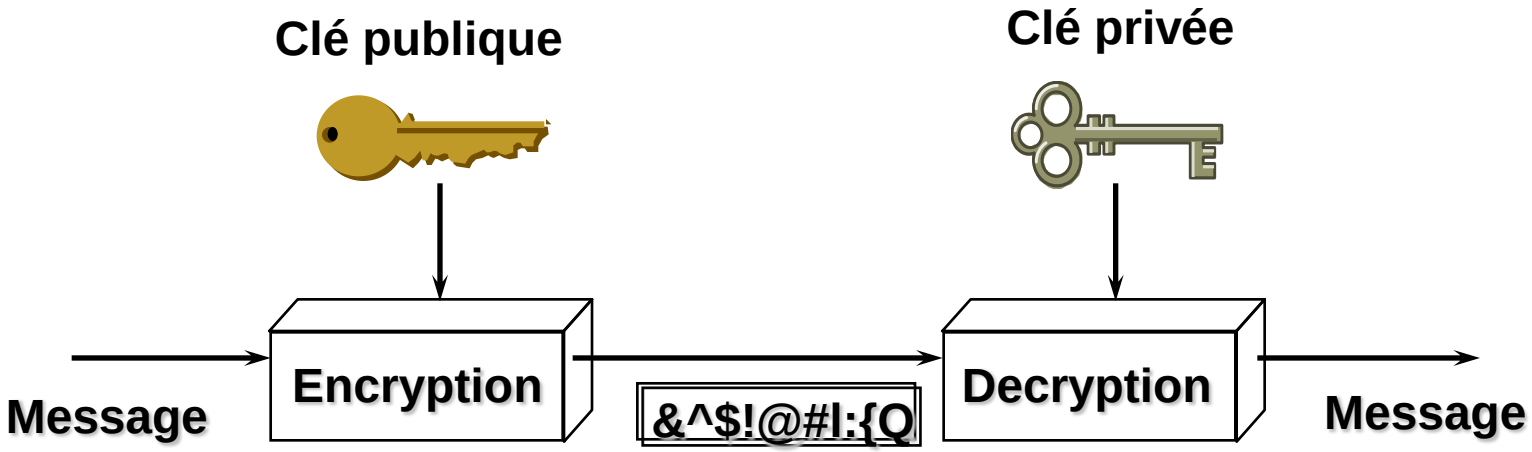
	Taille des blocs	Taille de clé	Nombre de rondes
DES	64	56	16
IDEA	64	128	8

✓ IDEA est deux fois plus rapide !

✓ Chip VLSI IDEA ⇨ 200 Mb/s

✓ IDEA le remplaçant de DES

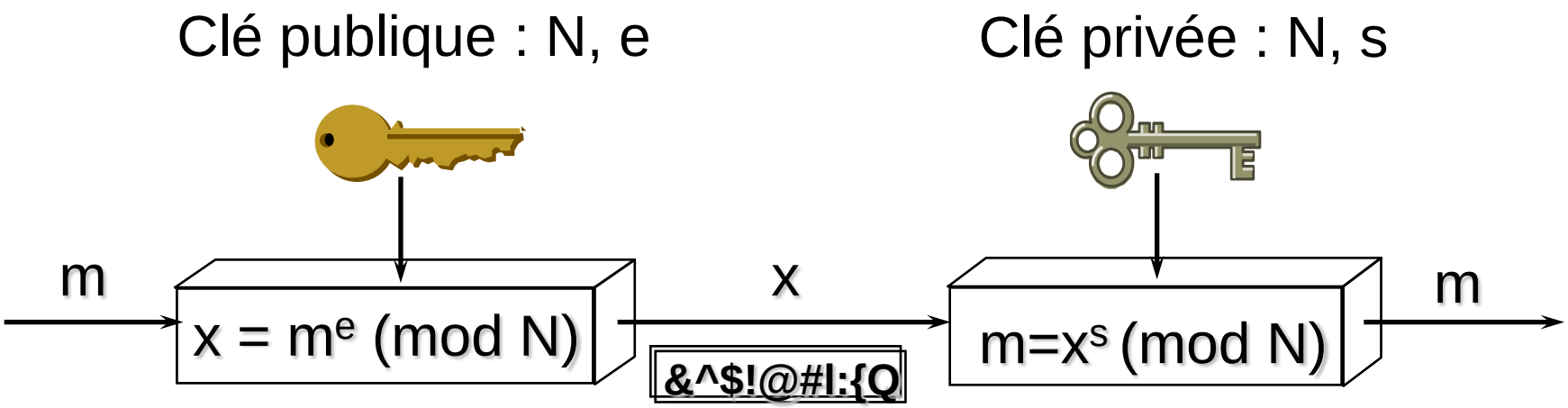
• Chiffrage à clé publique



- ✓ Encryptor and decryptor use different keys
- ✓ Encryptor and decryptor use different mathematical functions
- ✓ Slow
- ✓ Example: public key algorithms (RSA, Diffie-Hellman, ...)

- **RSA (Rivest Shamir Adleman / 1978)**

⇨ Basé sur des propriétés algébriques : - multiplication ☺
- factorisation ☹



- Choisir N = p . q avec p et q premiers (512 bits soit # 200 chiffres)
- Choisir s / s premier avec z=(p-1) .(q-1)
- e / e. s = 1 (mod z) e<<s

💣 Sécurité dépend des connaissances arithmétiques !

