Introduction à la cryptographie

Informations générales

- Laurence Herbiet
  - Institut de mathématique (B37) – 0/8
  - 04/366.26.02
  - laurence.herbiet@ulg.ac.be
  - http://montefiore.ulg.ac.be/~herbiet/sco.html

Organisation du cours

- Organisation :
  - Cryptographie (± 7 semaines) – L. Herbiet
  - Systèmes d'exploitation – T.A. Banh
- Examen :
  - Cryptographie (50%) : Une question parmi les questions proposées sur le site du cours
  - Systèmes d'exploitation (50%) :
    - Soit un travail sur un sujet relatif aux O.S. (voir Mr Banh)
    - Soit une des questions parmi la liste des questions proposées sur le site du cours

Références

- **Cryptography : Theory and practice (2e edition)** – *Douglas Stinson* – CRC Press, 2002 – [Stinson]
- **Cryptography and Network Security (3e edition)** – *William Stallings* – Prentice Hall,2002 – [Stallings]
- **Les protocoles de sécurité d'internet** – *Stephane Natkin* – Dunod, 2001 – [Natkin]
- **Applied Cryptography** - *B. Schneier-* John Wiley & Sons, 1996
- Tutoriel simple de cryptographie : www.uqtr.ca

Cryptographie

(© Pour la Science N.269 mars 2000)

Programme

- Cryptographie :
  - Cryptographie classique
  - Rappels mathématiques
  - Chiffrement symétrique/asymétrique – hashage
- Protocoles de sécurité
  - SSL, IPSEC, SET, PGP
  - Systèmes sécurisés
  - …

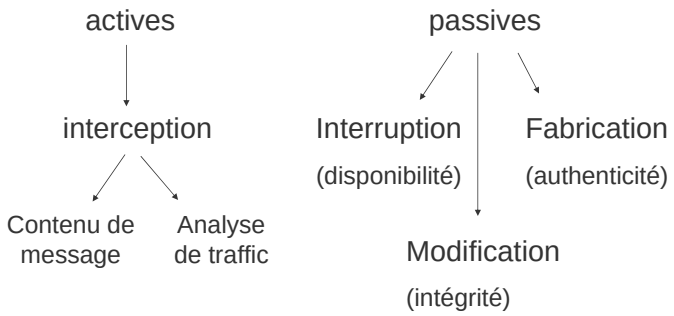
Introduction

Motivation

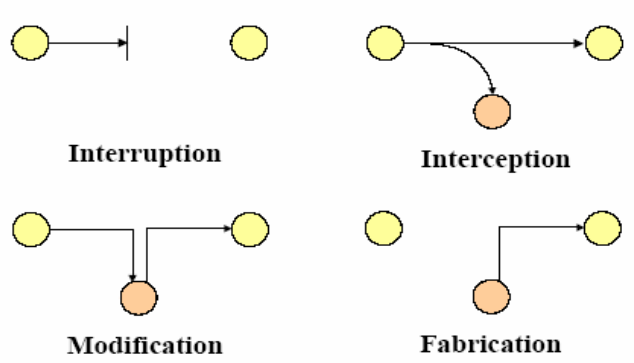
Besoin en sécurité de l'information

- Utilisation répandue du matériel informatique
  → sécurité informatique
- Utilisation répandue des réseaux informatiques et des systèmes distribués
  → sécurité réseau

Menaces réseau



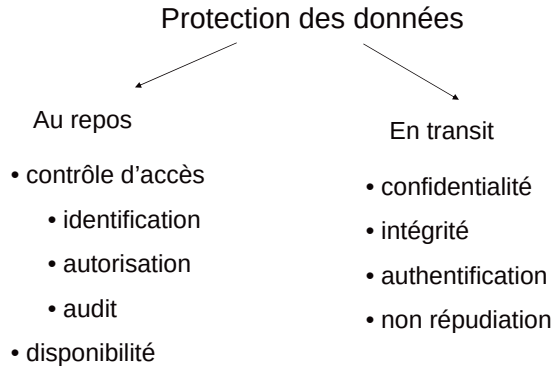
Menaces réseau (2)



Attaqueurs potentiels

- Les hackers
- Les concurrents industriels
- Les espions
- La presse
- Les agences nationales
- …

