Deuxième partie

Cryptographie

Bibliographie (1/2)

- Cours de Cryptographie et de Cryptanalyse
  S. Julia et B. Martin – Université de Nice-Sophia Antipolis – 2002

- Codage, Cryptologie et Applications
  Bruno Martin – Presses Polytechniques et Universitaires romanes – Lausanne 2004

- Introduction à l'Informatique Quantique
  Chapitre 1.6 : Cryptographie Quantique
  Michel Le Bellac – Cours donné à L'ESSI – 2003

- L'Art du Secret – La Cryptographie
  Dossier de la Revue « Pour la Science » – Juillet 2002

- Initiation à la Cryptographie, 3ème Edition
  Gilles Dubertret – Vuibert – Paris, février 2002

Bibliographie (2/2)

- Histoire des codes secrets *(The Code Book)*
  (De l'Egypte des Pharaons à l'ordinateur quantique)
  Simon Singh – *Fourth Estate Limited, 1999*
  Texte Français : Catherine Coqueret -
  Editions Jean-Claude Lattès, 1999

- Réseaux, 4ème Edition – Chapitre 8 : La sécurité des réseaux
  Andrew Tanenbaum – Prentice Hall – London2003
  Texte français : *Véronique Warion & Michel Dreyfus* –
  Pearson Éducation France - Paris 2003

- Cryptography and Network Security: Principles and Practice, 3rd Edition
  William Stallings – Prentice Hall 2002

Sources Internet (1/2)

- Ars Cryptographica – Cours de Cryptographie du *Dr. Didier Müller*
  http://www.apprendre-en-ligne.net/crypto/

- *La Cryptogr@phie expliquée*
  http://www.bibmath.net/crypto/

- Introduction à la Cryptographie
  Guide mis en ligne par PGP (Pretty Good Privacy)
  ftp://ftp.pgpi.org/pub/pgp/6.5/docs/french/IntroToCrypto.pdf

- Technical Resources and Course Web Site for Cryptography and Network Security: Principles and Practice,
  Second Edition by *Williams Stallings*
  http://williamstallings.com/Security2e.html

Sources Internet (2/2)

- RSA Laboratories - Cryptography FAQ, Version 4.1
  http://www.rsasecurity.com/rsalabs/node.asp?id=2152

- The International PGP Home Page
  http://www.pgpi.org/

- SecuriteInfo.com
  http://www.securiteinfo.com/

Problèmes de sécurité (1/2)

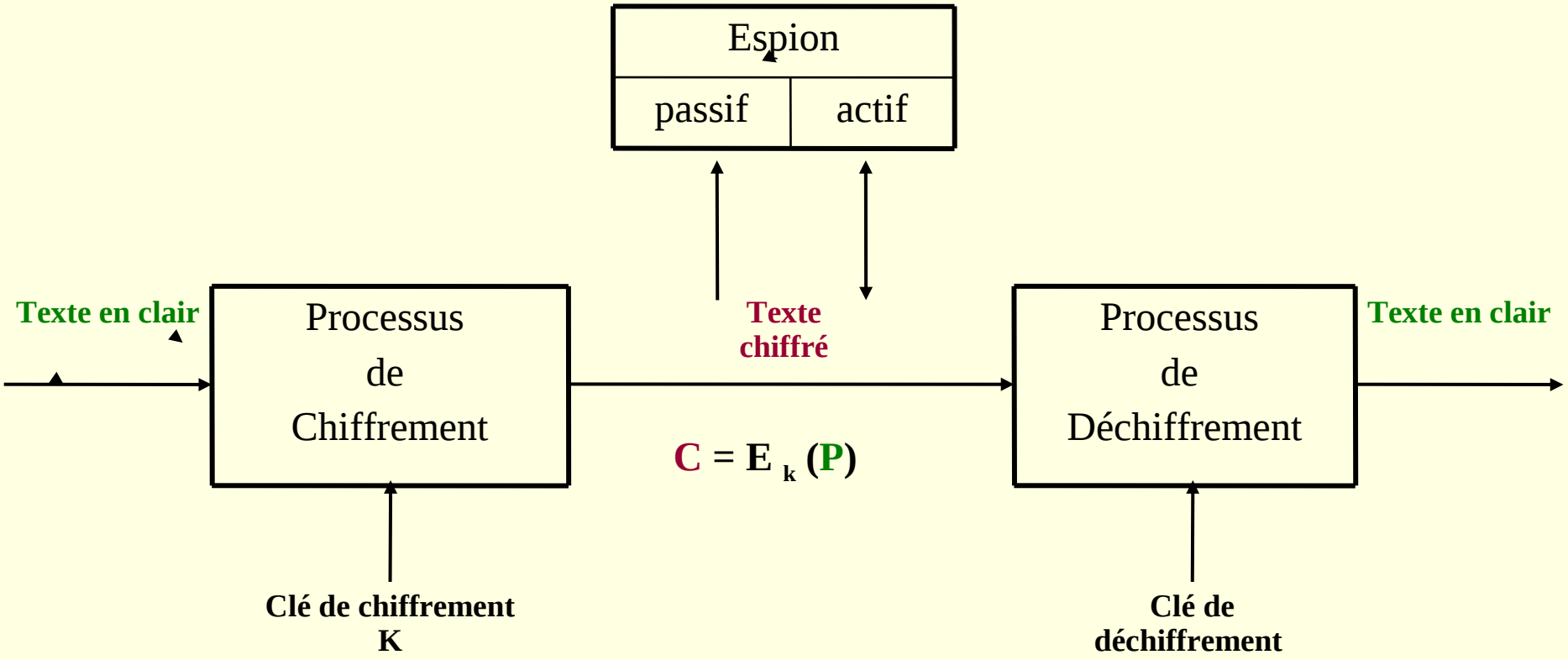
- Indiscrétion *(Eavesdropping)*
  - l'information n'est pas altérée, mais sa confidentialité est compromise
  - espionnage passif
  - Ex : récupération du N° d'une carte de crédit et de son code confidentiel

- Falsification (*Tampering*)
  - l'information en transit est modifiée ou remplacée avant d'être remise à son destinataire
  - espionnage actif
  - ex : changer le montant d'un virement bancaire

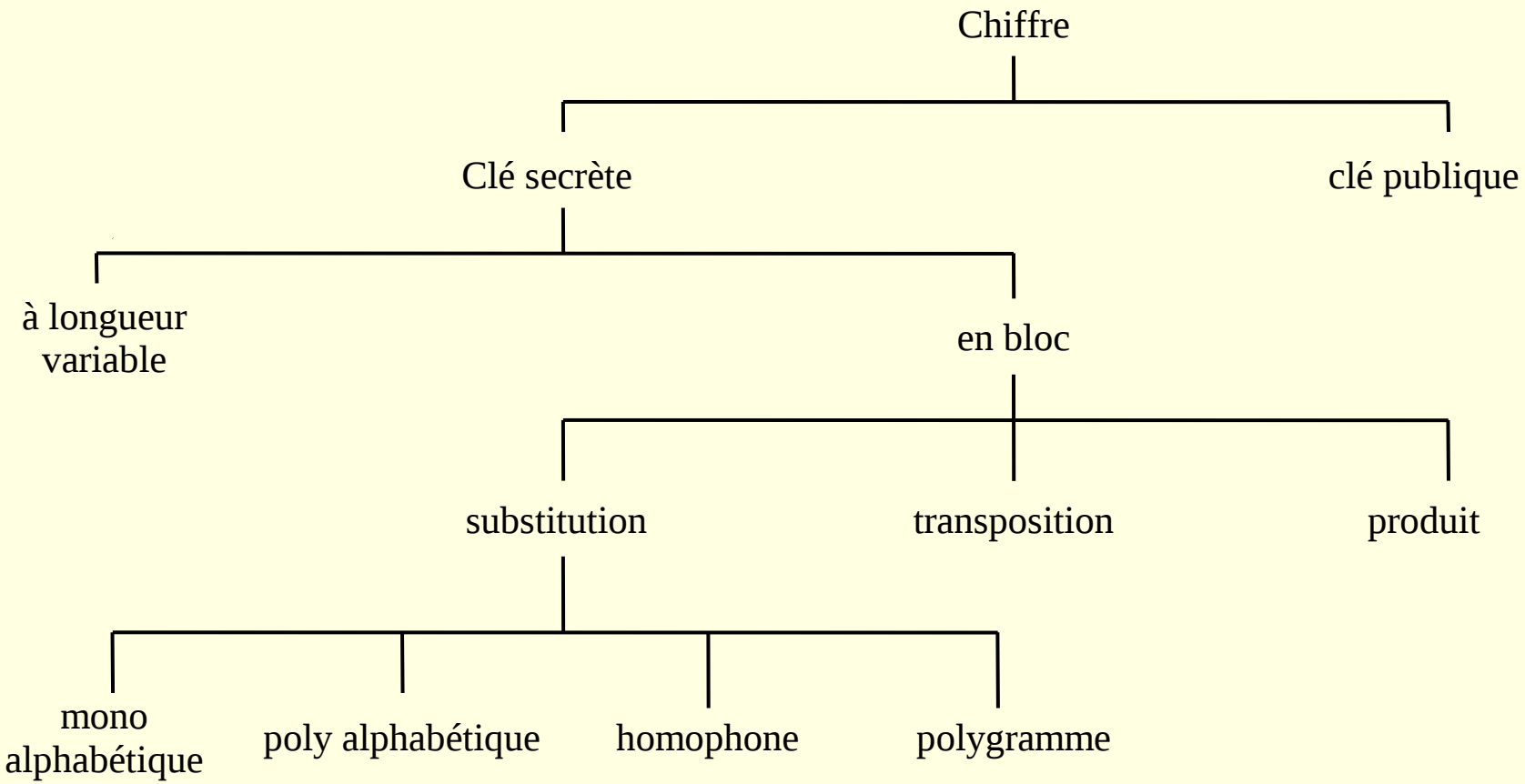
Problèmes de sécurité (2/2)

- Imitation *(Impersonation)*
  - Mystification *(Spoofing)*
    - ✓ une personne ou une entité se fait passer pour une autre
    - ✓ ex : utilisation frauduleuse de l'adresse e-mail d'une personne
  - Imposture (*Misrepresentation*)
    - ✓ une personne ou une organisation prétend être ce qu'elle n'est pas
    - ✓ ex : le site www.escroc.fr prétend commercialisé des fournitures informatiques alors qu'il ne fait qu'encaisser les paiements par cartes de crédit sans jamais livrer de marchandises.