✓Exemple simple de RSA

- p=3 et q=11 ⇨ N = 33 ⇨ z = 20
- s = 7 ⇨ 7.e = 1 (mod 20) ⇨ e = 3
- $C = M^3 . \pmod{33}$ et $M = C^7 . \pmod{33}$

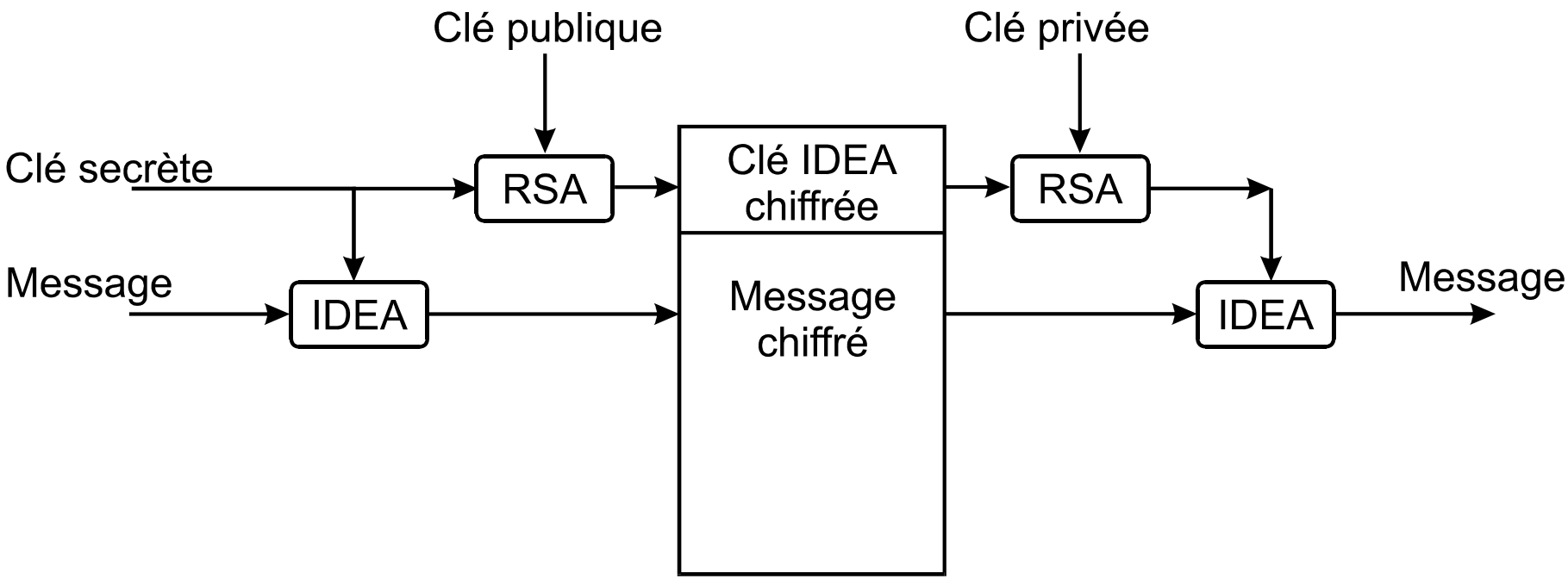
Texte en clair (M)		Texte chiffré (C)			Après déchiffrage	
Carac-tère	Valeur	P^3	$P^3 \pmod{33}$	C^7	$C^7 \pmod{33}$	Carac-tère
S	19	6859	28	13492928512	19	S
U	21	9261	21	1801088541	21	U
Z	26	17576	20	1280000000	26	Z
A	01	1	1	1	1	A
N	14	2744	5	78125	14	N
N	14	2744	5	78125	14	N
E	05	125	26	8031810176	5	E

Calculs de l'émetteur

Calculs du récepteur

- **PGP (Pretty Good Privacy / 1991)**

  ⇨ Algorithme hybride : PGP = (RSA + IDEA)



💣 Interdit en France ! (jusqu'en 1999)

- **Comparaison**

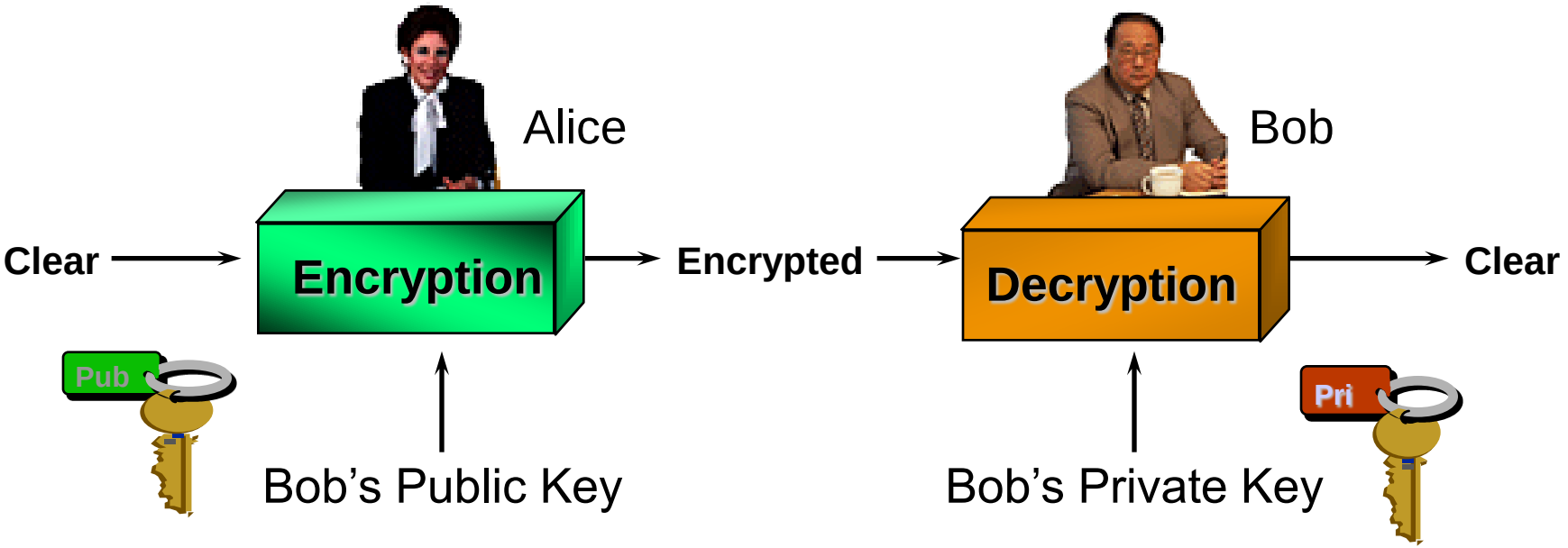
	Symmetric	Asymmetric
Number of keys	1	2
Usual key length	56 bits	512+ bits
Performance	fast	very slow
Dedicated hardware	yes	very rare
Code breaking	difficult	almost impossible