Services de sécurité attendus

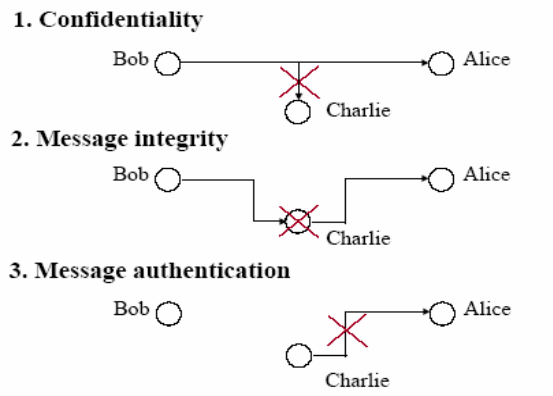


Identification (authentification utilisateur)

Sur base de

- Ce que vous savez
  - Mots de passe, PINs, …
- Ce que vous avez
  - Carte magnétique, carte à puces, …
- Ce que vous êtes
  - Empreintes digitales, voix, signatures, scanner rétinien, …

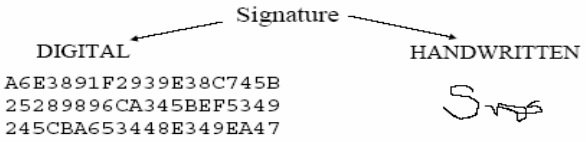
Services de base



Services de base (2)

4. Non-repudiation
- of sender - of receiver - mutual

Technique: *digital signature*



- But principal :
  - Identification unique
  - preuve d'accord sur le contenu du document

Signatures manuelles et digitales

- Points communs

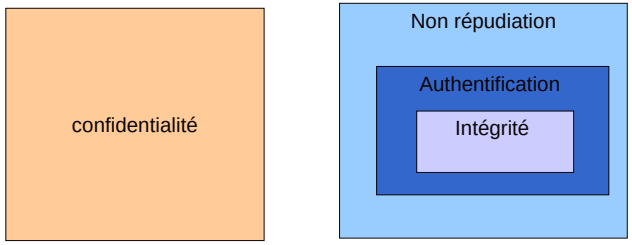
Signatures digitales	Signatures manuelles
1. unique	
2. Impossible à forger	
3. impossible à répudier de la part de son auteur	
4. facile à vérifier par un tiers	
5. facile à générer	

Signatures manuelles et digitales

- Différences

Signatures digitales	Signatures manuelles
6. Possibilité de la stocker et de l'envoyer indépendamment du document	6. associée physiquement avec le document
7. fonction du document	7. identique pour tous les documents
8. couvre l'entièreté du document	8. habituellement à la dernière page

Relations entre ces services

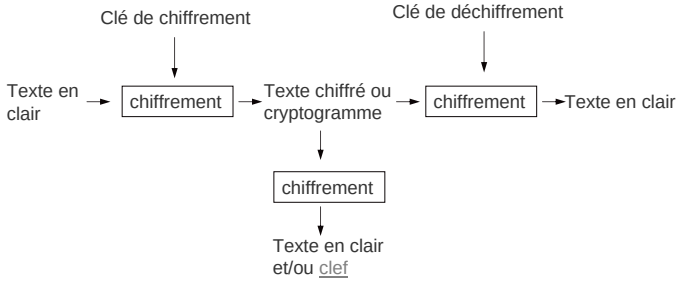


Introduction

Vocabulaire de base

Vocabulaire de base

- Cryptologie = cryptographie + cryptanalyse
- Chiffrement, déchiffrement, décryptement



La cryptologie est une science mathématique qui comporte 2 branches : la cryptographie et la cryptanalyse.

La cryptographie traditionnelle est l'étude des méthodes permettant de transmettre des données de manière confidentielle. Afin de protéger un message, on lui applique une transformation qui le rend incompréhensible; c'est ce qu'on appelle **le chiffrement**, qui, à partir d'un texte clair, donne un **texte chiffré ou cryptogramme**. Inversement, **le déchiffrement** est l'action qui permet de reconstruire le texte en clair à partir du texte chiffré. Dans la cryptographie moderne, les transformations en question sont des fonctions mathématiques, appelées **algorithmes cryptographiques**, qui dépendent d'un paramètre appelé **clef.**

La cryptanalyse, à l'inverse est l'étude des procédés cryptographiques dans le bute de trouver des faiblesses et, en particulier, de pouvoir décrypter des textes chiffrés**. Le décryptement** est l'action consistant à retrouver le texte clair sans connaître la clef de déchiffrement.