Principe du chiffrement



Méthodes de chiffrement



Utilisation dans les réseaux

- Quatre objectifs non disjoints :
  - Confidentialité
    - ✓ Seules les personnes habilités ont accès à l'information
  - Contrôle d'Intégrité
    - ✓ L'information reçue est identique à celle qui a été envoyée
  - Authentification
    - ✓ L'interlocuteur est bien celui que l'on croit
  - Non-répudiation
    - ✓ Validité de la signature

Définitions (1/3)

- Cryptologie
  - Science des messages secrets. Elle se décompose en deux disciplines: la cryptographie et la cryptanalyse.
- Cryptographie
  - du grec κρυπτος (kryptos) : caché
    et γραφειν (graphein) : écrire
  - Art de transformer un message clair en un message inintelligible par celui qui ne possède pas les clefs de chiffrement.

Définitions (2/3)

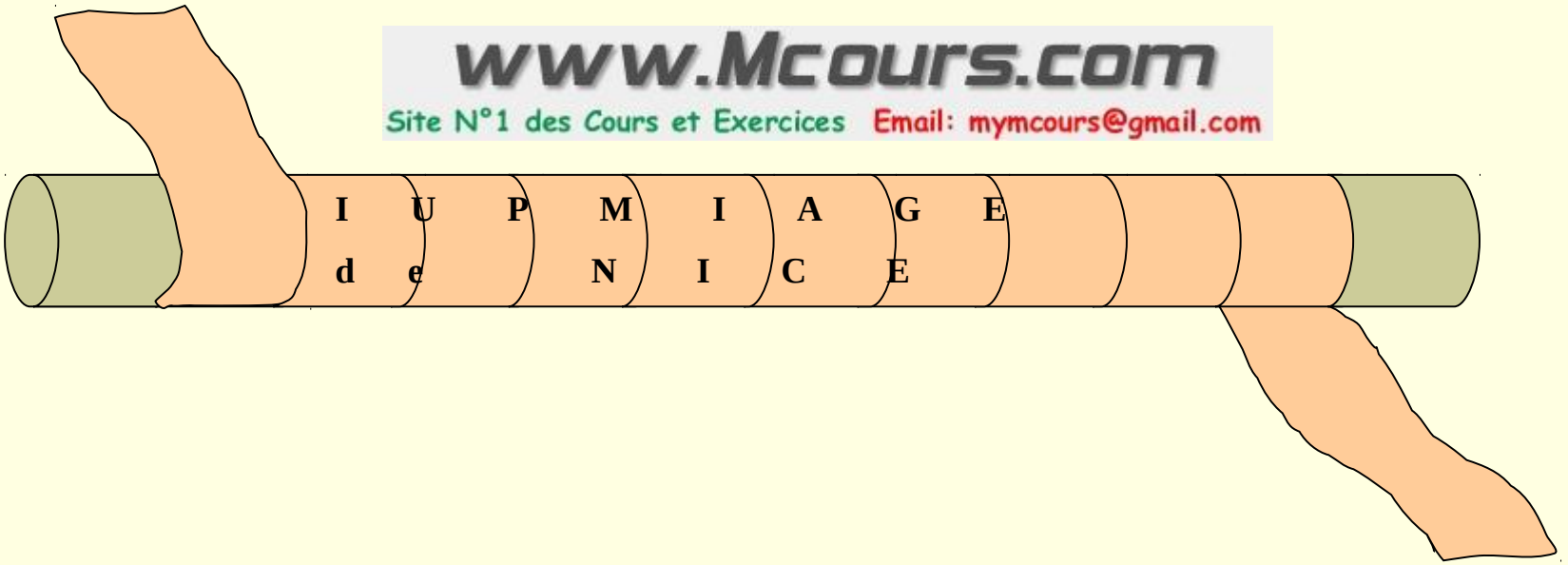
- Cryptographie (suite)
  - Stéganographie
    - ✓ du grec στεγανος (steganos) : couvert
      et γραφειν (graphein) : écrire
    - ✓ Branche particulière de la cryptographie qui consiste non pas à rendre le message inintelligible, mais à le camoufler dans un support (texte, image, etc.) de manière à masquer sa présence.

Définitions (3/3)

- Cryptanalyse
  - Art d'analyser un message chiffré afin de le décrypter.
  - Déchiffrement
    - ✓ Opération inverse du chiffrement, i.e. obtenir la version originale d'un message qui a été précédemment chiffré en connaissant la méthode de chiffrement et les clefs.
  - Décryptement
    - ✓ Restauration des données qui avaient été chiffrées à leur état premier ("en clair"), sans disposer des clefs théoriquement nécessaires.

Historique (1/2)

- Grèce antique : La scytale utilisée à Sparte :
  - Algorithme : Texte écrit sur un ruban enroulé autour d'un bâton
  - Clé : diamètre du bâton



Historique (2/2)

- Code secret de Jules César
  - Chiffrement par substitution une lettre en remplace une autre
  - Exemple très simple de cryptographie conventionnelle :
    - ✓ Algorithme : décalage des lettres de l'alphabet
    - ✓ Clé : nombre de lettre de décalage
  - Si on utilise 3 comme valeur de la clé la lettre A est remplacé par *D*, B par *E*, C par *F* etc. :

ABCDEFGHIJKLMNOPQRSTUVWXYZ
DEFGHIJKLMNOPQRSTUVWXYZABC

Exemple de codage :

Texte clair : **IUPMIAGE**

Texte chiffré : ***LXSPLDJH***

Codes de substitution (1/2)

- Substitution mono alphabétique
  - Amélioration du code de Jules césar
  - Clé constituée d'une chaîne correspondant à l'alphabet tout entier : chaque lettre est remplacée par une lettre quelconque
    $26! \approx 4 \times 10^{26}$ clés possibles
  - Exemple :
    - ✓ clé : ABCDEFGHIJKLMNOPQRSTUVWXYZ
      LZQANFTEPIWBHSYKMVGUDOJXCR
    - ✓ codage : Texte clair : **IUPMIAGE**
      Texte chiffré : ***PDKHPLSN***
  - Relativement facile à casser à partir des propriétés statistiques des langues naturelles

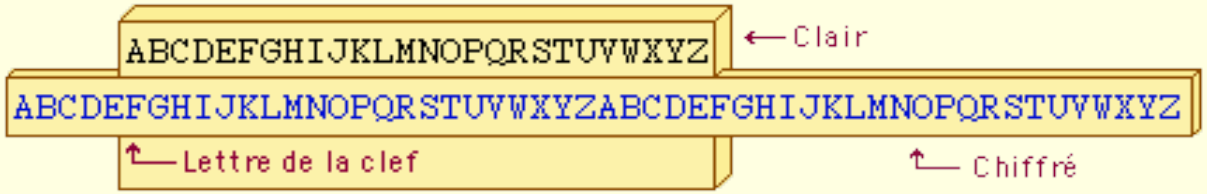
Codes de substitution (1/2)

- Substitution polyalphabétique
  - Exemple : Code de Vigenére (vers 1560)
    - ✓ Amélioration du code de César
    - ✓ Utilisation de 26 alphabets décalés (versus 1 dans le code de César)
    - ✓ Clé : définit le décalage pour chaque lettre du message
    - ✓ Avantage : différentes occurrences de la même lettre du message pourront être codée de façon différente
    - ✓ Exemple :

Texte clair	C	H	I	F	F	R	E	D	E	V	I	G	E	N	E	R	E
Clé	I	U	P	M	I	A	G	E	I	U	P	M	I	A	G	E	I
Décalage	8	20	15	12	8	0	6	4	8	20	15	12	8	0	6	4	8
Texte crypté	*K*	*B*	*X*	*R*	*N*	*R*	*K*	*H*	*M*	*P*	*X*	*S*	*M*	*N*	*K*	*V*	*M*

Codes de substitution (2/2)

- Variantes du chiffre de Vigenère
  - Carré de Vigenère (ou de Trithème)
  - Réglette de Saint-Cyr



Codes de transposition

- Algorithme : change l'ordre des lettres (mais ne les masque pas)
- Transposition par colonnes

M	I	A	G	E
5	4	1	3	2
e	x	e	m	p
l	e	d	e	c
o	d	e	u	t
i	l	i	s	a
n	t	l	a	t
r	a	n	s	p
o	s	i	t	i
o	n	p	a	r
c	o	l	o	n
n	e	s	a	b

Clé : MIAGE
Colonnes numérotées dans l'ordre alphabétique des lettres de la clé

Texte en clair :

```
exempledecodeutilisantlatransp
ositionparcolonnes
```

Texte encrypté :

```
edeilniplspctatpirnbmeusastaoa
xedltasnoeeloinroocn
```

Masque jetable (1/2)

- Blocs jetables (*one time pad*)
  - Principe
    - ✓ Clé : chaîne aléatoire de nombres (par exemple de bits) aussi longue que le texte à chiffrer
    - ✓ Caractères du message convertis en nombre (par exemple en binaire avec le code ASCII)
    - ✓ Caractère = fonction arithmétique ou logique du nombre correspondant au caractère à coder et du nombre correspondant de la clé (Exemple : OU exclusif entre les bits du message et ceux de la clé)
  - Inviolable
  - Exemple de clé : contenu d' un CD

Masque jetable (2/2)

- Exemple : Message de Che Guevara à Fidel Castro
  - Substitution des lettres par des chiffres

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
6	38	32	4	8	30	36	34	39	31	78	72	70	76	9	79	71	58	2	0	52	50	56	54	1	59

Clé = séquence aléatoire de chiffre connue uniquement des correspondants.
Chaîne de chiffres découpée en blocs de 5

Chiffrage : bloc additionné modulo 10 avec les 5 chiffres correspondants de la clé

Déchiffrage : soustraction modulo 10 des 5 chiffres de la clé au bloc crypté, puis remplacer les nombres par les lettres

Cryptanalyse : les attaques (1/2)

- L'attaque à texte chiffré seulement *(cipher text only)*
  - Le cryptanalyste dispose du texte chiffré de plusieurs messages, tous ayant été chiffrés avec le même algorithme.
    Objectif : retrouver le plus grand nombre de messages clairs possibles, ou mieux encore retrouver la ou les clefs qui ont été utilisées.

- L'attaque à texte clair connu *(known plaintext)*
  - Le cryptanalyste a non seulement accès aux textes chiffrés de plusieurs messages, mais aussi aux textes clairs correspondants. Objectif ; retrouver la ou les clefs qui ont été utilisées pour chiffrer ces messages ou un algorithme qui permet de déchiffrer d'autres messages chiffrés avec ces mêmes clefs.