Nombre de personnes	Nombre de clés secrètes	Nombre total de clés privées ET publiques
2	1	4
3	3	6
4	6	8
5	10	10
6	15	12
7	21	14
8	28	16
9	36	18
10	45	20
15	105	30
20	190	40
50	1 225	100
100	4 950	200
500	124 750	1000
1 000	499 500	2000
10 000	49 995 000	20 000
n	n(n-1)/2	2n

✓ Usage des approches clé publique

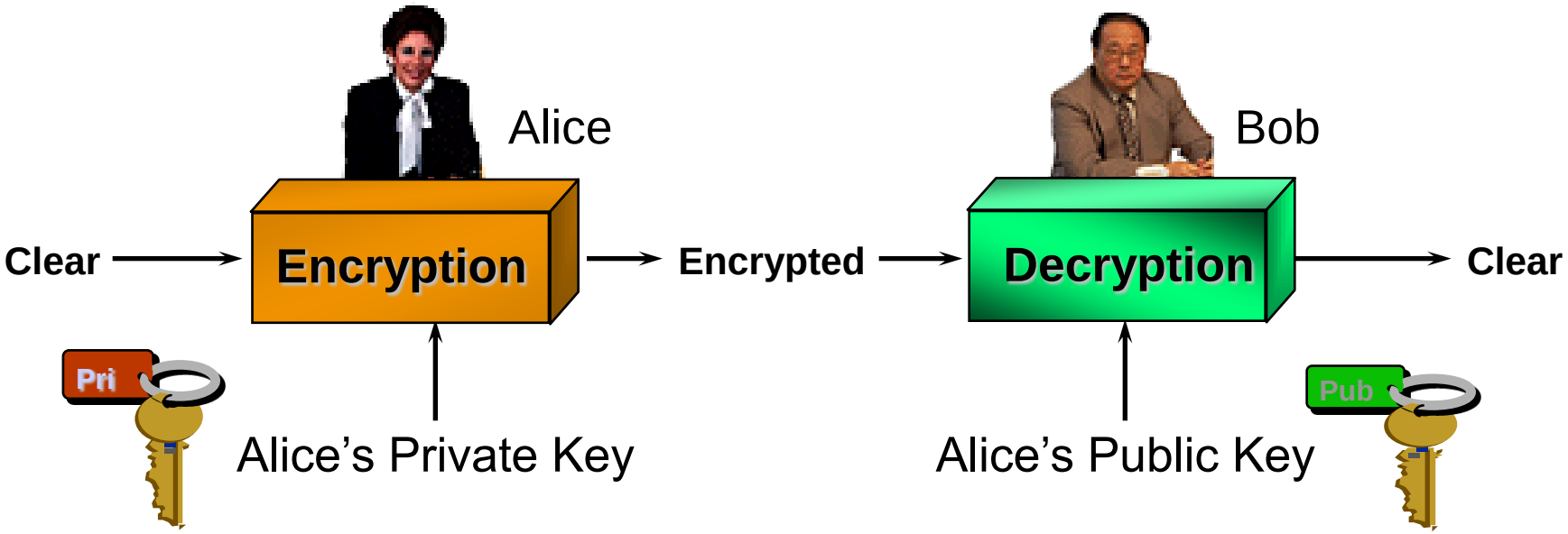
- **Confidentialité**
- **Authentification**
- **Confidentialité & authentification**
- **Signature**
- **Certificat**
- **Échanges sécurisés**