Note : les termes « cryptage » et « crypter » sont des anglicismes, dérivés de l'anglais *to encrypt*, souvent employés incorrectement à la place de chiffrement et chiffrer.

Notation

- M : texte clair
- C : texte chiffré
- K : clé
- E(x) : fonction de chiffrement
- D(x) : fonction de déchiffrement
- Il faut évidemment :

$$M = D(E(M))$$

Algorithme - clé

- Les opérations de chiffrement/déchiffrement sont basées sur deux éléments fondamentaux:
  - Un **algorithme** cryptographique qui est une fonction mathématique réalisant ces 2 opérations.
  - Une **Clé.**

  appliqués au texte à transformer.

Principe de Kerckhoff

- Remarques importantes:
  - Aucun secret ne doit résider dans l'algorithme (principe de Kerckhoff)

    Tout le secret réside dans la clé !
  - Il convient de distinguer **Secret** et **Robustesse** de l'algorithme**.**

→ Sans K, impossible de retrouver M à partir de C

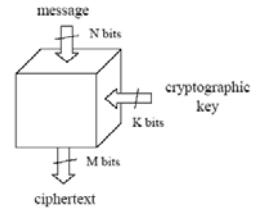
→ Si on connaît K, déchiffrement

Le principe de Kerckhoff :

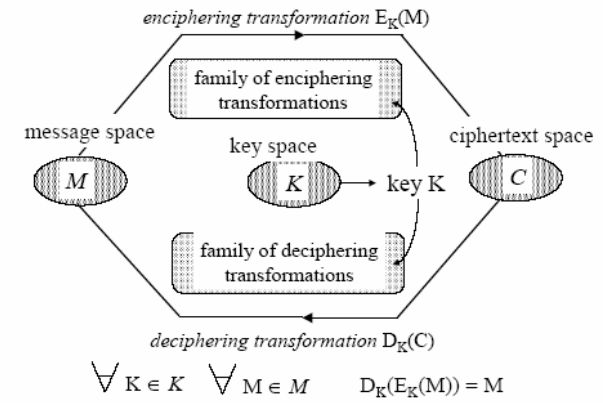
« La sécurité d'un chiffre NE DOIT PAS dépendre
de tout ce qui ne peut pas être facilement changé »
A. Kerckhoff, 1883

Cryptosystème

Un **cryptosystème** est défini comme l'ensemble des clés possibles (espace de clés), des textes clairs et chiffrés possibles associés à un algorithme donné.



Cryptosystème (définition)



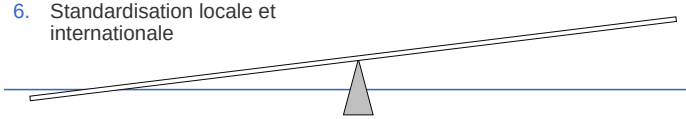
Algorithme publié vs secret

Algorithme publié

1. La seule manière fiable d'évaluer la sécurité du chiffre
2. empêche des backdoors cachées par les concepteurs
3. Grand nombre des réalisations = prix réduit + performance élevée
4. Aucun besoin de protection contre le reverse-engineering
5. Implémentations logicielles
6. Standardisation locale et internationale

Algorithme secret

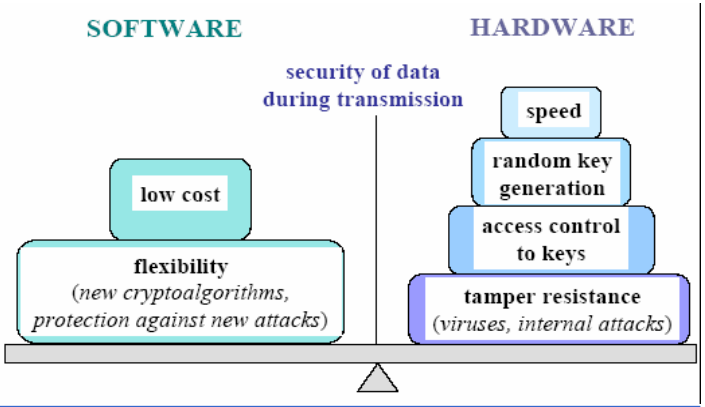
1. La cryptanalyse doit inclure la récupération de l'algorithme
2. Un plus petit nombre d'utilisateurs = une plus petite motivation à casser
3. Indisponible pour autre pays



Idée fondamentale de cryptographie

Si un bon nombre de gens futés n'ont pas résolu un problème, alors il ne sera probablement pas résolu de si tôt

Solution logicielle ou matérielle ?



