

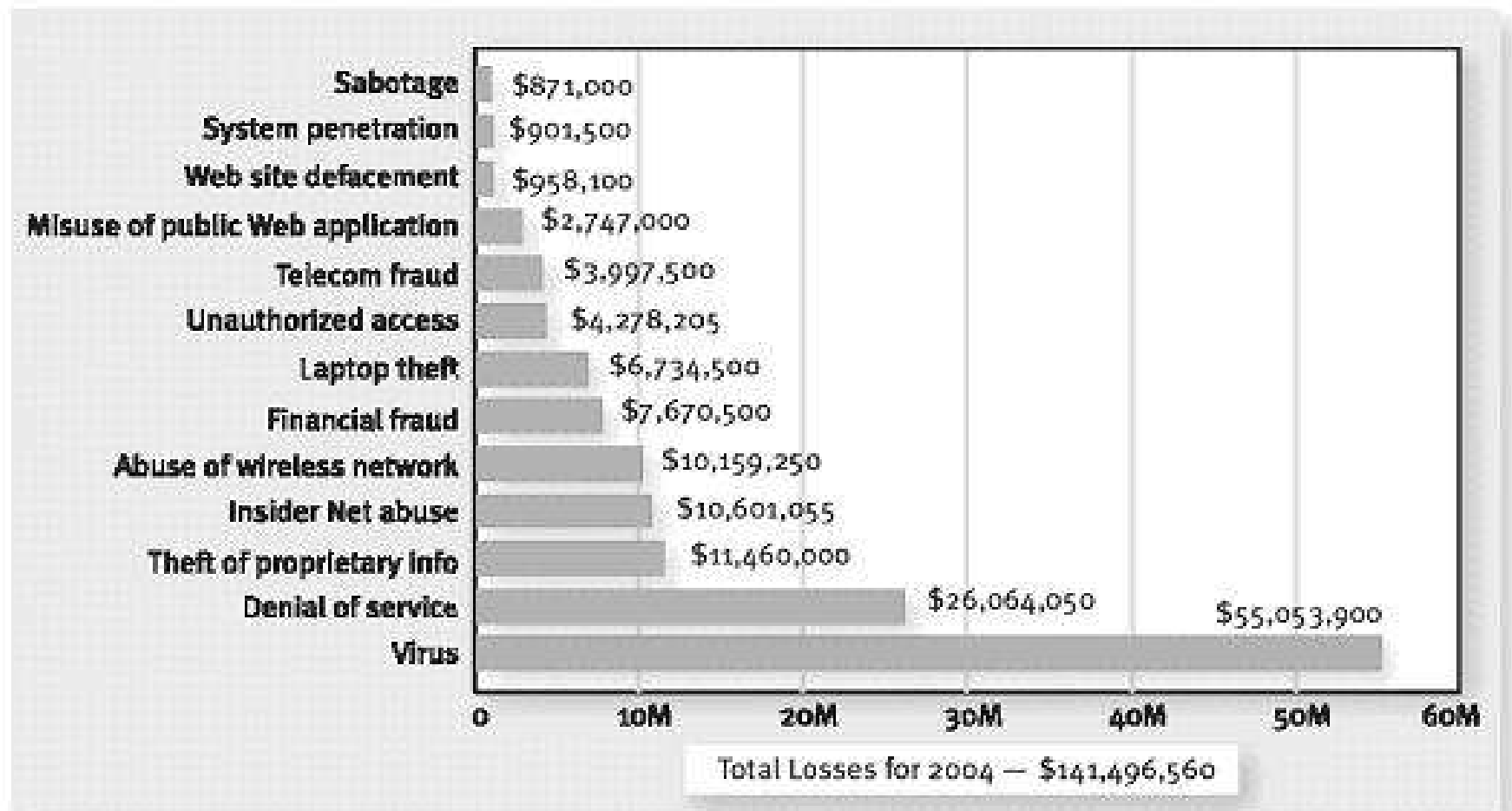


Sécurité de l'information

Tunis, 22 Juin 2005

aalain@trstech.net

Introduction(1)



CSI/FBI 2004 Computer Crime and Security Survey
Source: Computer Security Institute

2004: 269 Respondents

Introduction(2)



- ❑ Le changement majeur ayant affecté la sécurité est l'introduction des systèmes distribués, l'utilisation des réseaux et outils de communication pour transporter des données entre les terminaux et les ordinateurs et entre ordinateurs.

- ❑ Des mesures de sécurité réseau sont nécessaires:
 - ❑ Pour protéger les données pendant les transmissions
 - ❑ Pour contrôler l' accès aux données

Exemples de Violations de Sécurité(1)



□ A envoie un fichier à B. Le fichier contient des données sensibles (la paye).

C non autorisé à lire le fichier écoute la transmission et prend une copie du fichier.

Exemples de Violations de Sécurité(2)

- Une application d'administration réseau D, envoie un message à un ordinateur E, sous son contrôle. Le message instruit E de mettre à jour son fichier d'autorisation pour inclure les identités de nouveaux utilisateurs .
F intercepte le message, change le contenu, l'envoie à E qui l'accepte comme message venant de D.

Exemples de Violations de Sécurité(3)



- Au lieu d'intercepter le message, F construit son propre message et l'envoie à E comme message venant de D.

E accepte le message et met à jour son fichier.

Exemples de Violations de Sécurité(4)

- Un employé est viré sans préavis.

Le DAF envoie un message à un serveur pour invalider le compte de l'employé. Après invalidation du compte, un message doit être posté au dossier de l'employé en guise de confirmation. L'employé intercepte le message, le retarde aussi longtemps qu'il lui faut pour accéder au serveur et copier des informations sensibles.

Exemples de Violations de Sécurité (4) Suite



Le message est transmis, l'action exécutée et l'accusé posté. L'action de l'employé pourrait passer inaperçu pendant un bon moment.

Exemples de Violations de Sécurité(5)



- Un message est envoyé à un gestionnaire de compte à la bourse des valeurs pour des transactions. Les investissements sont perdus et le client nie avoir envoyé le message.