• Confidentialité



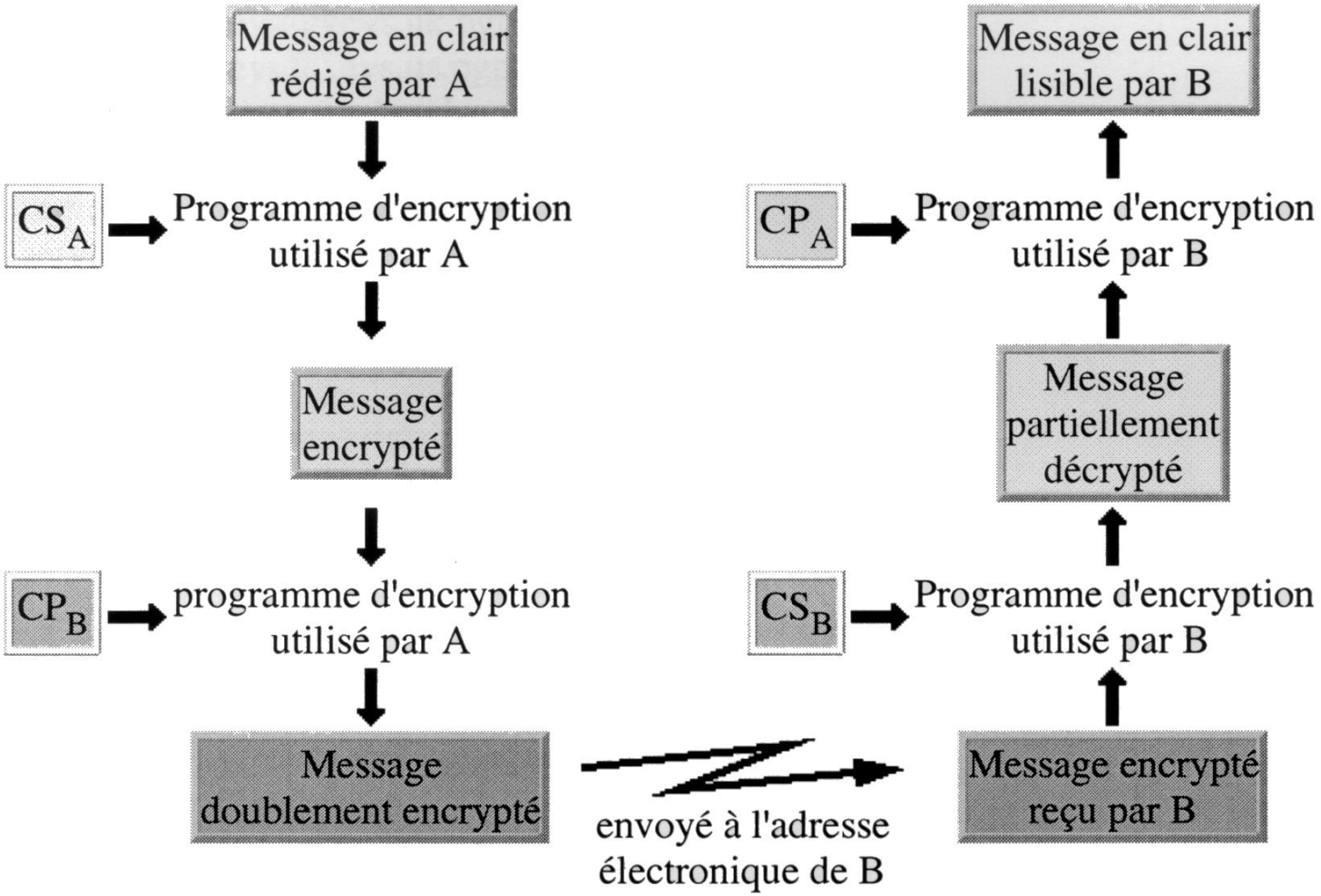
- Alice gets Bob's public key
- Alice encrypts message with Bob's public key
- Bob decrypts using his private key

• Authentification



- Alice encrypts message with her private key
- Bob gets Alice's public key
- Bob decrypts using Alice's public key

• Confidentialité & Authentification



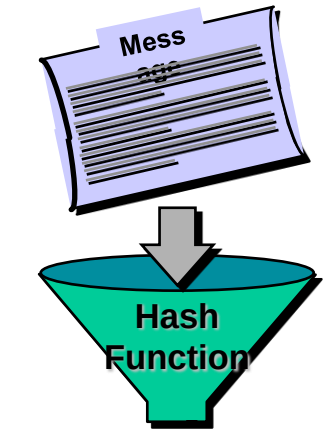
- **Signature : Authentification & Intégrité**

  ✓ **DSS**

  - *Digital Signature Standard* from NIST
  - Public and private keys (512+ bits)
  - Applied on a *digest* of the message to be signed