Types d'applications logicielles

ELECTRONIC FUND TRANSFER - EFT

- intra-bank fund transfers
- inter-bank fund transfers
- home banking
- electronic cash

ELECTRONIC DATA INTERCHANGE - ED

- financial transactions among companies

HOME-SHOPPING

- digital goods (e.g., software)
- services (e.g., travel reservations)
- non-digital goods (e.g., books, CDs)
- micropayments (e.g., database access)

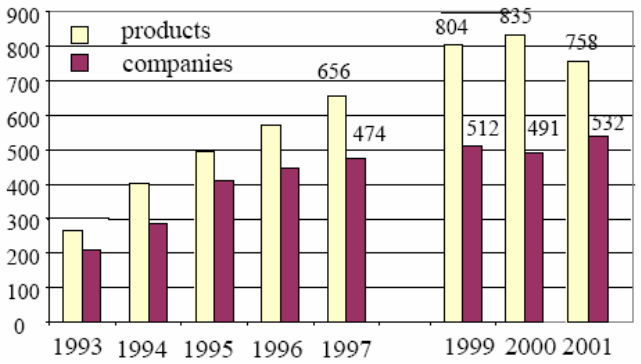
Hardware :

- Puce VLSI
- Carte PCMCIA
- Carte à puce
- Carte cryptographique
- dispositif cryptographique autonome

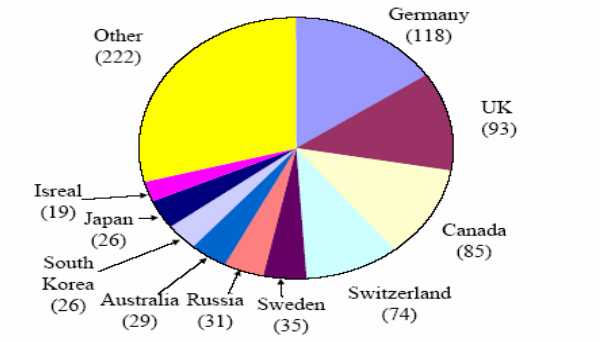
Types d'applications hardware :

- Accélérateurs de matériel pour des gateways ou des routeurs
- Communication sans fil
- Carte à puce universelle pour le commerce électronique
- Valise électronique
- Autorité de certification – centre d'enregistrement des clés publiques
- Dispositifs militaires
- Dispositifs de haute sécurité

Croissance d'utilisation de produits cryptographiques



Produits cryptographiques hors USA



Introduction

Concepts cryptographiques

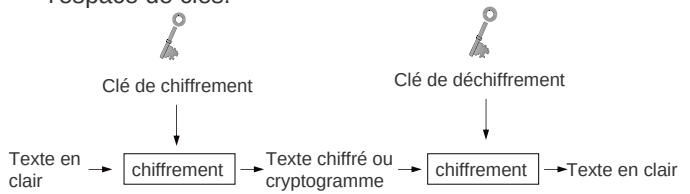
31

Suivant la nature des clés et de l'algo, on distingue deux grandes familles de cryptosystèmes:

- •Cryptosystèmes à clés symétriques
- •Cryptosystèmes à clés publiques

Cryptosystèmes à clés symétriques

- **Caractéristiques:**
  - Clés identiques: $K_E=K_D=K$
  - Clé secrète!
  - Algorithmes standards: DES, AES, …
  - **Génération des clés**: Clé choisie aléatoirement dans l'espace de clés.

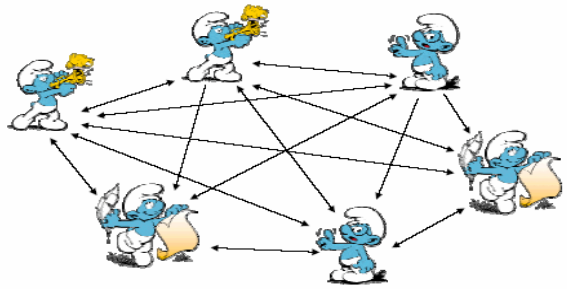


Cryptographie - 32

Cryptosystèmes à clés symétriques

- **Caractéristiques (suite):**
  - **Principe:** Algorithmes basés sur des opérations de transposition et de substitution des bits du texte clair, en fonction de la clé.
  - **Taille des clés**: (standard) 64 ou 128 bits.
  - **Performances**: Chiffrement très rapide.
  - **Distribution des clés:**
    - Opération critique.
    - Doit s'effectuer de manière sécurisée (voir manuellement).