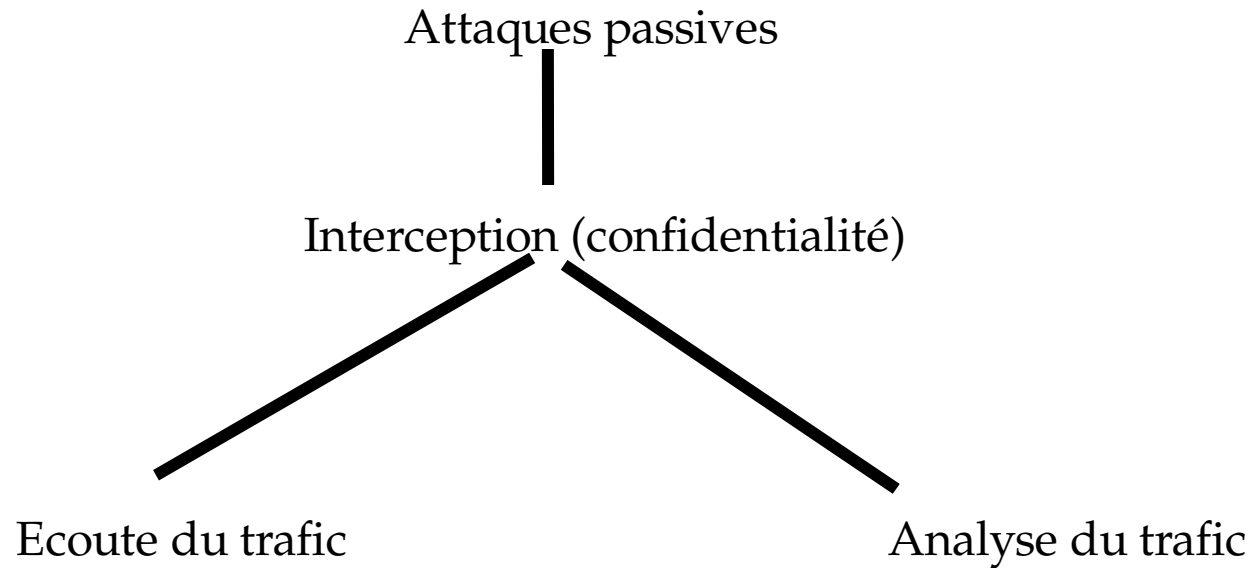


Risques et Menaces

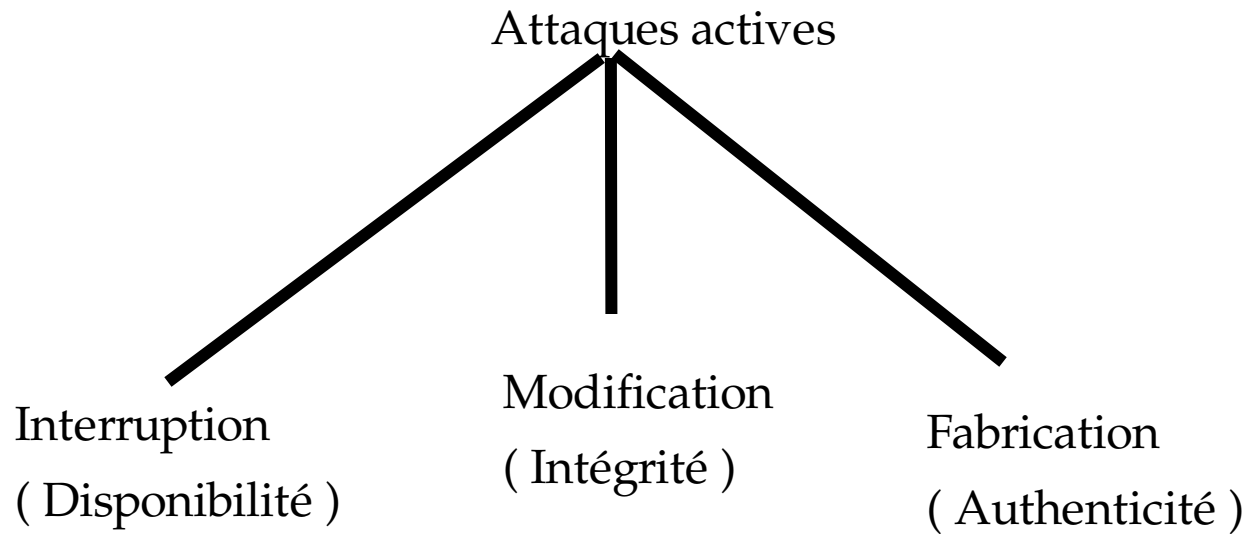
Risques et Menaces

- ❑ Une façon d'aborder le concept de sécurité de l'information est de considérer les aspects suivants:
 - ❑ Les attaques
 - ❑ Toutes les actions qui peuvent compromettre la sécurité d'une information.
 - ❑ Les mécanismes de sécurité
 - ❑ Des mécanismes conçus pour détecter, prévenir, ou réparer les effets d'une attaque.
 - ❑ Les services de sécurité
 - ❑ Des services qui consolident la sécurité des données et des transferts.
 - ❑ Les services sont faits pour bloquer les attaques. Ils utilisent un ou plusieurs mécanismes pour fournir le service.

Attaques(1)



Attaques(2)



Services de Sécurité(1)



Une classification utile des services de sécurité est la suivante :

❑ Confidentialité

- ❑ Protection des données transmises contre les attaques passives

❑ Authentification

- ❑ Assurer l'authenticité des communications.
- ❑ Permettre au destinataire de vérifier l'authenticité de l'expéditeur
- ❑ Dans le cadre d'une transaction, permettre aux parties de vérifier l'authenticité de leur interlocuteur.

Services de Sécurité(2)



□ Intégrité

- S'assurer que les messages sont reçus tels quels sont envoyés
 - Sans duplication, Insertion, Modification, changement d'ordre et retransmission.

□ Disponibilité

- S'assurer que l'information est disponible et accessible par les utilisateurs légitimes

Services de Sécurité(3)



Non reniement

- Empêcher l'émetteur ou le destinataire de nier la transmission ou la réception d'un message.