Cryptanalyse : les attaques (2/2)

- L'attaque à texte clair choisi *(chosen plain text)*
  - Le cryptanalyste a non seulement accès aux textes chiffrés et aux textes clairs correspondants, mais de plus il peut choisir les textes en clair.
    Cette attaque est plus efficace que l'attaque à texte clair connu, car le cryptanalyste peut choisir des textes en clair spécifiques qui donneront plus d'informations sur la clef.

- L'attaque à texte chiffré connu *(chosen cipher text)*
  - Le cryptanalyste peut choisir différents textes chiffrés à déchiffrer. Les textes déchiffrés lui sont alors fournis.
    Par exemple, le cryptanalyste a un dispositif qui ne peut être désassemblé et qui fait du déchiffrement automatique. Sa tâche est de retrouver la clef.

Cryptanalyse : Techniques (1/2)

- Recherche exhaustive de la clef
  - Cette technique consiste simplement à essayer toutes les clefs possibles, jusqu'à ce qu'on trouve la bonne. Pour les chiffres à alphabet décalé, cette recherche est envisageable, puisqu'il y a peu de possibilités (par exemple 26 avec l'alphabet latin occidental)

- Analyse des fréquences
  - Dans le cas d'un chiffre mono alphabétique, c'est-à-dire quand l'alphabet est désordonné, ou que chaque lettre est remplacée par un symbole, on peut s'appuyer sur une analyse des fréquences des lettres ou des bi grammes.

Cryptanalyse : Techniques (2/2)

- Technique du mot probable
  - Une technique très puissante de décryptement consiste à supposer qu'une séquence de lettres du cryptogramme correspond à un mot que l'on devine. Ce type d'attaque marche aussi bien pour les substitutions simples que pour le chiffre de Vigenère (méthode de Bazeries), les homophoniques, ou encore le chiffre de Hill.
- Test de Friedman
  - Le test de Friedman permet de savoir si l'on a affaire à un chiffre mono alphabétique ou poly alphabétique. Il peut aussi être utilisé pour trouver la longueur de la clef d'un chiffre de Vigenère.
- Méthode de Babbage / Kasiski
  - Pour décrypter un chiffre de Vigenère, Babbage et Kasiski ont mis indépendamment au point une technique qui consiste à repérer des séquences de lettres qui se répètent dans le cryptogramme.

Cryptographie moderne

- Utilise la transposition et la substitution comme la cryptographie traditionnelle mais de façon différente :

  - Cryptographie traditionnelle
    - ✓ algorithmes relativement simples
    - ✓ clés longues pour assurer la sécurité

  - Cryptographie moderne
    - ✓ algorithmes très complexes
    - ✓ clés relativement courtes

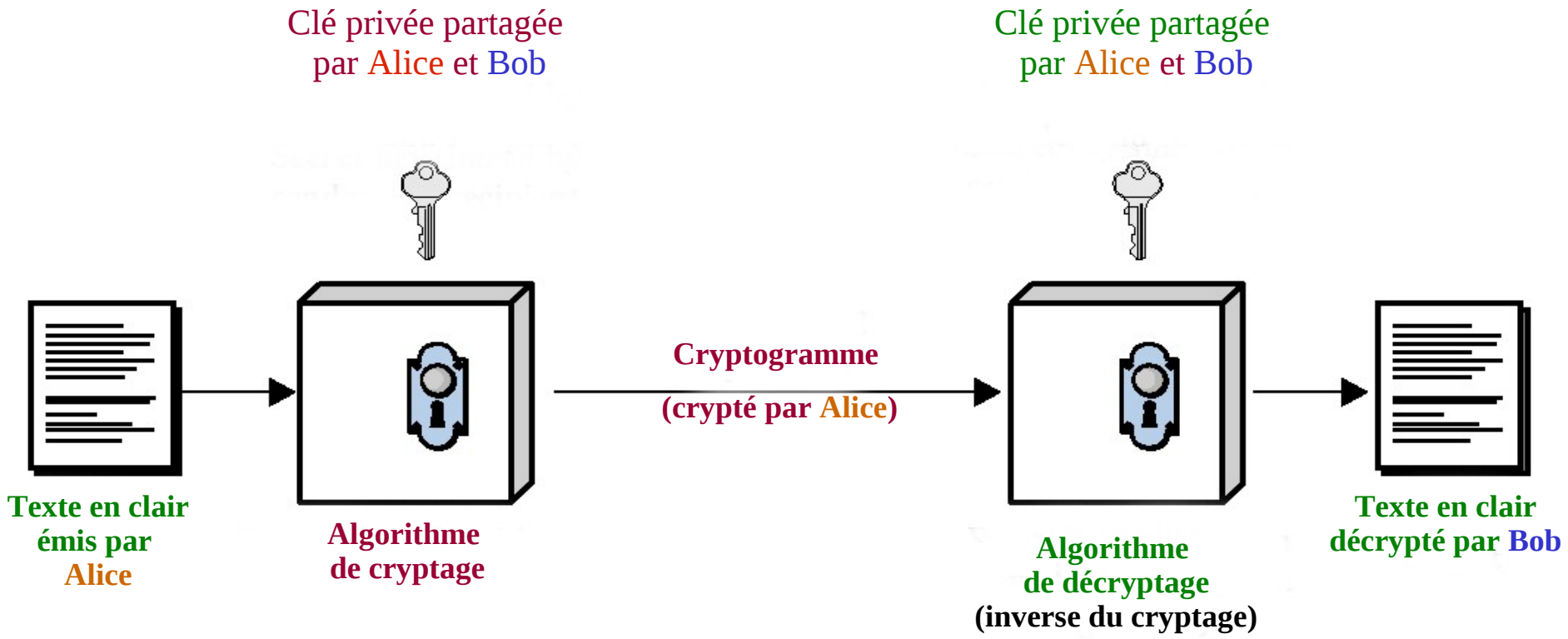
Cryptographie à clé privée

- Sécurité inconditionnelle (*Perfect secrecy*)

- Symétrique
  - Même algorithme pour chiffrement et déchiffrement
  - Même clé pour chiffrement et déchiffrement

- Clé secrète
  - Connue uniquement des interlocuteurs et parfois d’un tiers de confiance

Modèle simplifié



Modèle simplifié de cryptage symétrique à clé privée

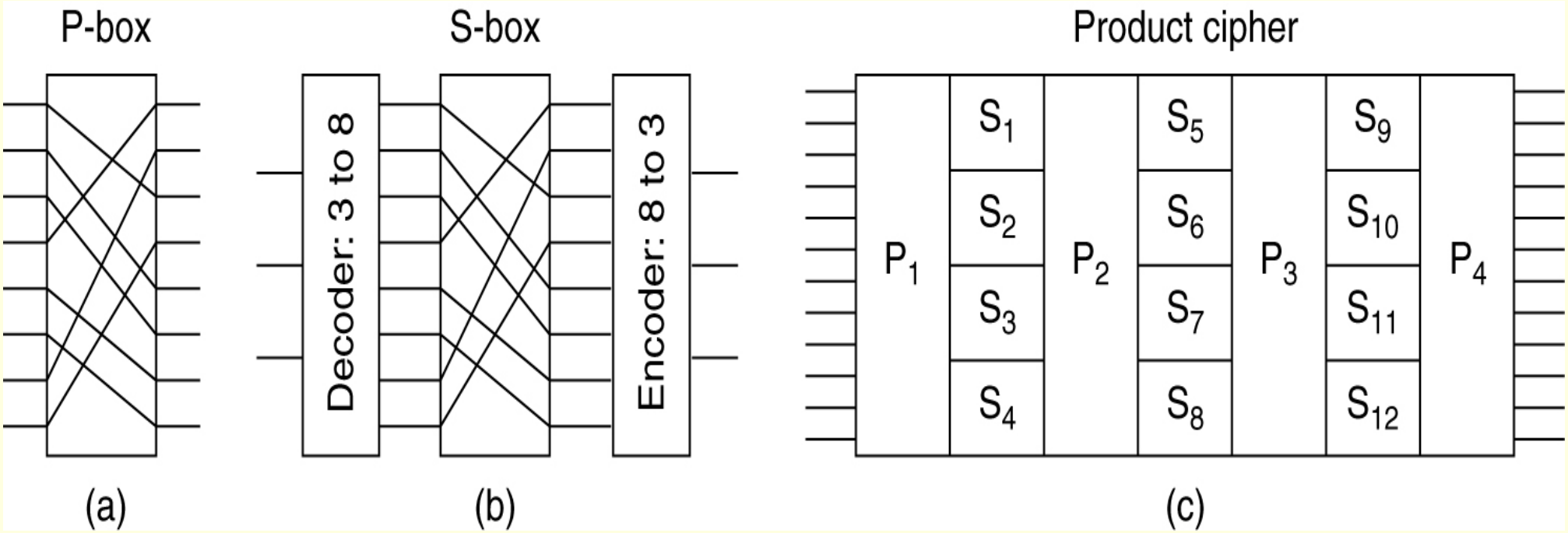
Chiffrement par blocs (1/3)

- Principe :
  - Remplacer les caractères du message par des codes binaires (ex: ASCII)
  - Segmenter la chaîne binaire en blocs de chacun N bits
  - Crypter successivement chaque bloc :
    - ✓ Opération logique bit à bit avec une clé (ex: Ou exclusif)
    - ✓ Déplacement de certains bits à l'intérieur du bloc (ex: permutation)
    - ✓ Recommencer un certain nombre de fois les opérations précédentes (appelées une ronde)
  - Concaténer les blocs pour obtenir le message encodé

Chiffrement par blocs (2/3)

- Réalisation :
  - Les permutations et les substitutions sont réalisées dans des dispositifs appelés :
    - ✓ Boites-P *(P-box)* pour les Permutations
    - ✓ Boites-S *(S-box)* pour les Substitutions
  - L'algorithme de cryptage est réalisé par une succession de boÎtes-P et de boîtes-S