Distribution des clés

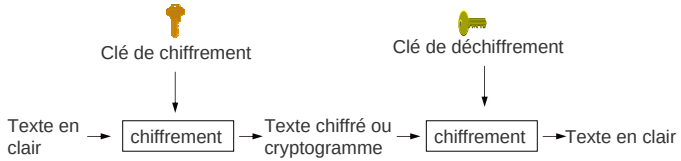


N - Users ⇨ $\frac{N \cdot (N-1)}{2}$ Keys

Users	Keys
100	5,000
1000	500,000

Cryptosystèmes à clés publiques

- **Caractéristiques:**
  - 1 Clé publique: P_K
  - 1 Clé privée: S_K (secrète)
  - **Propriétés**:
    - La connaissance de P_K ne permet pas de déduire S_K.
    - $D_{P_k}(E_{S_k}(M)) = M$
  - Algorithmes standards: RSA, DH



Cryptosystèmes à clés publiques

- **Caractéristiques (suite):**
  - **Principe:**
    - Fonction unidirectionnelle à trappe.
      - "Facile" à calculer dans un sens. "Difficile" à inverser.
      - Sauf si on connaît une info secrète (la trappe)
    - Algorithmes basés sur des opérations d'exponentiation en algèbre modulo.
  - **Exemple : f := Y = f(X) = A^X mod P**
    - Où A et P sont constants, P est un grand nombre premier et A est un entier plus petit que P

Number of bits of P	Average number of multiplications necessary to compute	
	f	f^{-1}
1000	1500	10^{30}

TRAPPES

Il existe parfois ce que l'on nomme des "trappes" dans le clés publiques et secrètes. Ceci est du au fait que lors de la génération de la clé, qui doit se faire aléatoirement en respectant certaines contraintes théoriques prédéfinies, le générateur aléatoire a un défaut (parfois le défaut est volontaire de la part du fournisseur… espionnage oblige).

Dans les clés secrètes, les trappes se situent au niveau de l'entropie de la clé, directement liée à l'entropie du générateur aléatoire. On définit l'entropie d'un générateur de clés par le nombre moyen optimal de questions binaires (c'est-à-dire donnant lieu à des réponses du type oui/non) qu'il faut poser à quelqu'un connaissant une clé produite par ce générateur, pour la déterminer. Plus l'entropie d'un générateur de clé est élevée, plus il faut de questions pour déterminer cette clé. A l'inverse, plus l'entropie est faible, moins il faut de questions, de sorte que la recherche d'une clé est facilitée. L'entropie d'un générateur de clés de *n* bits n'excédera donc jamais *n* mais pourra cependant y être inférieure.

L'introduction de trappes dans les clés de systèmes asymétriques est beaucoup plus difficile, puisque ce type de clé possède déjà une structure mathématique intrinsèque: leur constructions n'est pas due au hasard, mais résulte de règles mathématiques. Le hasard est ici dans le choix des grands nombres premiers utilisés. Si le générateur aléatoire qui engendre ces nombres est biaisé (voir la définition de ce terme dans la section probabilités du site), ce biais facilitera la recherche des nombres premiers ayant servi à l'élaboration de la clé qu'un attaquent tente de casser.

Cryptosystèmes à clés publiques

- **Caractéristiques (suite):**
  - **Génération des clés**:
    - A partir de grands nombres premiers PK = f(SK) mais le calcul de SK = f^{-1}(PK) est impossible.
  - **Taille des clés**: (standard) 512 ou 1024 bits.
  - **Performances**: Chiffrement de l'ordre de 1000 fois plus lent que les algorithmes à clés symétriques.
  - **Nombre de clés:** (si n entités) : n paires.
  - **Distribution des clés:**

    Facilitée car pas d'échange de clés secrètes nécessaires:

    - La clé secrète est conservée par les entités.
    - Seule la clé publique est échangée.

Algorithmes de hashage

- 3ème grande famille d'algorithmes utilisés en cryptographie.
- **Principe:**
  - Ces algorithmes convertissent un texte original de longueur quelconque en un message de longueur fixe (en général de longueur inférieure).
- **Utilisation** en cryptographie.
  - Le but est d'utiliser le message haché comme empreinte digitale du message original qu'il identifie de manière univoque.