Contrôle d'accès

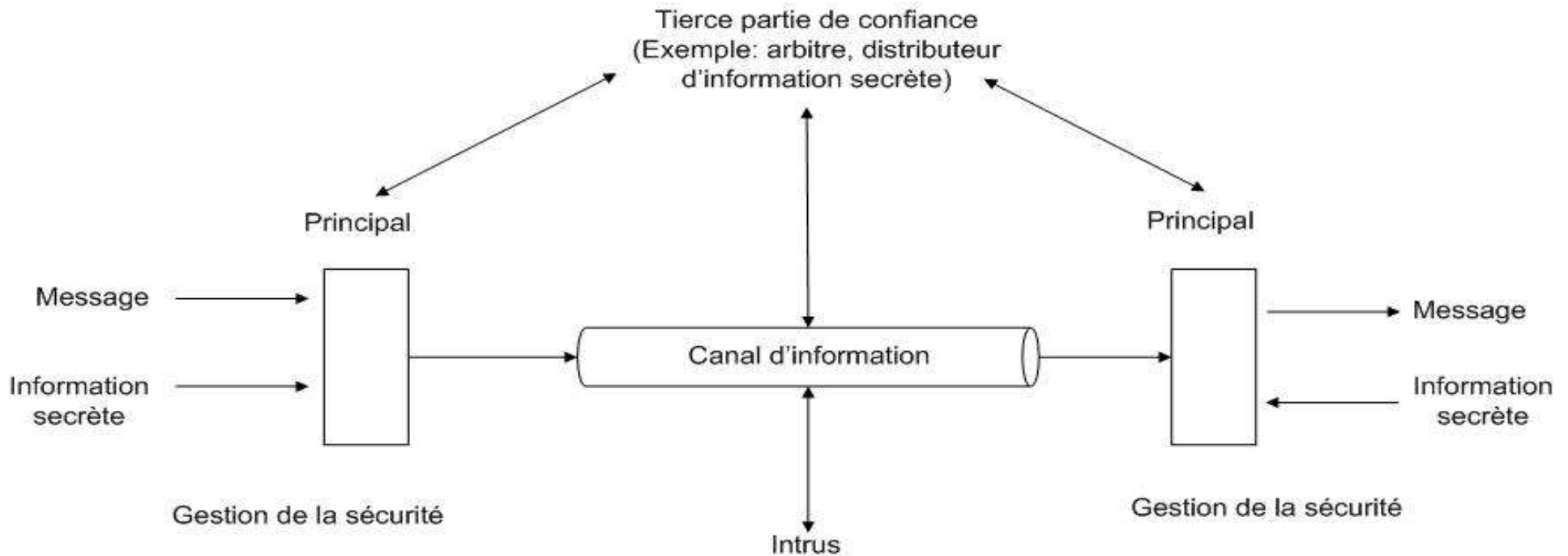
- Limiter et Contrôler l'accès aux systèmes et applications via les canaux de communication.
- Identifier, authentifier les accès.

Mécanismes de Sécurité

- ❑ Il n'existe pas un simple mécanisme qui fournit les services de sécurité ci-dessus.
- ❑ Cependant, un élément particulier est à la base de la plupart des mécanismes de sécurité :

Les Techniques de cryptographie

Modèle de Sécurité(1)

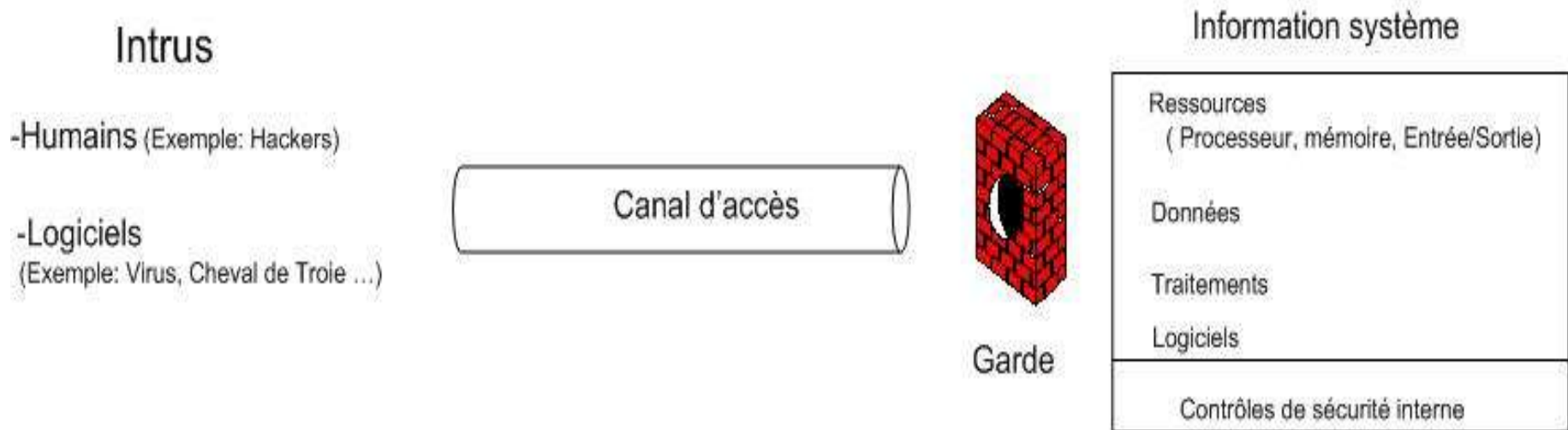


Modèle de Sécurité(2)

- ❑ Ce modèle indique les quatre(4) tâches dans la conception d'un service de sécurité :
 - ❑ 1- Concevoir un algorithme pour la transformation sécuritaire
 - ❑ 2- Générer le code secret à utiliser avec l'algorithme
 - ❑ 3- Développer une méthode de distribution et de partage du code secret
 - ❑ 4- Spécifier le protocole à utiliser par les deux parties pour mettre en œuvre l'algorithme

Modèle de Sécurité(3)

L'autre modèle de sécurité est le modèle de sécurité des accès réseau.