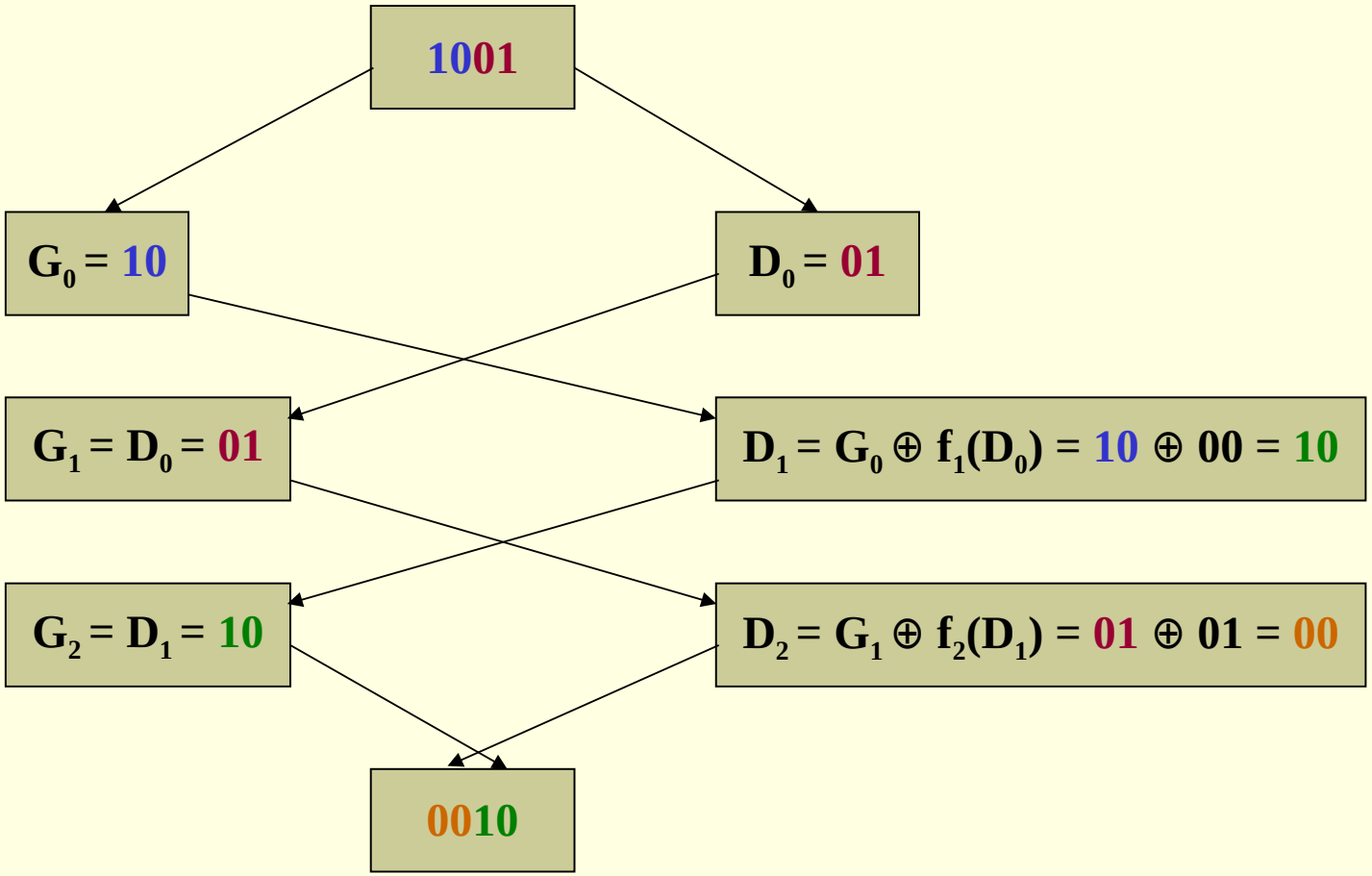
Chiffrement par blocs (3/3)



Réseau de Feistel

- Base de pratiquement tous les algorithmes modernes à clé secrète (en particulier DES)
  Proposé par Horst Feistel (IBM) en 1973
- Système de chiffrement par blocs
  - division d'un bloc en clair en deux partie de même taille
  - modification d'une moitié par application d'une ronde
  - modification de l'autre moitié : OU exclusif avec la première moitié
  - permutation des deux moitiés
  - application de la ronde suivante
- Chiffrement et déchiffrement structurellement identiques

Réseau de Feistel : Exemple simplifié



Entrée	f1	Sortie
00	→	10
01	→	00
10	→	11
11	→	10

Entrée	f2	Sortie
00	→	00
01	→	01
10	→	01
11	→	10

DES (1/3)

- DES : The **D**ata **E**ncryption **S**tandard
- Mis au point par IBM et adopté en 1977 par l'agence nationale de sécurité américaine le NSA (National Security Agency) fin 1976
- Algorithme standard et connu publiquement
  - Basé sur les réseaux de Feistel
    - le texte en clair est découpés en blocs de 64 bits qui sont encodés séparément puis concaténés
    - clés : 64 bits dont 56 seulement sont utilisées
    - nombre de rondes : 16

DES (2/3)

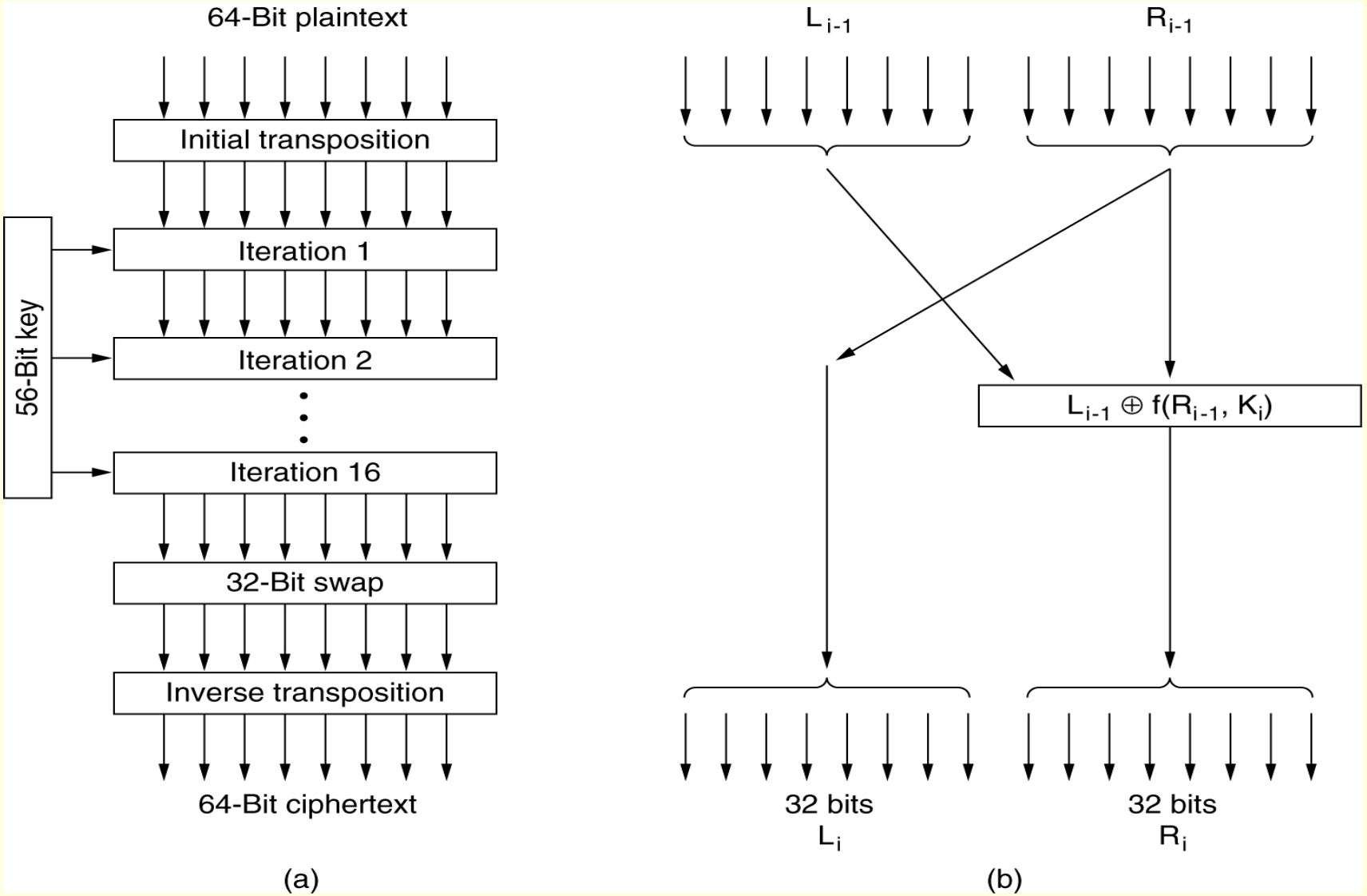


Schéma général **Détail d'une itération**

DES (3/3)

- Avantages du DES
  - Bonne sécurité (Résiste à des attaques raisonnables (moins de 10 M$ et moins d'un mois)
  - Nombre de clés élevé : $2^{56} = 7{,}2 \times 10^{16}$
  - Facilement réalisable matériellement
  - Certains circuits chiffrent jusqu'à 1 Go par seconde
- Questions et doutes
  - Existe-t-il une faille dans la sécurité introduite par la NSA ?
  - Faiblesse de certaines clés
  - 56 bits sont-ils une longueur suffisante pour la clé ?
- Conclusion
  - Système actuellement le plus utilisé
  - AES (Advanced Encryption Standard) en cours de développement

DES - Améliorations

- Triple DES
  - IBM en 1979
  - 3 étages : chiffrement-déchiffrement-chiffrement
  - 2 clés : K1 et K2
  - Compatibilité avec DES simple : K1=K2
- DES-CBC
  - CBC : Cipher Block Chaining
  - faiblesse du DES : 2 textes clairs identiques donnent toujours le même cryptogramme
  - solution : faire dépendre le chiffrement du contenu du block précédent (en plus de la clé et du texte clair)

AES

- AES : The **A**dvanced **E**ncryption **S**tandard
- Proposition pour succéder au DES
- Objectifs :
  - algorithme de cryptage «à blocs symétriques»
  - conception entièrement publique
  - longueurs de clés : 128, 192 et 256 bits
  - réalisations logicielles et matérielles
  - algorithme public ou exploitable sous licence de façon non discriminatoire

IDEA

- Parmi tous les algorithmes de chiffrage par blocs proposés comme alternative au DES un des plus connus est l'IDEA (International Data Encryption Algorithm)
  - mis au point par des chercheurs suisse
  - clé de 128 bits
  - incassables avec les machines et les techniques actuelles
  - premières réalisations
    - ✓ logicielle : sur un 386 à 33MHz : 0,88Mbit/s
    - ✓ matérielle : VLSI expérimental à 25Mhz : 177Mbit/s
    - ✓ (Source : Tanenbaum : Réseaux, 3ème édition)