Algorithmes de hashage

- A cet effet, on utilise des algorithmes de hashage:
  - *Unidirectionnels - Sans collisions*
  - *En effet, il est pratiquement impossible :*

Etant donné	De trouver
H(m)	m
H(m) et m	m' ≠ m tel que h(m') = h(m)
	m' ≠ m tel que h(m') = h(m)

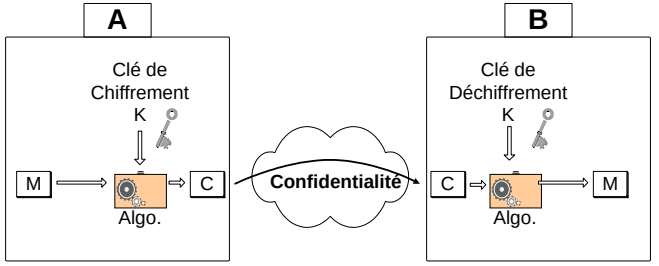
Protocoles cryptographiques

- Dès que plusieurs entités sont impliquées dans un échange de messages sécurisés, des règles doivent déterminer l'ensemble des opérations cryptographiques à réaliser, leur séquence, afin de sécuriser la communication
- C'est ce que l'on appelle les **protocoles cryptographiques.**
- Que signifie sécuriser un échange?
  - Les 3 propriétés fondamentales sont:
    Confidentialité – Authentification – Intégrité

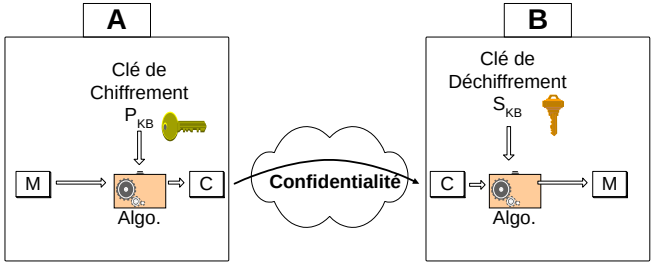
Protocoles cryptographiques

- **Confidentialité**
  - A l'aide de cryptosystèmes à clés symétriques.
    - La même clé secrète est utilisée pour E(M) et D(C)
    - Echange préalable et sécurisé de la clé K entre A et B.
  - A l'aide de cryptosystèmes à clés publiques.
    - Chaque entité possède sa paire de clés P_{KA}, S_{KA}/ P_{KB}, S_{KB}.
  - A l'aide de cryptosystèmes hybrides.
    - Cryptosystème à clés publiques pour l'échange confidentiel de la clé (de session) K.
    - Cryptosystème à clés symétriques pour l'échange confidentiel du message.

Confidentialité – système symétrique

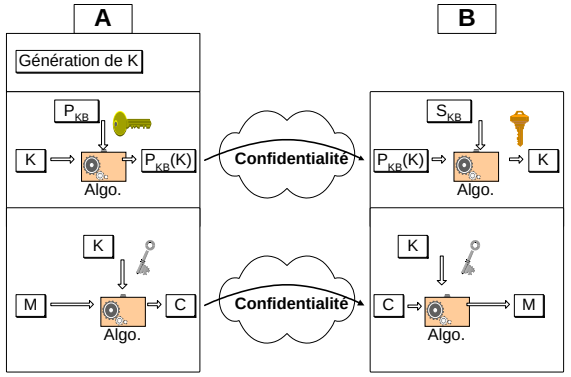


Confidentialité – système asymétrique



Idée : chiffrer avec la clé publique de B ainsi seul B peut déchiffrer le message.

Confidentialité – système hybride



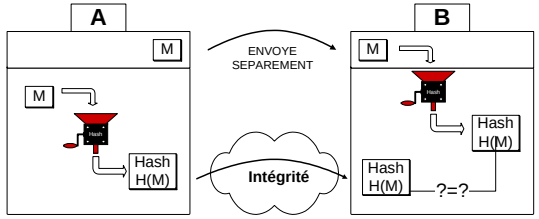
Hybride : les systèmes asymétriques sont très lourds et très lents même si ce sont les plus sûrs. L'idée est d'échanger une clé de session (symétrique) par le biais d'un échange asymétrique. Ensuite, on continue les communications avec cette clé de session.