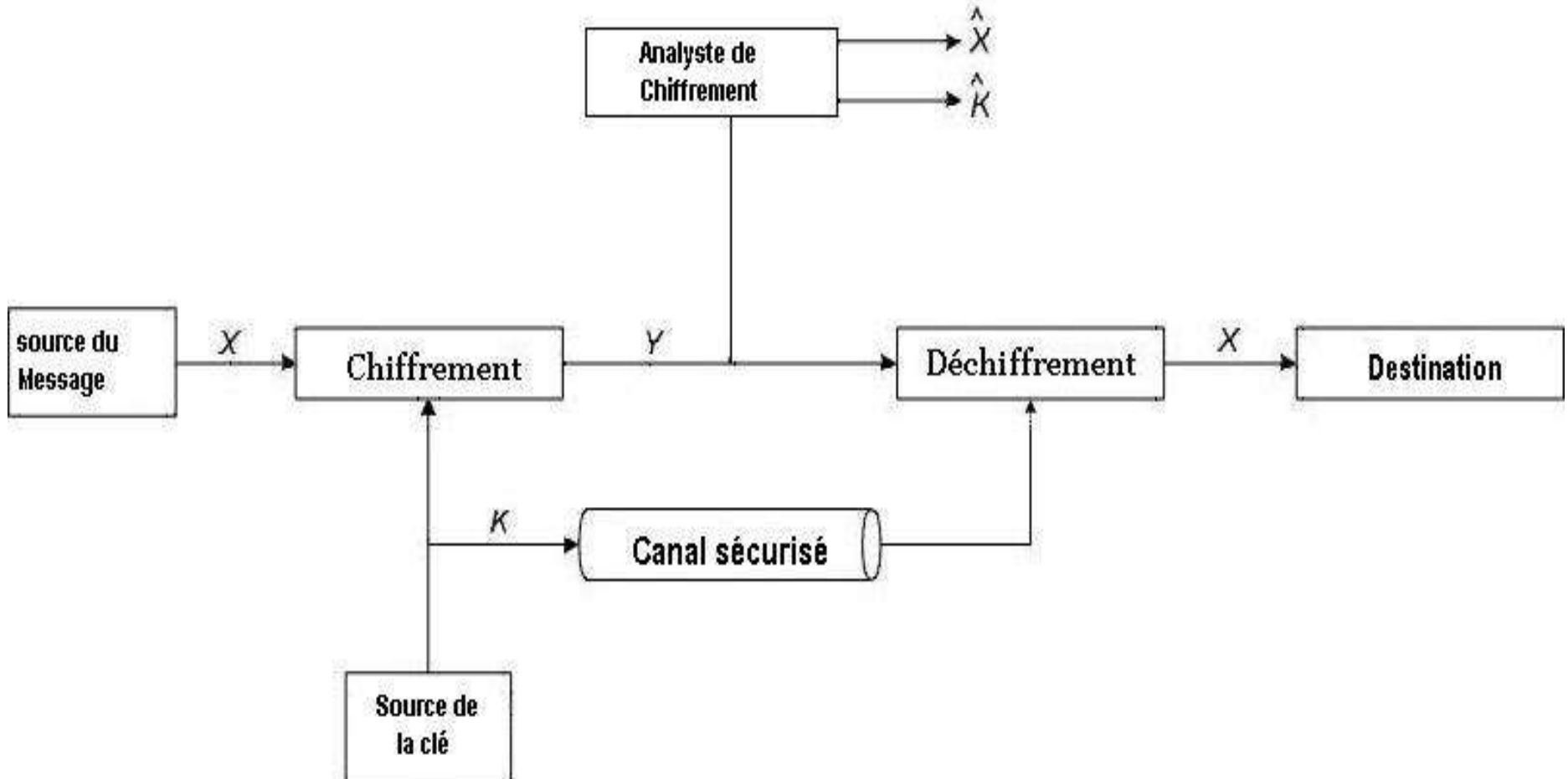


Chiffrement et Déchiffrement

Chiffrement et Déchiffrement

- Il existe deux types de techniques de chiffrement
 - Chiffrement convention ou symétrique
 - Les deux parties doivent partager une clé secrète
 - Utilise les techniques de substitution et de permutation
 - Problème de distribution de la clé secrète
 - Chiffrement à clé publique ou asymétrique
 - Utilise deux clés: une publique et une secrète
 - Utilise des techniques mathématiques
 - Règle le problème de distribution de clé
 - Peut servir à faire les signatures digitales