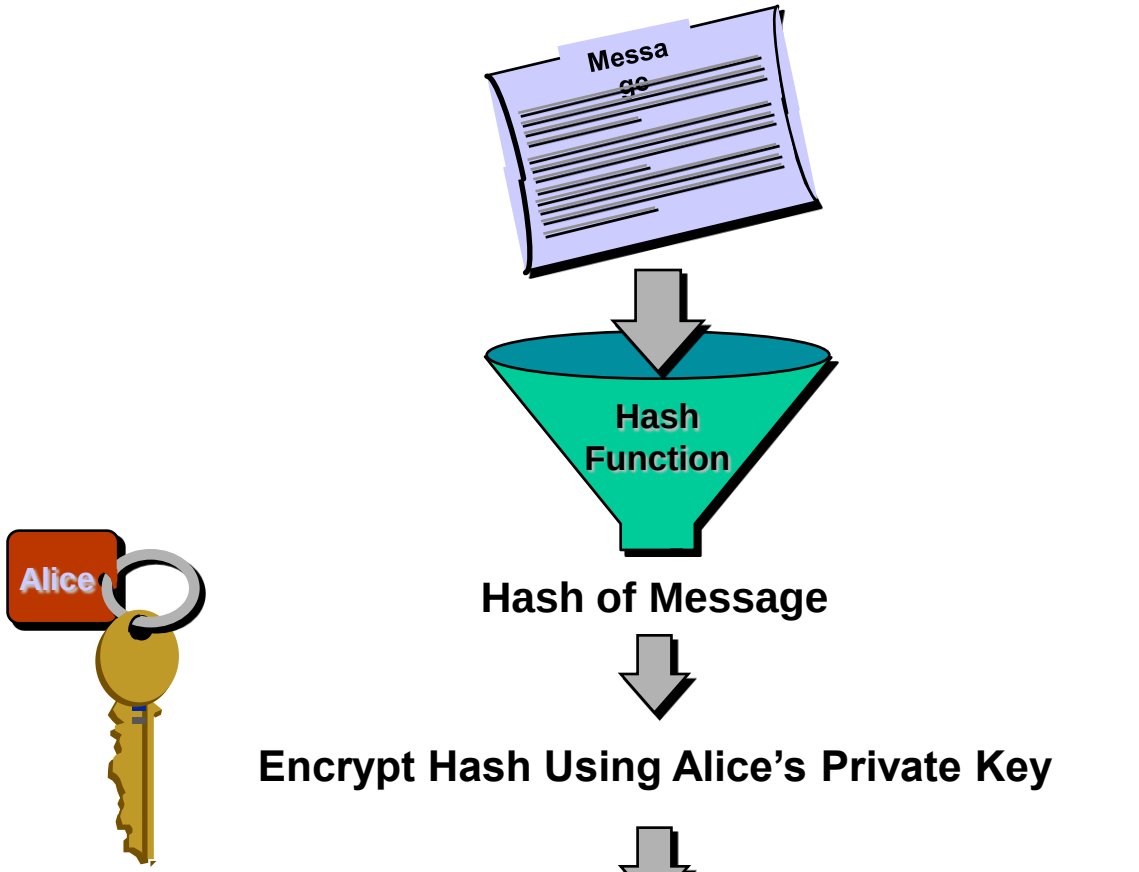
  ✓ **Digest (Hash)**

  - one-way cryptographic function
  - maps a large message into a short hash
  - typical hash size 128 bits
  - examples: MD5, SHA