Avantages d'un système hybride

	logiciel	matériel
$\frac{\text{Vitesse de déchiffrement du 3DES}}{\text{Vitesse de déchiffrement du RSA-1024}}$	$\simeq$ 100	$\simeq$ 1000

Protocoles cryptographiques

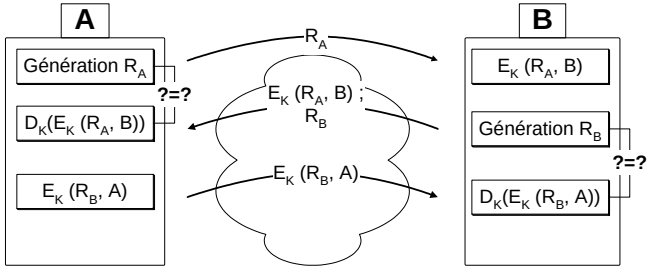
- **Intégrité du message.**
  - Vérification qu 'un message n 'a pas été altéré durant la communication.
  - A cette fin, on utilise les fonctions de *hashage.*



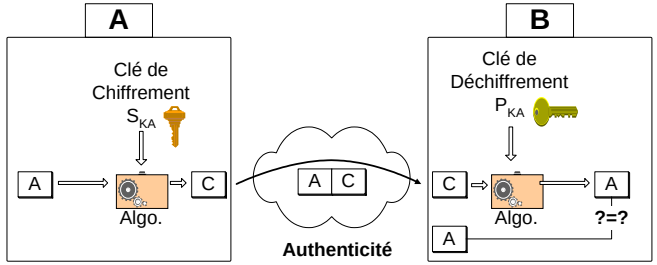
Protocoles cryptographiques

- **Authentification.**
  - **Des parties de la communication.**
    - A l 'aide d'un cryptosystème à clés symétriques.
      - Si on suppose que A et B partagent une même clé secrète K
    - A l 'aide d'un cryptosystème à clés publiques.
      - Chaque partie possède une paire de clés publique/privée (PKA/SKA, PKB/SKB).

Authentification des parties - symétrique



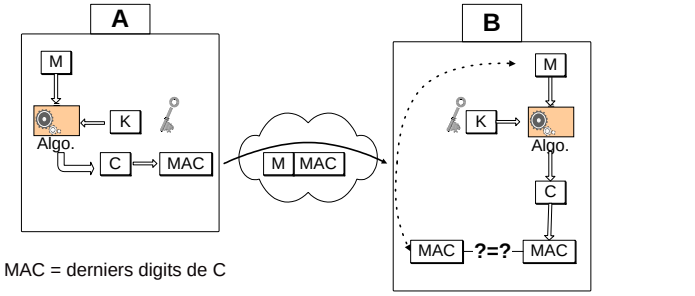
Authentification des parties - symétrique



Protocoles cryptographiques

- **Authentification (suite).**
  - **Du message.**
    - **A l'aide d'un MAC (Message Authentication Code).**
      - Un MAC peut-être généré de deux manières:
        - A l 'aide d 'un cryptosystème symétrique.
        - A l 'aide d 'une fonction de hashage.

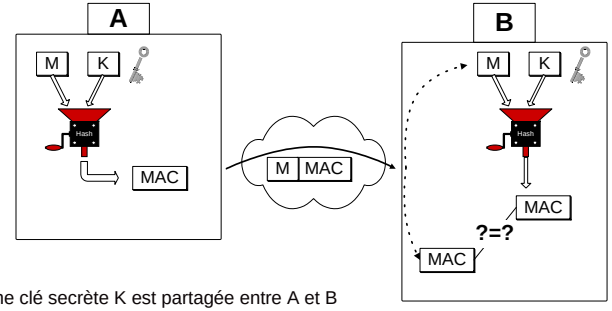
Authentification message – MAC – Sym.



MAC = derniers digits de C

Authentification grâce à K + Intégrité

Authentification message – MAC – Hash



Une clé secrète K est partagée entre A et B

Authentification grâce à K + Intégrité

Protocoles cryptographiques

- **Authentification (suite).**
  - **Du message.**
    - **A l 'aide d'un MAC (Message Authentication Code).**
    - **A l 'aide d'une signature digitale.**
      - Les signatures digitales doivent posséder les propriétés suivantes:
        1. Authentique.;
        2. Infalsifiable;
        3. Non-réutilisable;
        4. Inaltérable;
        5. Non-répudiable.