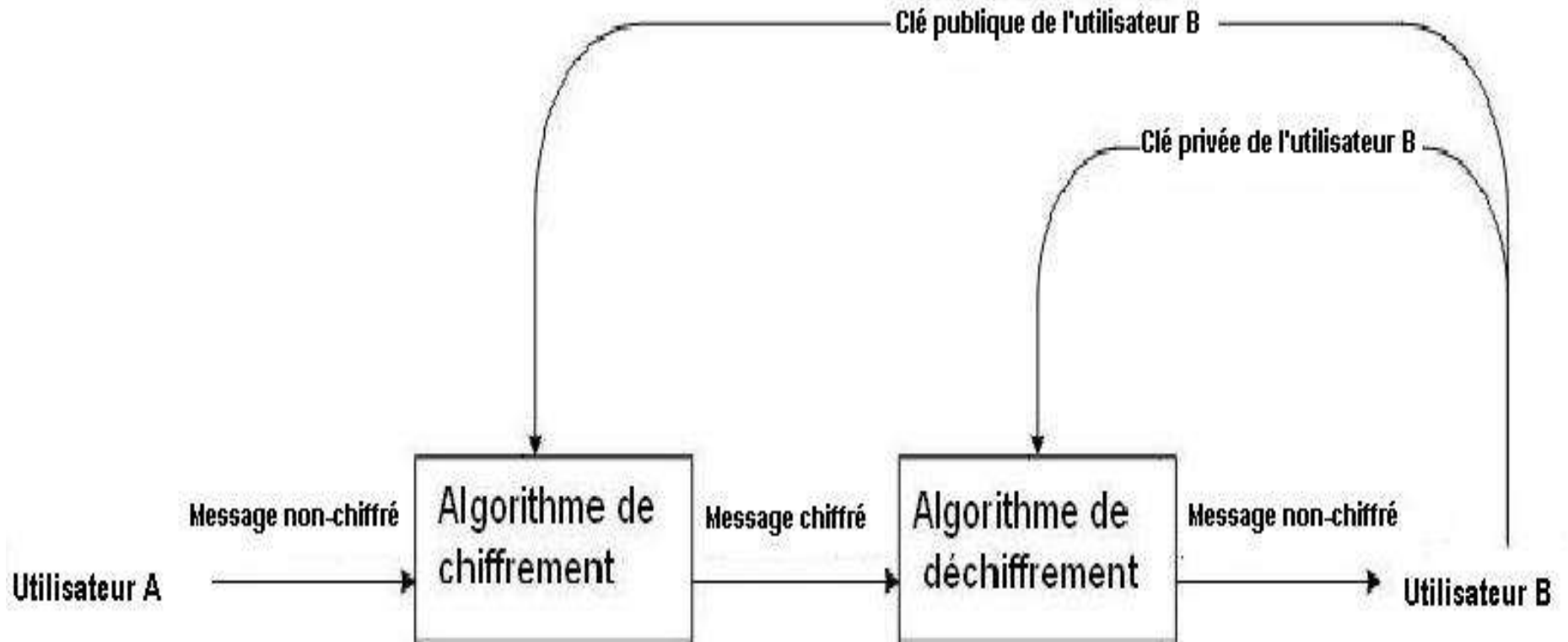
Modèle du Chiffrement symétrique



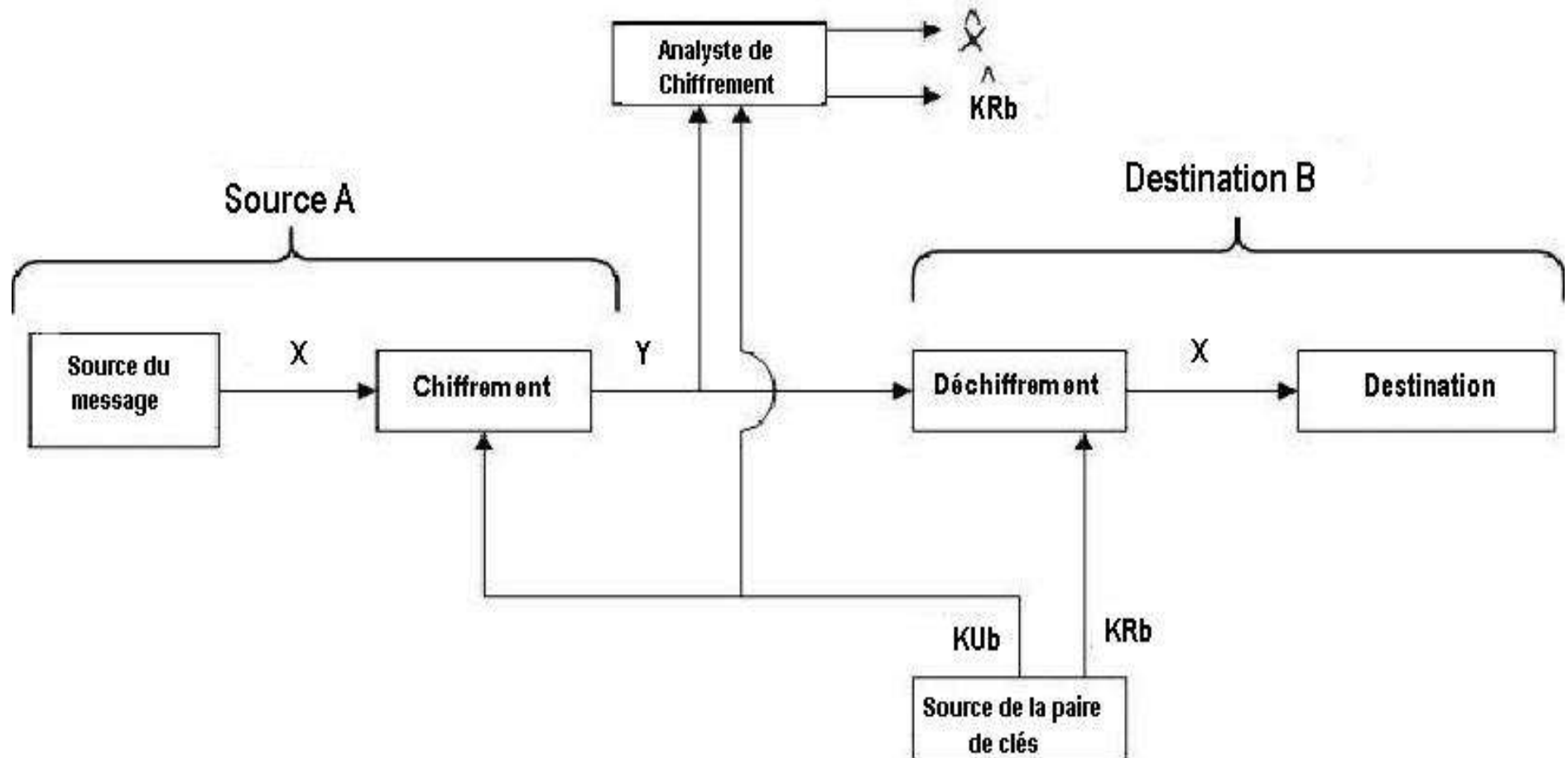
Algorithmes de chiffrement symétrique

Algorithme	Taille de la clé
DES	56 bits
Triple DES	112 ou 168 bits
IDEA	128 bits
Blowfish	Jusqu'à 448 bits
RC5	Jusqu'à 2048 bits
CAST-128	40 à 128 bits
AES	128bits, 192 bits et 256 bits