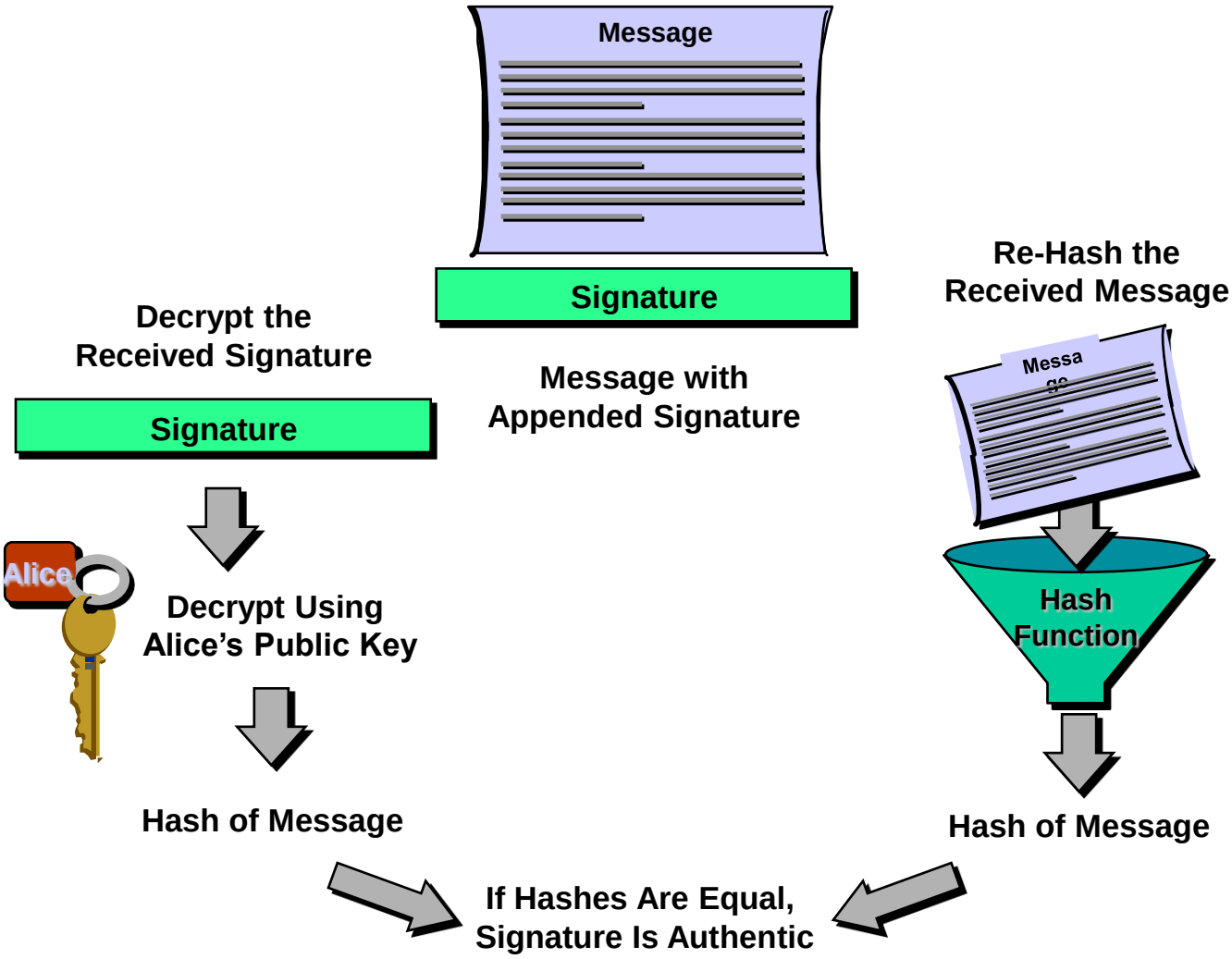


Hash of Message

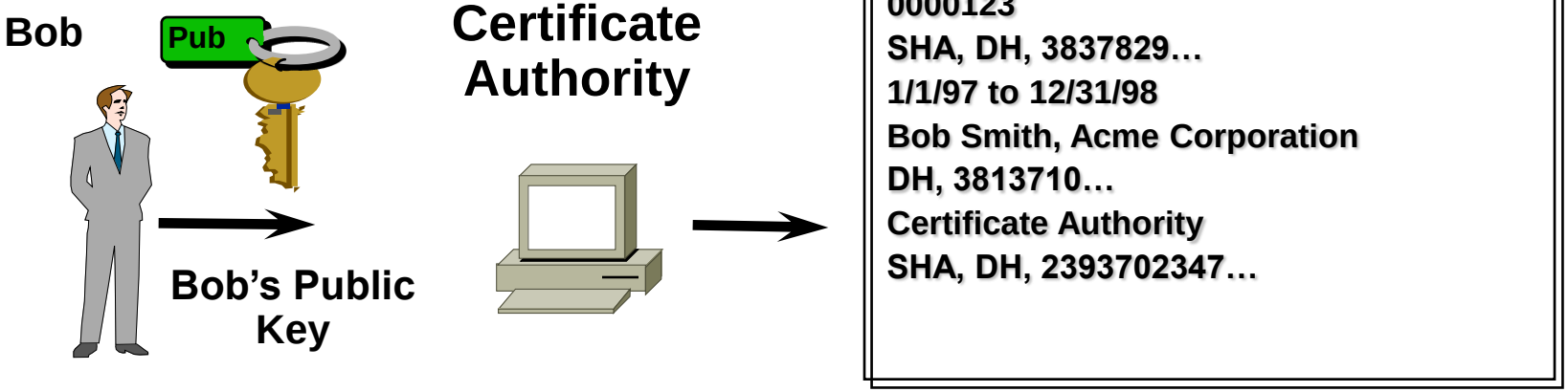
- **How does Alice sign her message?**



- **How does Bob verify Alice's signature?**



- **How can Bob be assured that the Alice's public key belongs to Alice?**



- **Digital certificate** is signed message that attests to authenticity of user's public key

• Certificat : l'identité électronique

- A digital certificate contains
  - Serial number of the certificate
  - Issuer algorithm information
  - Valid to/from date
  - User public key information
  - Signature of issuing authority

0000123
SHA,DH, 3837829....
1/1/93 to 12/31/98
Alice Smith, Acme Corp
DH, 3813710...
Acme Corporation, Security Dept.
SHA,DH, 2393702347 ...

- Tiers de confiance / sequestre
- Norme CCITT **X. 509**

- **Protocoles réseaux sécurisés**

  - ✓ **SSL (Secure Socket Layer)**
  - ✓ **SET (Secure Electronic Transaction)**
  - ✓ **Secure HTTP**
  - ✓ **Secure TCP/IP ⇨ IP v.6**
  - ✓ **...**

- **S S L**

  - ✓ **Communication sécurisée entre deux entités**

  - ✓ **Protocole de handshake**
    - Client vérifie le certificat du serveur
    - Client génère paire de clé
    - Demande la clé publique du serveur
    - Envoie de la clé publique du client chiffrée au serveur
    - Test émis par le serveur

  - ✓ **Échange de données sur liaison sécurisée**

⇨ Commerce électronique

• Commerce électronique

✓ Evolution exponentielle, initiée par les professionnels, tirée par les particuliers

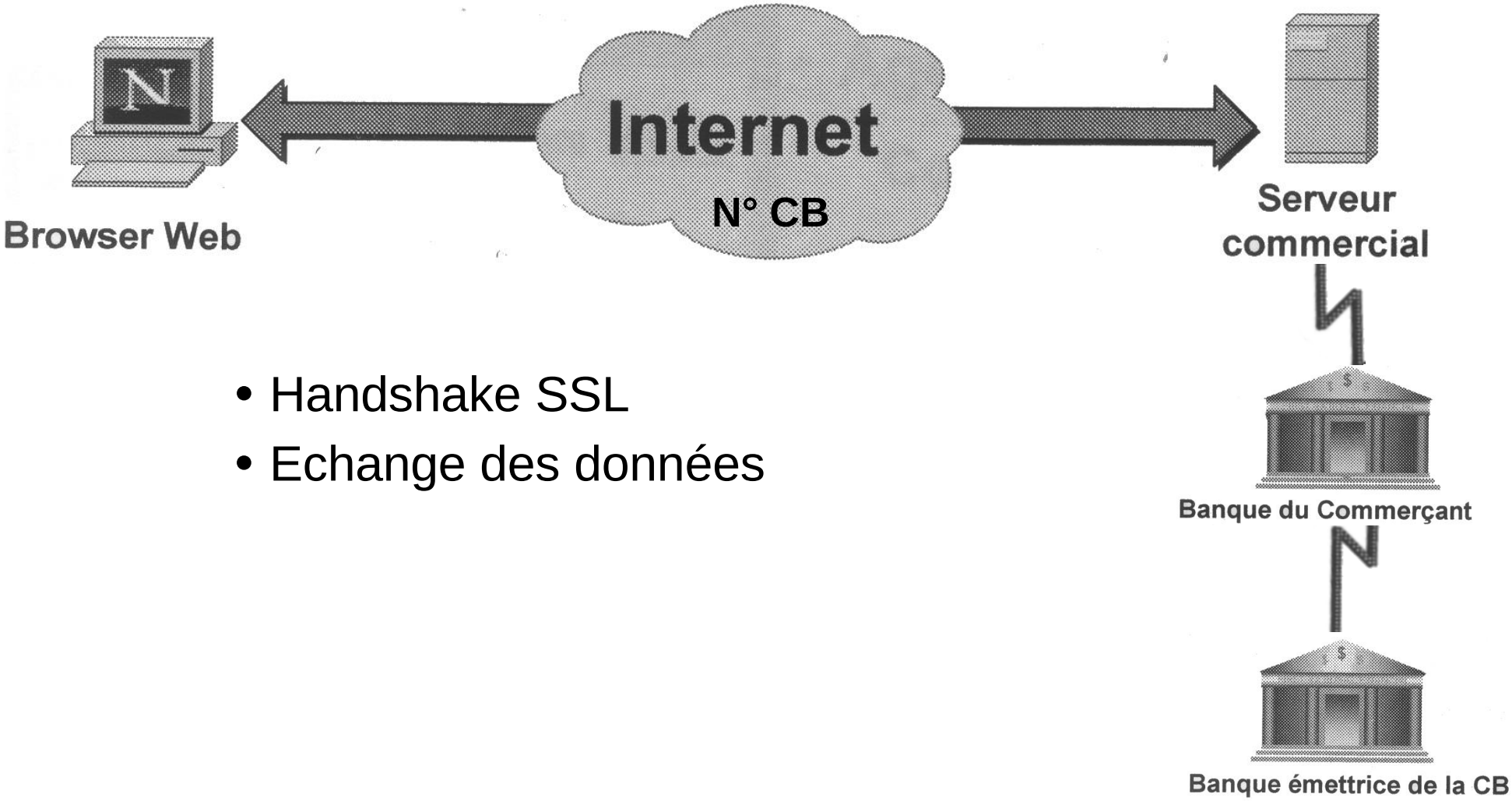
✓ Pose tous les problèmes traités par la cryptologie