Résumé

Chiffre	Auteur	Longueur de clé	Commentaires
Blowfish	Bruce Schneier	1 à 448 bits	Vieux et lent
DES	IBM	56 bits	Trop faible pour une utilisation actuelle
IDEA	Massey et Xuejia	128 bits	Efficace, mais breveté
RC4	Ronald Rivest	1 à 2 048 bits	Attention : certaines clés sont faibles
RC5	Ronald Rivest	128 à 256 bits	Efficace, mais breveté
Rijndael	Daemen & Rijmen	128 à 256 bits	Meilleur choix
Serpent	Anderson, Biham et Knudsen	128 à 256 bits	Très fort
Triple DES	IBM	168 bits	Second meilleur choix
Twofish	Bruce Schneier	128 à 256 bits	Très fort, largement utilisé

D'après Réseaux 4ème édition de AndrewTanenbaum

Cryptographie à clé publique

- Inconvénient des systèmes à clés secrètes :
  - la même clé sert à chiffrer et à déchiffrer d'où un problème de confidentialité et de distribution aux utilisateurs
- 1976 Diffie et Hellmann de l'université de Standford proposent une approche différente basée sur deux clés distinctes :
  - une clé de chiffrement (algorithme de chiffrement C)
  - une clé de déchiffrement différente (algorithme de déchiffrement D)

  les algorithmes D et C devant satisfaire 3 contraintes
  - D (C(M)) = M
  - Extrêmement difficile de déduire D à partir de C
  - C résiste à toute attaque « texte en clair choisi »

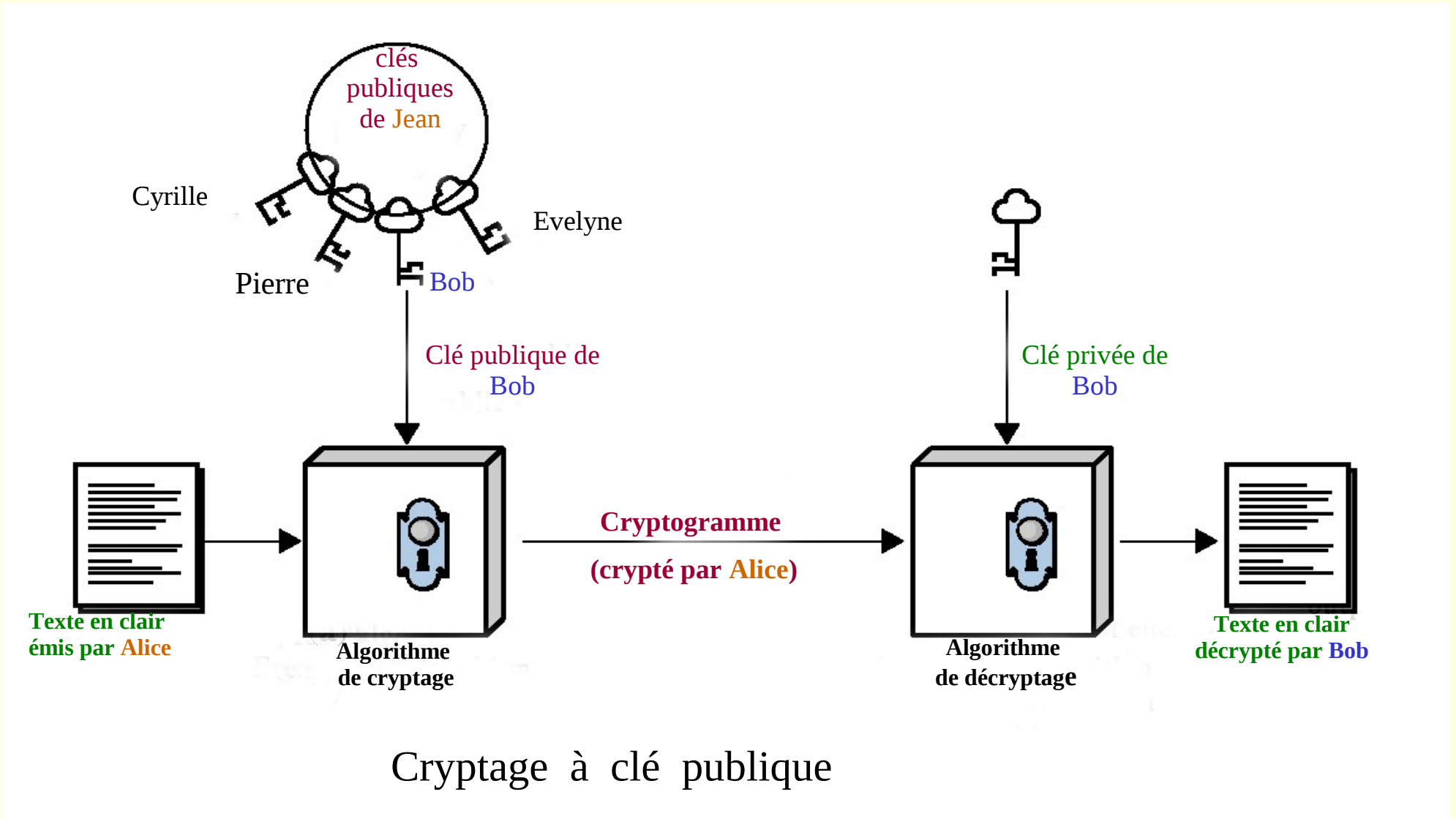
Cryptographie à clé publique

- Public Key Cryptography
  - PKI (Public Key Infrastructure – Netscape)

- Sécurité calculatoire
  - la durée du processus de calcul nécessaire pour casser la clé doit être supérieure à la durée de vie de l'information à protéger

- Non symétrique
  - Algorithme de chiffrement ≠ algorithme de déchiffrement
  - Clé publique pour chiffrer ≠ clé privée pour déchiffrer

Modèle de cryptage à clé publique



Cryptage à clé publique

Le Chiffre de Merkle-Hellman

- Problème du sac à dos (*Knapsack problem*)
  - Premier algorithme à clé publique (1978)
  - Principe
    - ✓ un très grand nombre d'objets, chacun de poids différents
      la liste de tous les objets est publique
    - ✓ le message est chiffré en choisissant secrètement un certain nombre d'objets qui sont mis dans le sac à dos
    - ✓ le poids total du sac à dos est public
    - ✓ le contenu du sac à dos est secret
  - L'algorithme à clé publique est basé sur le fait qu'il est très très difficile de trouver la listes des objets à partir de leur poids total

RSA : Algorithme (1/4)

- RSA : méthode proposée pour choisir les clés par Rivest, Shamir et Adelman du MIT (Massachusetts Institute of Technology) en 1978

- La sécurité repose sur la difficulté de factoriser un nombre qui est le produit de deux nombre premiers très grands.

- Les clés publique et privée sont générées à partir de deux nombres premiers très grands (plus de 100 chiffres)

RSA : Algorithme (2/4)

- Principe
  - Prendre 2 nombres premiers très grands : p et q
  - Calculer $n = p \times q$
  - Calculer $z = \Phi(n) = (p-1) \times (q-1)$
  - Prendre un nombre e premier avec z :
    PGCD $(z,e) = 1$ avec $1 < e < z$
  - Calculer d tel que $d \times e = 1 \bmod z$
  - La clé publique correspond au couple : $\{e,n\}$
  - La clé privé correspond au couple : $\{d,n\}$

RSA : Algorithme (3/4)

- Exemple simplifié (avec p et q très petits)
  - On choisit : $p = 5$ et $q = 11$
  - Ce qui implique :
    - ✓ $\boldsymbol{n} = p \times q = 5 \times 11 = 55$
    - ✓ $z = \Phi(n) = (p-1) \times (q-1) = 4 \times 10 = 40$
  - On peut choisir $e = 7$ (7 est premier avec 40)
    - ✓ Et on calcule d tel que :
      $d \times e = 1 \bmod z \Rightarrow d \times 7 = 1 \bmod 40 \Rightarrow d = 23$
  - On obtient donc :
    - ✓ Clé publique : {7, 55}
    - ✓ Clé privée : {23, 55}

Chiffrement						
Clair		Clé publique : 7	Chiffré			
		P^7	$P^7 \bmod 55$			
I	9	4782969	4	70368744177664	9	I
U	21	1801088541	21	25765808751082182919290758696 61	21	U
P	16	268435456	36	623673825204293256669089197883129856	16	P
M	13	62748517	7	27368747340080916343	13	M
I	9	4782969	4	70368744177664	9	I
A	1	1	1	1	1	A
G	7	823543	28	1925904380037276068854119113162752	7	G
E	5	78125	25	1421085471520200371742248535156 25	5	E
					C^{23}	$C^{23} \bmod 55$
			Chiffré	Clé privé : 23	Déchiffré	
			Déchiffrement			

Autres algorithmes

- Algorithmes basés sur la difficulté à calculer des logarithmes
  - Chiffre de Rabin (1979)
  - El Gamal (1981)
  - Schnorr (1991)

- Algorithmes fondées sur les courbes elliptiques
  - Menezes et Vandstone (1993)

Authentification

- 2 grandes familles de systèmes basées soit sur :
  - une clé secrète partagée
    - ✓ nombreuses façon de :
      - s'échanger
      - créer