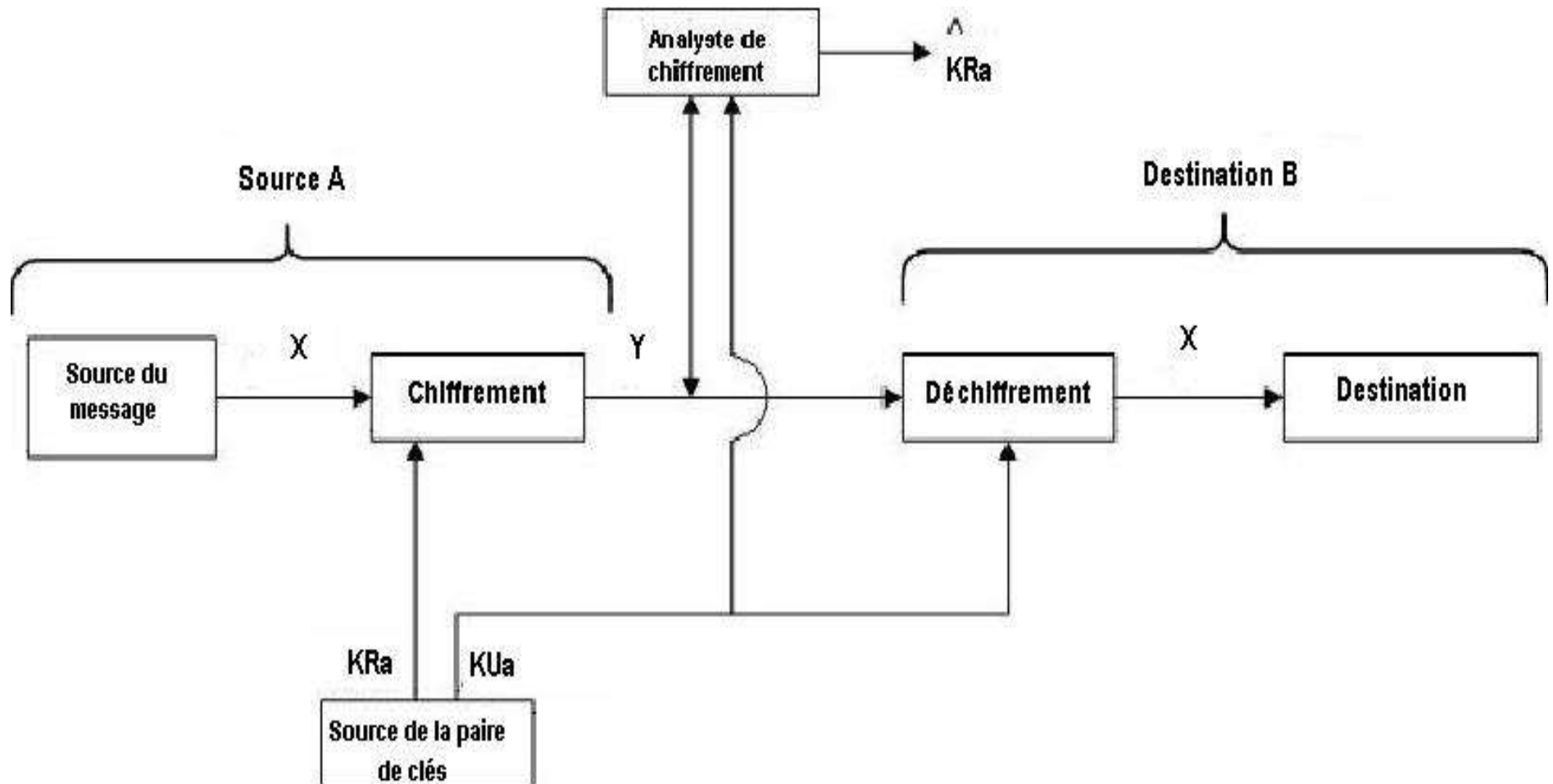
Modèle de Chiffrement asymétrique



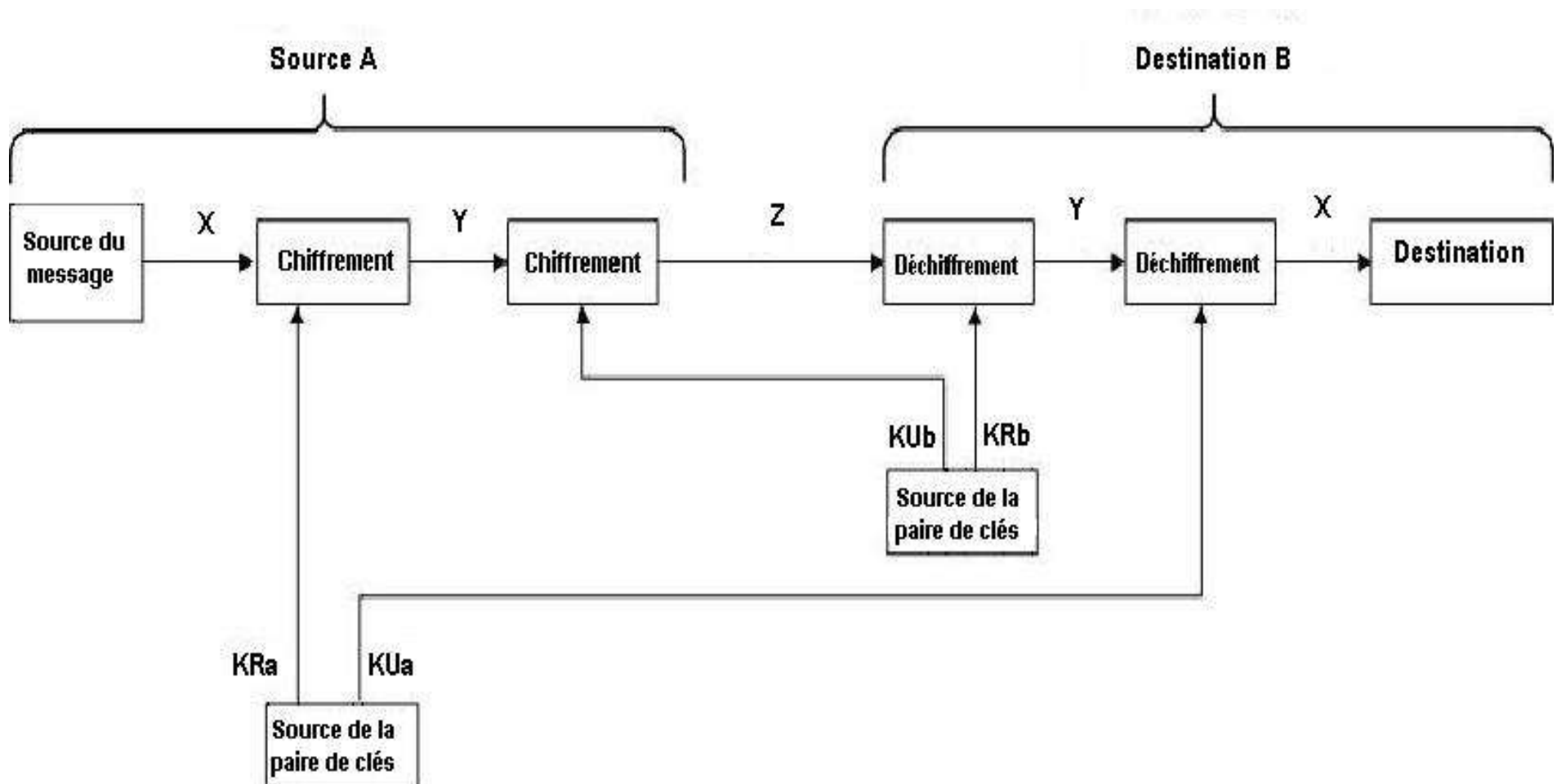
Chiffrement asymétrique: confidentialité