- Authentification
- Intégrité
- Confidentialité
- Non répudiation

✓ 2 voies principales

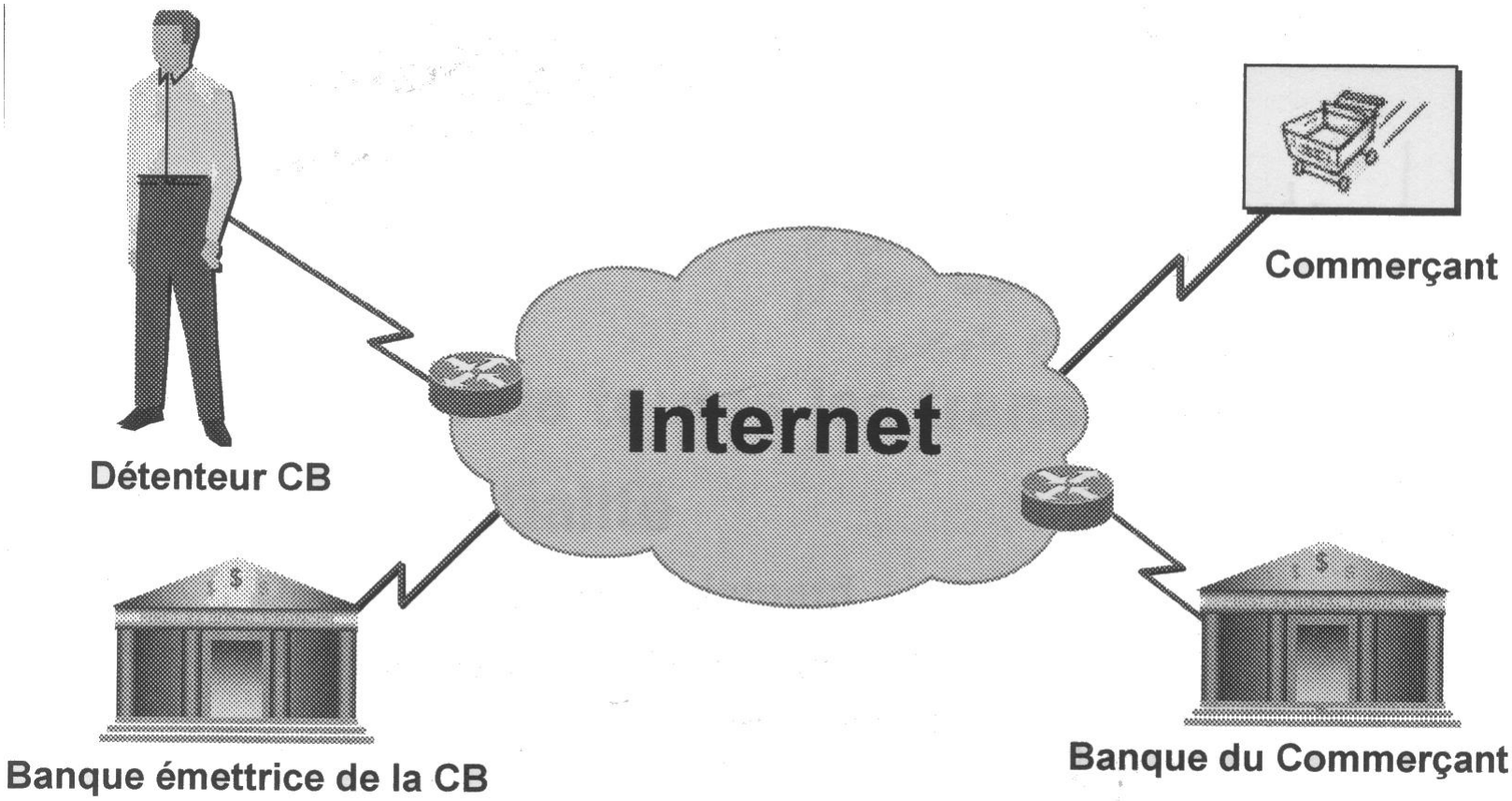
- Acheteur / Vendeur ⇨ SSL
- Acheteur / Vendeur + Banques ⇨ SET