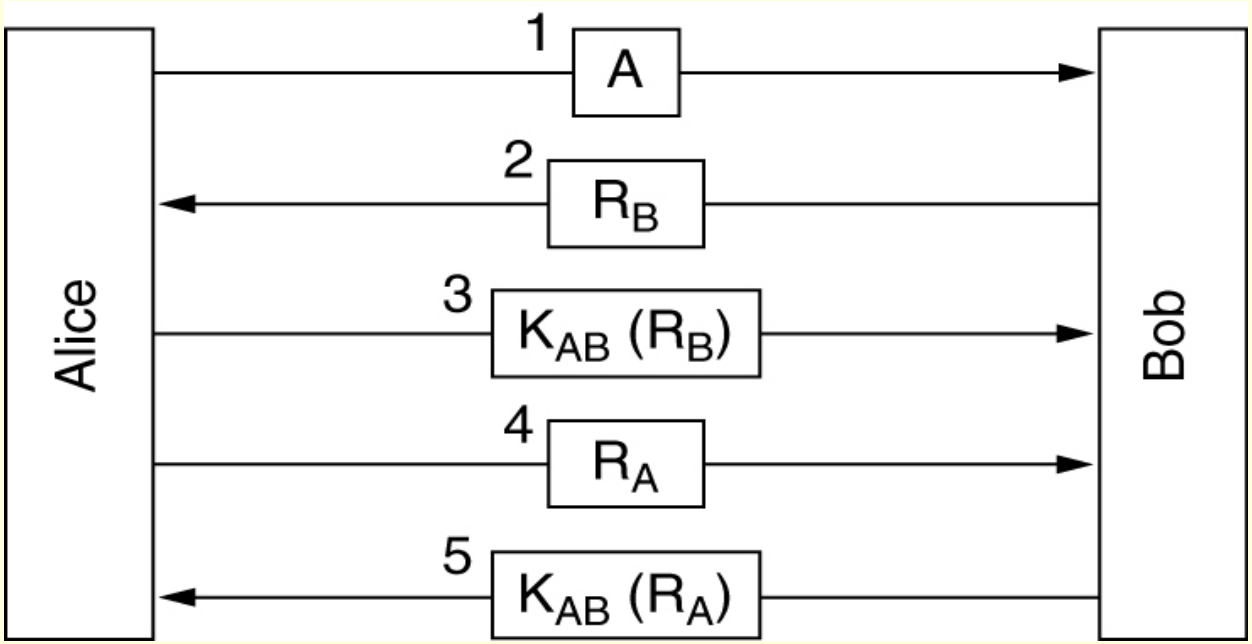
      la clé privée
  - l'utilisation des mécanismes à clés publiques
    - ✓ certificats
    - ✓ centre de distribution de clés

Clé secrète partagée

- Protocole question-réponse *(challenge-response)*
  - les deux protagonistes possède une clé secrète K_{AB}
  - Principe : un des deux protagonistes envoie un grand nombre aléatoire à son homologue qui le crypte et le lui renvoie

Clé secrète partagée

- Exemple : Authentification mutuelle par question-réponse



1- Alice s'identifie à Bob

2 - Bob lui envoie un grand nombre aléatoire R_B

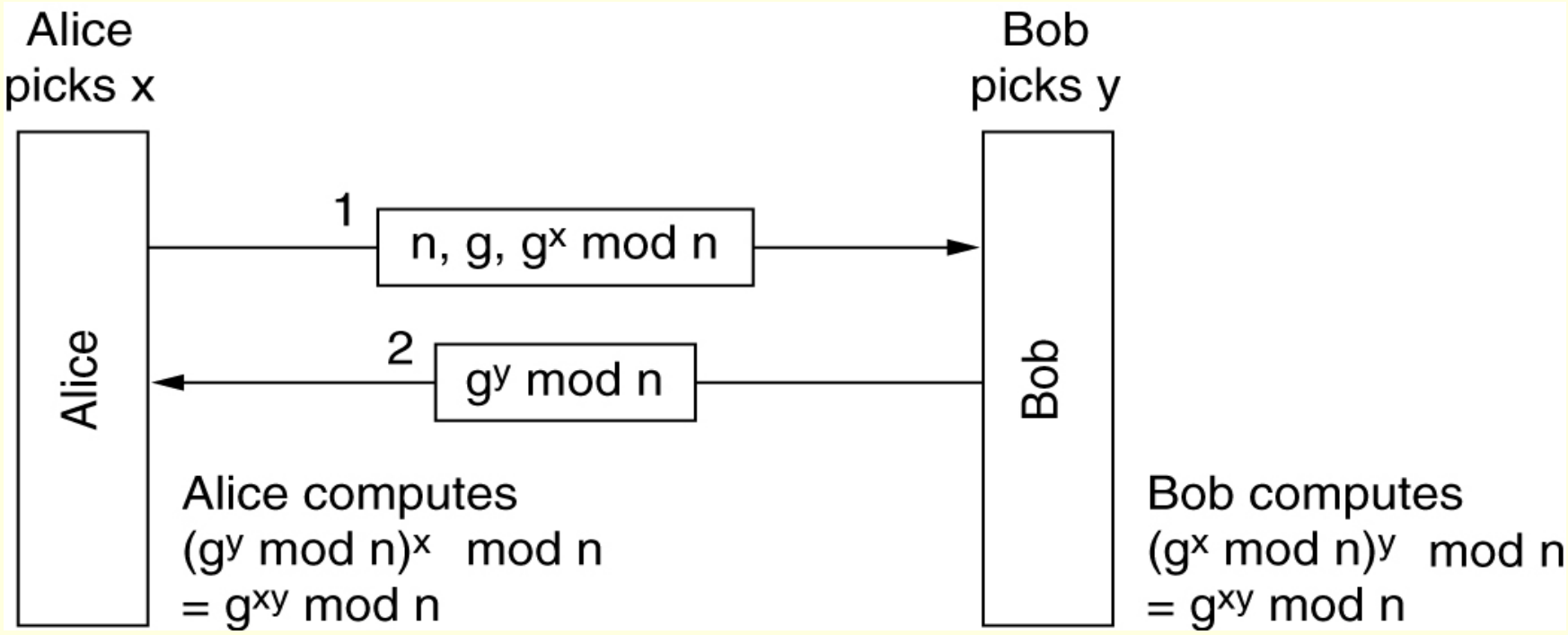
3 - Alice crypte R_B et le renvoie à Bob

4 - Alice envoie un grand nombre aléatoire R_A à Bob

5 - Bob crypte R_A et le renvoie à Alice

Clé secrète partagée

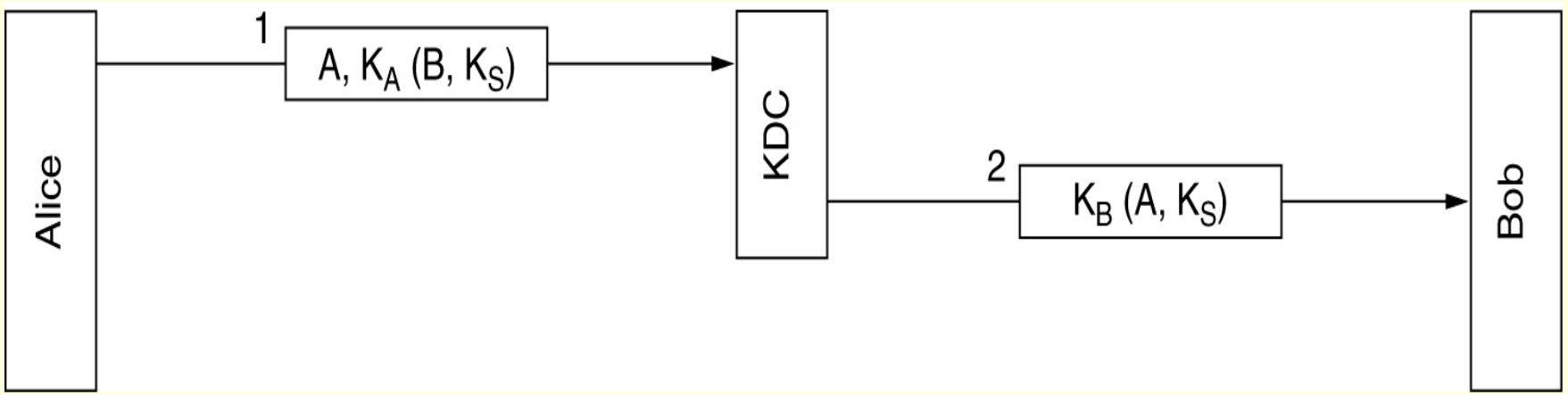
- Echange de clés de Diffie-Hellman (1976)
  - Permet à deux interlocuteurs ne se connaissant pas de créer une clé secrète



n et g = 2 grands nombres premiers avec (n-1)/2 premier et certaines conditions sur g

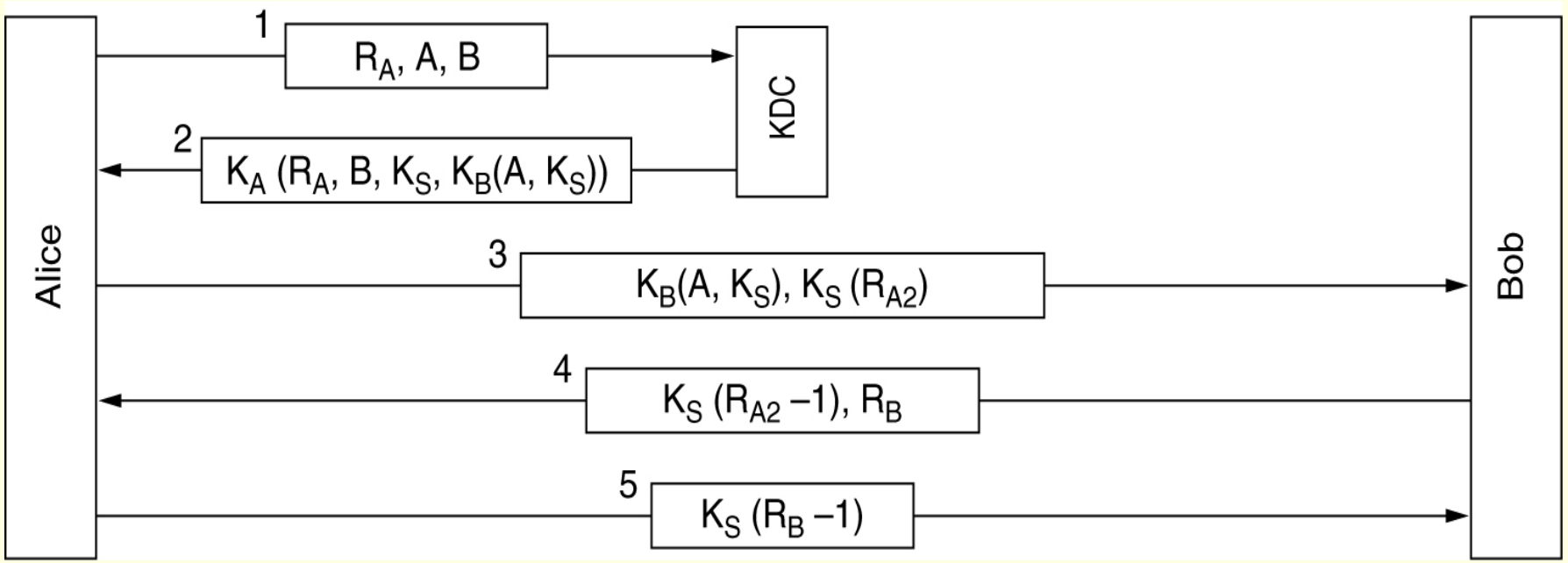
Clé secrète partagée : CDC

- CDC (Centre de Distribution de Clés)
  - Chaque utilisateur partage avec le CDC une seule clé
  - L'authentification et la gestion des clés de session se font via le CDC
  - Première approche :