Chiffrement asymétrique: authentification



Chiffrement asymétrique : Confidentialité et authentification



Utilisation du Chiffrement à Clé Publique

- ❑ L'un des rôles majeurs du Chiffrement asymétrique est la distribution des clés de chiffrement symétrique.
- ❑ Deux conditions sont à remplir pour l'utilisation du Chiffrement asymétrique à cet effet.
 - ❑ La distribution des clés publiques
 - ❑ L'authentification des clés publiques

Distribution des clés publiques



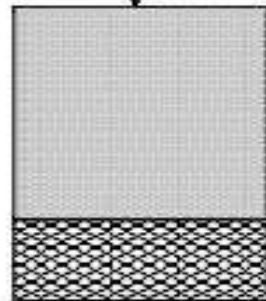
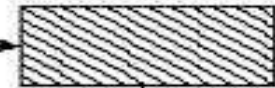
- ❑ Annonces publiques
- ❑ Annuaire publique
- ❑ Autorité de clés publiques
- ❑ Certificats de clés publiques

Certificat de clés publiques

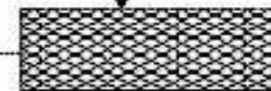
Certificat non signé:
Contient l' ID utilisateur,
la clé publique utilisateur



Génération d'un code haché
du certificat non signé

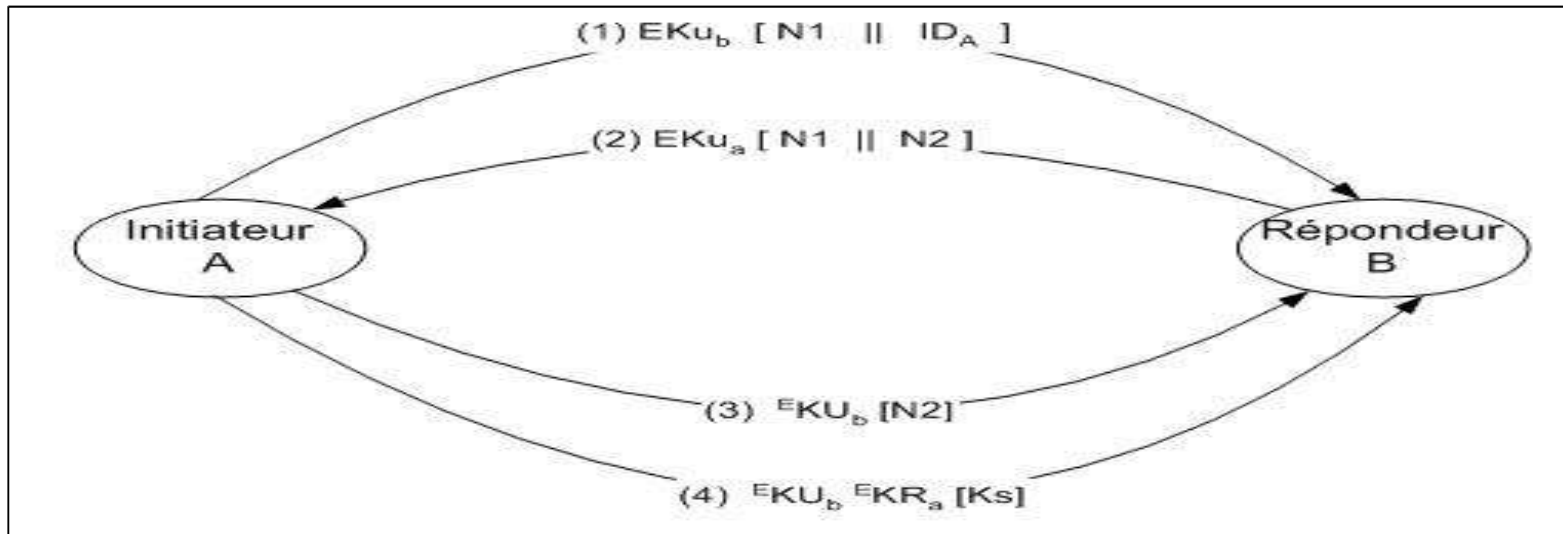
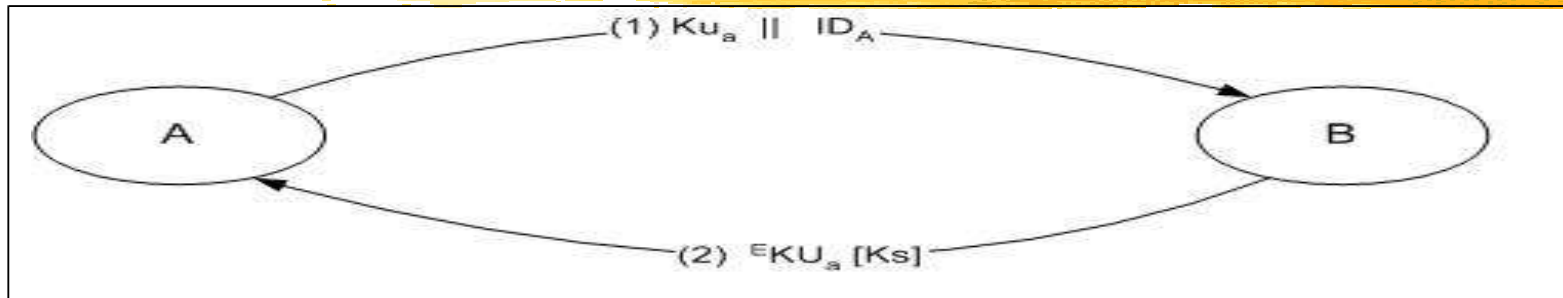


Chiffrement du code haché
avec clé privée du CA pour
former la signature



Certificat signé:
Le sujet peut vérifier la signature
utilisant la clé publique du CA.

Distribution de clés secrètes par clés publiques



Algorithmes de chiffrement à Clé Publique

Algorithme	Chiffrement Déchiffrement	Signature digitale	Echange de clés
RSA	OUI	OUI	OUI
Diffie-Hellman	NON	NON	OUI
DSA	NON	OUI	NON
Elliptic Curve	OUI	OUI	OUI



Mécanismes d'authentification

Mécanismes d'Authentification(1)

- ❑ Le chiffrement protège contre les attaques passives.