✓ Commerce Acheteur / Vendeur via SSL



- Handshake SSL
- Echange des données

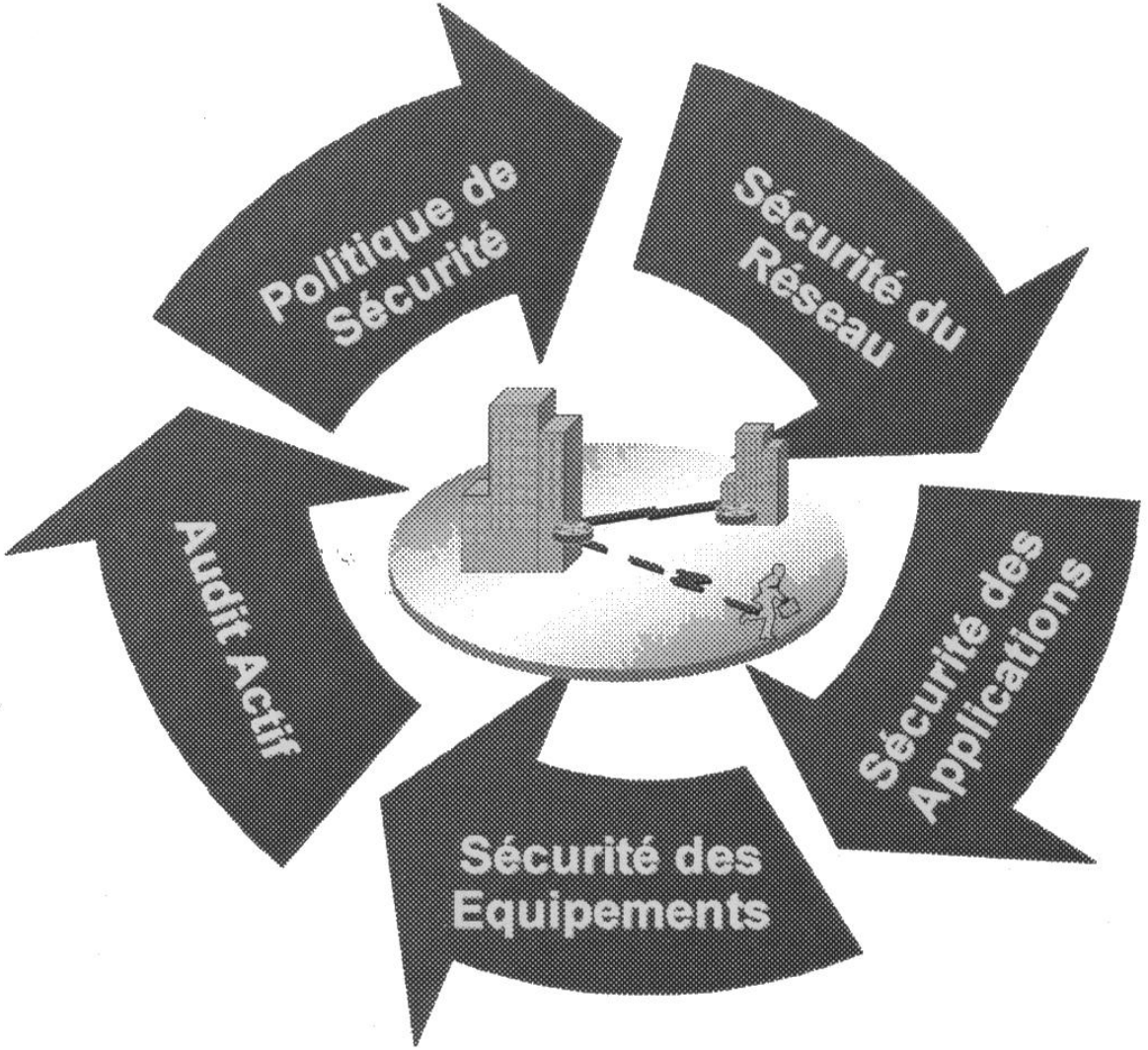
✓Secure Electronic Transaction (SET)



- ✓ SET prend en charge
  - Authentification acheteur & Vendeur
  - Intégrité des transmissions
  - Confidentialité du paiement et de la commande

- ✓ Déroulement d'une vente SET
  - Demande de l'acheteur
  - Vendeur vérifie la commande
  - Les banques vérifient Vendeur & Acheteur
  - Acquittement de l'ordre

Cryptologie = élément essentiel du cycle de sécurité



- **Législation & Cryptologie**

Pas de législation internationale + évolution rapide

⇨ Difficulté de standardisation des protocoles

(projets de loi UE en cours)

💣 Les logiciels de chiffrage ne sont pas comme les autres !

✓USA

- Cryptologie, armes et munitions ⇨ Même cadre juridique
- ITAR (International Traffic Arm Regulation) ⇨ Export (40 bits)

✓France

Old...

- Législation très restrictive mais évolutive
- SCSSI (Service Central de Sécurité des Sys. Informations) ⇨ Organisme d'état

- Décrets 98-206 & 207 du 23 Mars 1998
  - Autorisation ⇨ Déclaration ⇨ Sans formalité
    - 2^{40} essais, F U I E

- Sanctions encourues :
  - Import sans autorisation : 6 mois & 200 000 F
  - Tiers de confiance illégal : 2 ans & 300 000 F
  - Fourniture pour crime & délit : 3 ans & 500 000 F
  - Circonstance aggravante ?

- **Conclusion sur la cryptograhie**

✓Indispensable aux réseaux de communication

⇨ Sécurité Intranet / Extranet / Internet

✓Moteur de développement du @Business

✓Conséquences juridiques

7. Conclusion

Théorie de l'information ⇨ Domaine vaste (Continu, Modèle de réseaux, Théorie de la distorsion, …)