Clé secrète partagée : CDC

- Protocole d'authentification de Needham-Schroeder
  - Corrige certaines failles du protocole précédent :

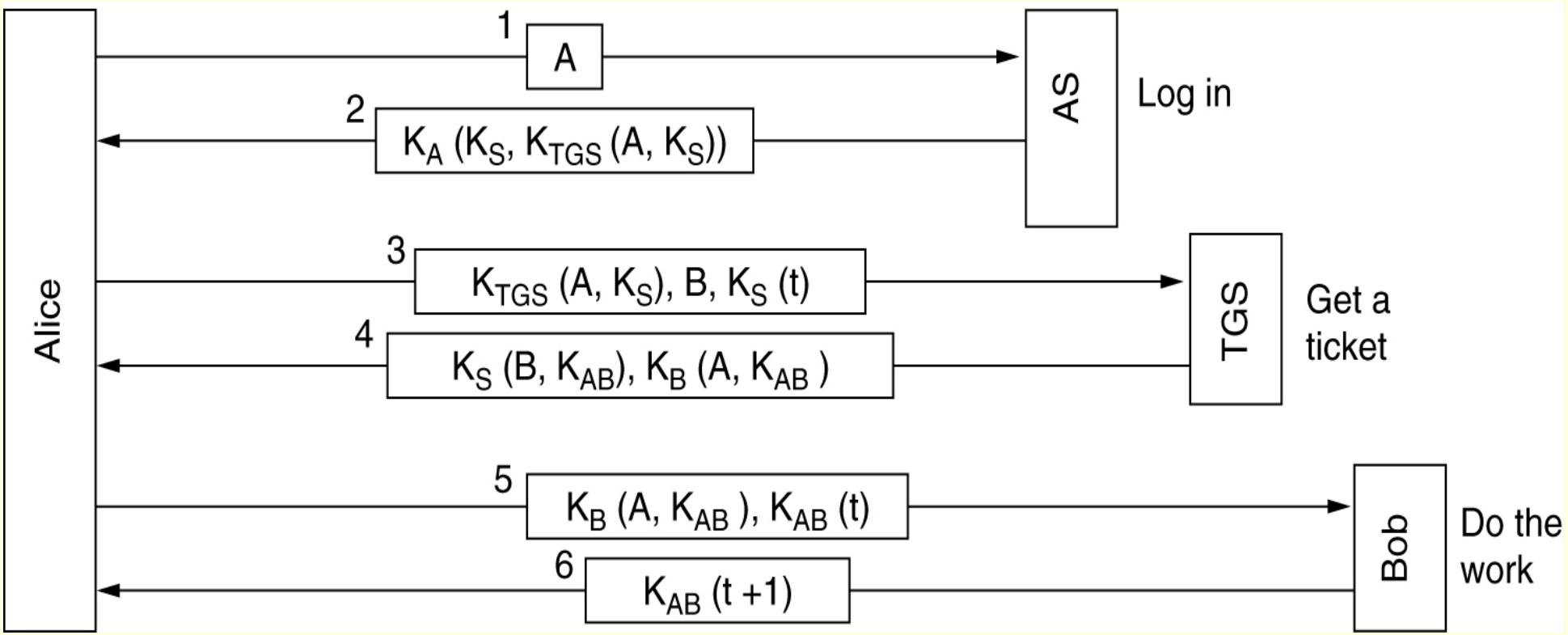


Clé secrète partagée : CDC

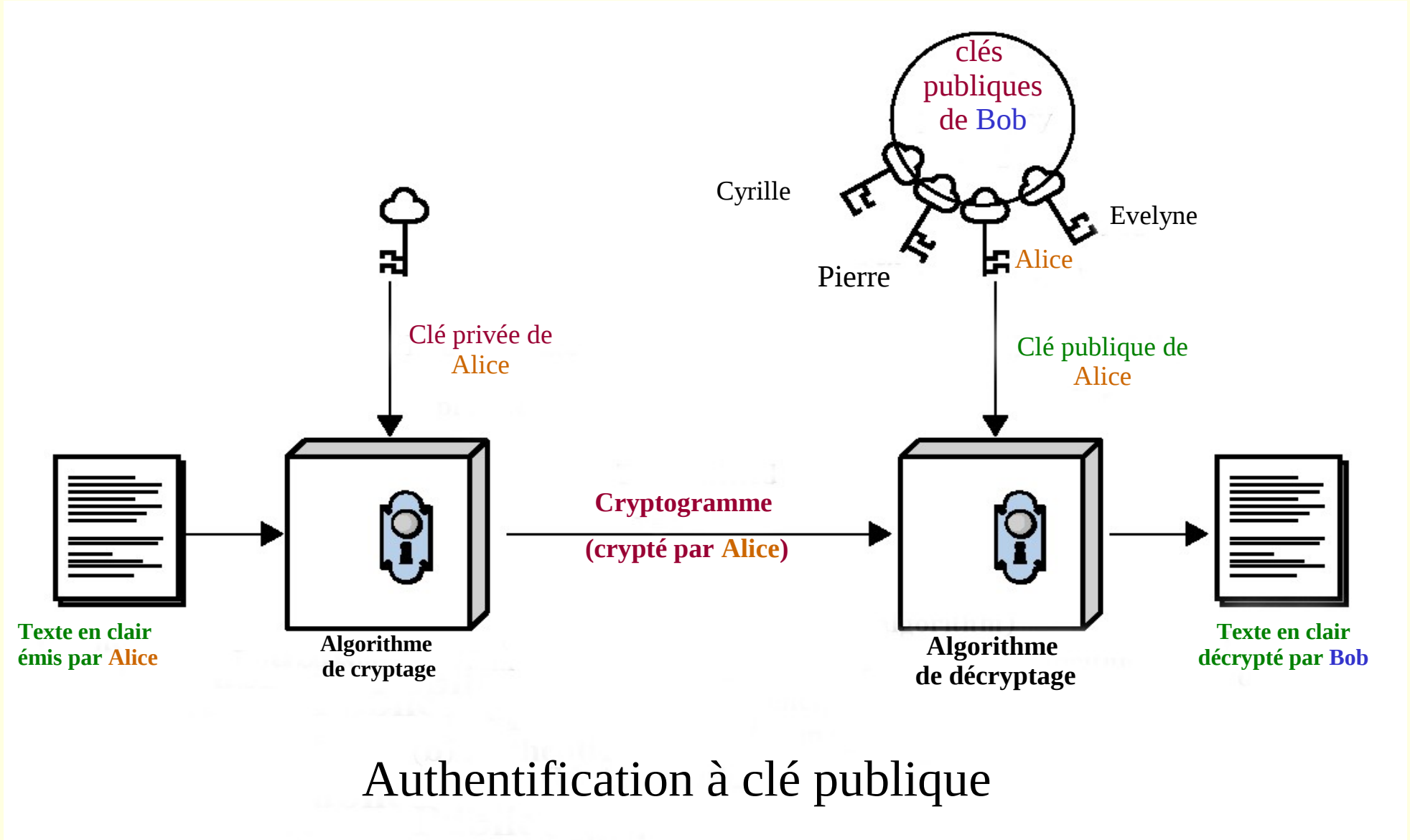
- Kerberos
  - Cerbère : chien à plusieurs têtes gardien de l'entrée des Hadès, dans la mythologie grecque
  - Mis au point au MIT pour permettre à des utilisateurs d'accéder à des stations de travail de façon sûre
  - Fournit un service centralisé pour authentifier les utilisateurs vis-à-vis de serveurs et réciproquement
  - Repose sur des techniques de cryptage n'utilisant pas les clés publiques
  - Deux versions en cours : version 4 et version 5
    - ✓ La version 4 utilise DES

Clé secrète partagée : CDC

- Principe de fonctionnement de Kerberos Version 4



Modèle d'authentification à clé publique



Authentification à clé publique

X.509

- Ensemble de serveurs distribués gérant une data base des utilisateurs
- Chaque certificat contient la clé publique d'un utilisateur et est signé avec la clé privé du CA (Certification Authority)
- Utilisé par S/MIME, IP Security, SSL et SET
- l'utilisation de RSA est préconisée

X.509

- Principaux champs d'un certificat X509

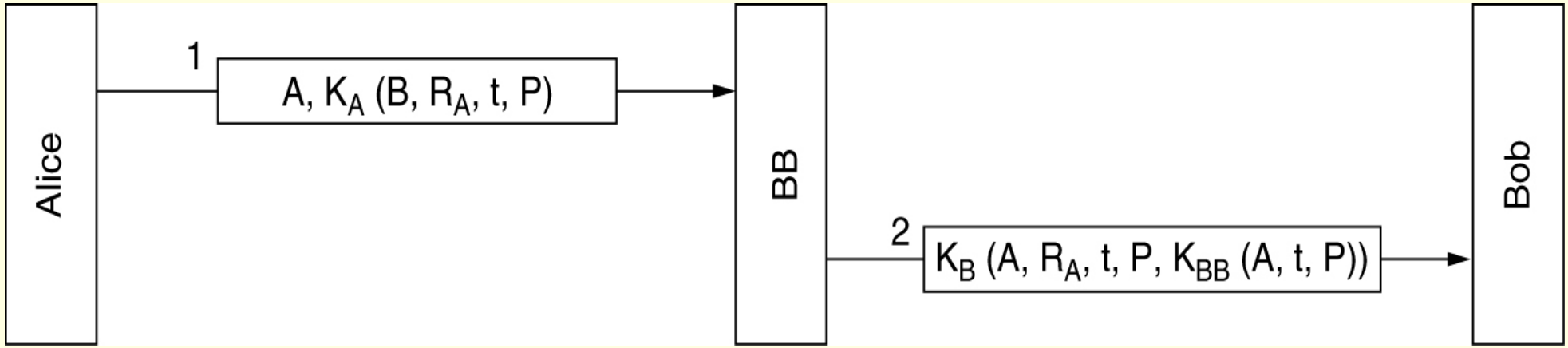
Field	Meaning
Version	Which version of X.509
Serial number	This number plus the CA's name uniquely identifies the certificate
Signature algorithm	The algorithm used to sign the certificate
Issuer	X.500 name of the CA
Validity period	The starting and ending times of the validity period
Subject name	The entity whose key is being certified
Public key	The subject's public key and the ID of the algorithm using it
Issuer ID	An optional ID uniquely identifying the certificate's issuer
Subject ID	An optional ID uniquely identifying the certificate's subject
Extensions	Many extensions have been defined
Signature	The certificate's signature (signed by the CA's private key)