- ❑ La protection contre les attaques actives requiert l'authentification des messages et des connexions.
 - ❑ Vérifier que le message vient de la source annoncée et n'a pas été modifiée
 - ❑ Vérifier l'ordre des messages et leur âge

- ❑ La signature digitale est une technique d'authentification qui inclut des mesures de lutte contre le reniement.

Mécanismes d'Authentification(2)

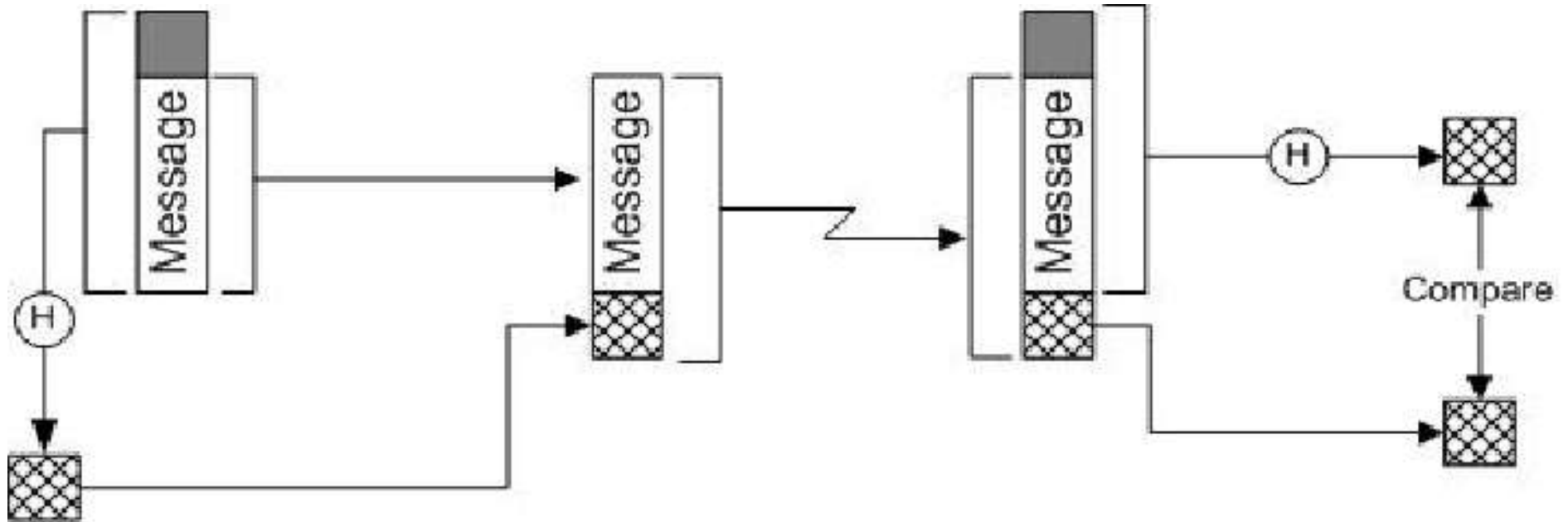
- ❑ Authentification avec le Chiffrement de messages.
- ❑ Authentification de messages sans Chiffrement.
 - ❑ Cas d'un système central chargé de vérifier l'authenticité.
 - ❑ Authentification par sélection de messages
 - ❑ Authentification sur les systèmes informatiques
- ❑ Authentification avec un code d'authentification de message (MAC)

Authentification avec MAC

- ❑ Utilise une clé secrète pour générer un petit bloc de donnée appelé MAC qui est joint au message
 - ❑ Les deux parties s'assurent que le message n'a pas été modifié
 - ❑ Le destinataire est assuré de l'authenticité de l'expéditeur
 - ❑ Si le message contient un numéro de séquence,
Le destinataire est assuré de l'ordre des messages

- ❑ Plusieurs algorithmes peuvent être utilisés pour générer le MAC.
 - ❑ Les algorithmes non réversibles, moins vulnérables que le Chiffrement symétrique sont recommandés.

Authentification de messages avec MAC



Fonctions « one-way hash »(1)

- ❑ Les fonctions « one-way hash » jouent un rôle important dans l'authentification des messages et dans les signatures digitales.
 - ❑ Elles acceptent un message de taille variable et produisent un code de taille fixe.
 - ❑ Pas de clé partagée et pas de chiffrement

Fonctions « one-way hash »(2)

- ❑ MD5, produit un code de 128 bits avec une taille de message infinie
- ❑ SHA-1, produit un code de 160 bits avec une taille de message de 2^{64} bits
- ❑ RIPEMD-160 , produit un code de 160bits, avec une taille de message infinie
- ❑ SHA-2(SHA-224, SHA-256, SHA-384, SHA-512)

Fonctions « one-way hash »(3)

- ❑ MD5 est vulnérable aux attaques de collision
 - déconseillé
- ❑ SHA-1 est utilisé par beaucoup d'applications et de protocoles de sécurité
- ❑ Début 2005, des vulnérabilités de collision auraient été découvertes dans le SHA-1
 - Si elles se confirment, elles affecteront:
 - ❑ Les signatures digitales non reniable des messages électroniques
 - ❑ Les signatures digitales non reniables dans les certificats

Authentification des interlocuteurs

- ❑ L'authentification des messages protège deux parties par rapport à un intrus.
- ❑ IL ne protège pas les deux parties l'une contre l'autre
- ❑ L'utilisation des signatures digitales est une solution idéale
 - ❑ On doit pouvoir vérifier l'auteur et la date de signature
 - ❑ On doit pouvoir authentifier le contenu à la date de signature
 - ❑ La signature doit être vérifiable par une tierce partie pour éviter les disputes.



Protocoles et applications de sécurité

Applications de sécurité(1)

- Applications d'authentification
 - Kerberos
 - Authentification avec certificats X509
- Session distantes
 - ssh
- Sécurité web
 - TLS,SSL
- Sécurité E-mail
 - PGP,S/MIME

Applications de sécurité(2)



- Sécurité IP - VPN

 - IPsec

- Contrôle d'accès

 - Pare-feu

 - Système de détection d'intrusion

 - Anti-virus

Questions ?