Avec un système symétrique :

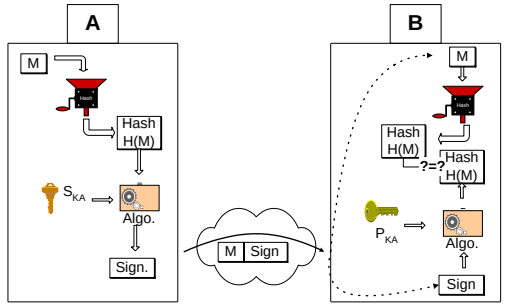
Les deux côtés correspondants ont la même information et peuvent produire une signature

→ **Il y a une possibilité pour**

Le récepteur de falsifier le message

L'expéditeur de nier qu' il/elle a envoyé le message

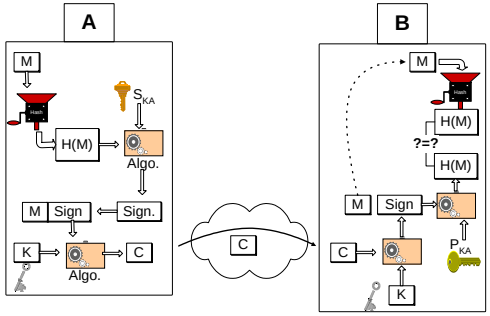
Signature digitales avec clé publique



Seul A a pu composer Sign

Protocoles cryptographiques

- **Authentification+Confidentialité**



Cryptanalyse

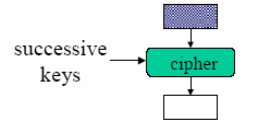
- Etude des mécanismes théoriques ou techniques visant à briser un algorithme de chiffrement.
  C'est à dire, retrouver le message M à partir de C, sans connaître la clé K à priori.
- On parle dans ce cas d'une "attaque" cryptanalytique.

Cryptanalyse des systèmes symétriques

1. Attaque sur le texte chiffré uniquement
   - Etant donné
     - Un texte chiffré
   - On recherche
     - Le texte clair et/ou
     - La clé
   - Technique
     - Analyse de fréquence des lettres dans le message (présence de 'e', …)
     - Ne fonctionne que pour la plupart des chiffrements classiques de base

Cryptanalyse des systèmes symétriques

2. Attaque sur le texte clair connu
   - Etant donné
     - Un texte chiffré
     - Un fragment deviné de texte clair
   - On recherche
     - Le texte clair restant
     - Et/ou la clé
   - Technique
     - Attaque par 'force brute' : on essaie toutes les clés

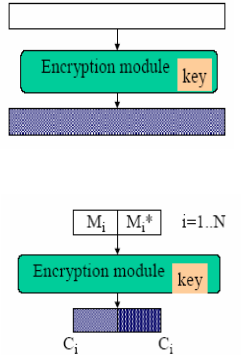


Performances

Key Size (bits)	Number of Alternative Keys	Time required at 1 encryption/μs	Time required at 10^6 encryptions/μs
32	$2^{32} = 4.3 \times 10^9$	$2^{31}\ \mu s = 35.8$ minutes	2.15 milliseconds
56	$2^{56} = 7.2 \times 10^{16}$	$2^{55}\ \mu s = 1142$ years	10.01 hours
128	$2^{128} = 3.4 \times 10^{38}$	$2^{127}\ \mu s = 5.4 \times 10^{24}$ years	5.4×10^{18} years
168	$2^{168} = 3.7 \times 10^{50}$	$2^{167}\ \mu s = 5.9 \times 10^{36}$ years	5.9×10^{30} years
26 characters (permutation)	$26! = 4 \times 10^{26}$	$2 \times 10^{26}\ \mu s = 6.4 \times 10^{12}$ years	6.4×10^6 years

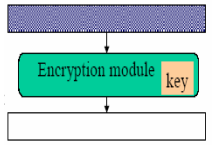
Cryptanalyse des systèmes symétriques

3. Attaque sur un texte clair sélectionné
   - Etant donné
     - La capacité de chiffrer un fragment de texte clair choisi arbitrairement
   - On recherche
     - La clé
   - Technique
     - Cryptanalyse différentielle



Cryptanalyse des systèmes symétriques

4. Attaque sur un texte chiffré sélectionné
   - Etant donné
     - La capacité de déchiffrer un fragment de texte chiffré choisi arbitrairement
   - On recherche
     - La clé



Évolution de la cryptologie