Signature

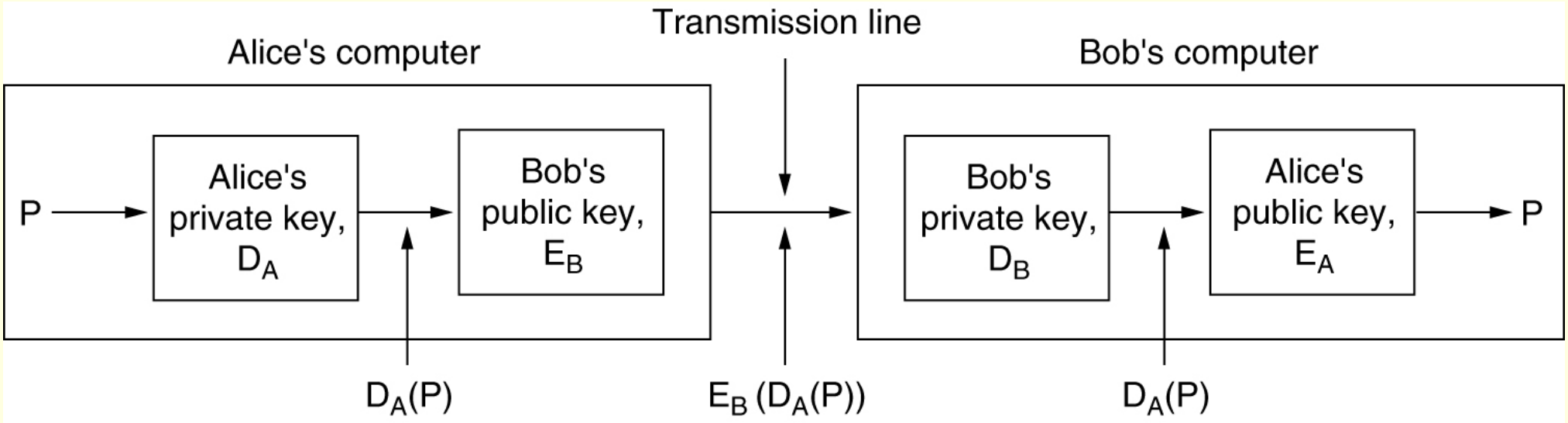
- La signature associée à un message doit permettre de résoudre trois problèmes :
  - le destinataire d'un message peut vérifier l'identité affichée par l'émetteur grâce à sa signature
  - l'émetteur ne pourra pas renier la paternité du contenu d'un message qu'il a envoyé et signé
  - le destinataire ne peut pas créer lui-même un message et faire croire qu'il a été émis par un tiers

Signature à l'aide de clés secrètes

- Utilisation d'une autorité centrale intermédiaire
  (BB comme Big Brother sur le Schéma)



Signature à l'aide de clés publiques



Intégrité des message – Hachage (1/2)

- Techniques utilisés lorsqu'on n'a pas besoin de confidentialité : le message peut être transmis en clair mais il doit être authentifié et son intégrité doit être garantie

- La fonction de hachage permet de créer un résumé du message de longueur fixe. Elle doit avoir trois propriétés importantes :
  - Etant donné M il est facile de calculer $R_M(M)$
  - Etant donné $R_M(M)$, il est impossible de trouver M
  - Personne ne peut engendrer deux messages différents ayant le même résumé

Intégrité des message – Hachage (2/2)

- Calcul du résumé d'un message beaucoup plus rapide que le chiffrement
- Grand nombre de fonctions de hachage. Les plus utilisées sont :
  - MD5 (Ron Rivest,1992) :chaque bit de sortie est affecté par chaque bit d'entrée
  - SHA (Secure Hash Algoritm) développé par la NSA

Sécurité des communications

- IPSec (IP Security)
- Firewalls
- Virtual Private Networks
- Wireless Security

Sécurité des E-Mails

- PGP (Pretty Good Privacy)
- PEM (Privacy Enhanced Mail)
- S/MIME

Sécurité du WEB

- Threats
- Secure Naming
  - Secure DNS (Domain Name Server)
- SSL (Secure Sockets Layer)
  - Mis au point par Netscape et Master card utilisé parMozilla, Internet explorer, etc.
  - Gestion des clés et authentification du serveur avant l'échange d'information
  - Assure l'authentification, la confidentialité et l'intégrité des données échangées
  - Utilise 2 types de cryptographie
    - ✓ Publique : RSA dans la phase d'établissement
    - ✓ Privée : RC2 ou RC4 pendant la session

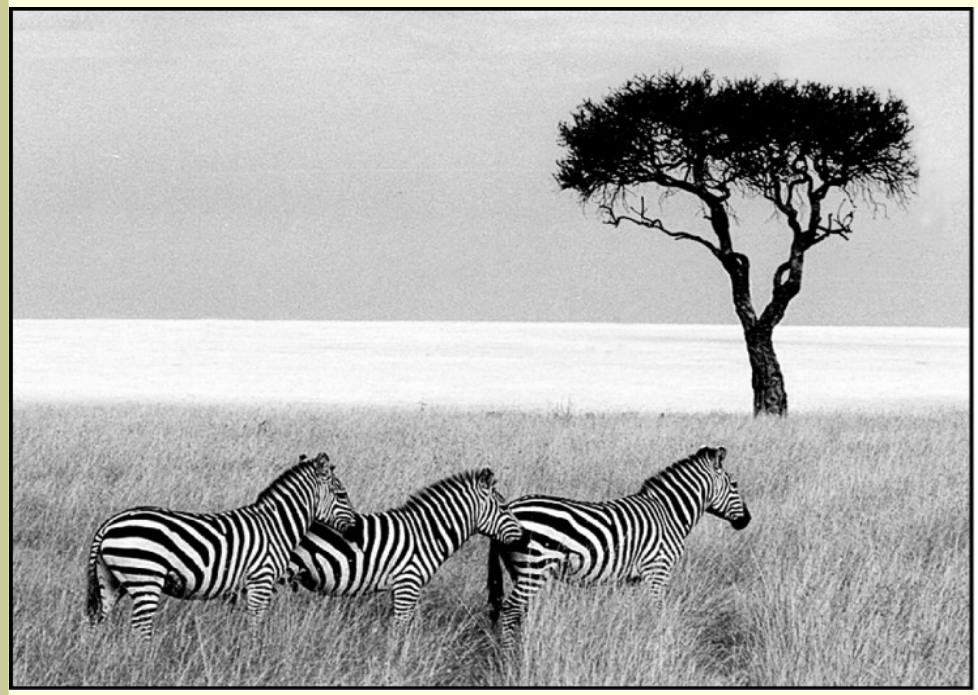
Sécurité du WEB

- SET (Secure Electronic Transaction)
  - Spécification technique écrite par Visa et MasterCard
    - ✓ Décrit les protocoles et algorithmes nécessaires à sécuriser les paiements sur des réseaux ouverts de type Internet
    - ✓ Objectifs:
      - Authentification des porteurs de cartes,
des commerçant
des banques des acheteurs
      - Confidentialité des paiements
      - Intégrité des données du paiement
- Mobile code Security (Java applet security)

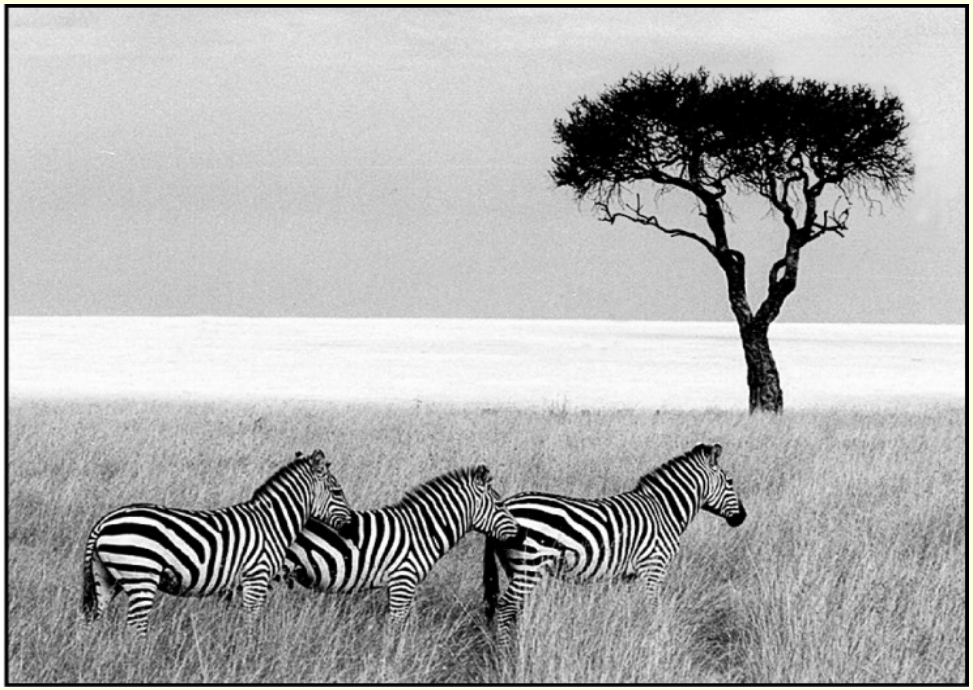
Stéganograhie

- Art de la dissimulation
- On peut dissimuler un message dans :
  - un autre texte
    - ✓ ex : encre sympathique ((jus de citron, ...)
    - ✓ ex: La Lettre de Georges Sand à Alfred de Musset
  - une image
    - ✓ utilisation des bits de poids faible des pixels

Stéganographie : exemple



3 zèbres et un arbre



3 zèbres et un arbre
et le texte complet de 5 pièces de Williams Shakespeare

Source : Computer networks – A. Tannebaum – 4th edition

Cryptographie quantique

- Codage de l'information quantique par la polarisation de la lumière
- Utilisé pour l'échange parfaitement sûr de clés secrètes
  - toute mesure perturbe le signal, en particulier toute écoute indiscrète
  - Protocole BB84 (C. Bennet et G. Brassard en 1984)

Plan général

- Introduction
- Principes de Bases de la Sécurité de l'Information
- Cryptographie
- Sécurité des Réseaux
- Sécurité des Applications
- Politique de sécurité
- Conclusion