

Sécurité des réseaux

Séminaire 2005-2006

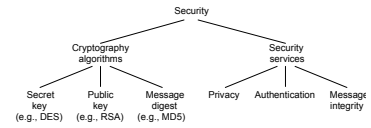
(plusieurs slides empruntées de L. Peterson.)

Infrastructures de Communication - Séminaire

1

Introduction

- Algorithms cryptographiques à
 - Clé symétrique (*secret key*) (e.g., DES)
 - Clé publique (*public key*) (e.g., RSA)
 - Condensats de messages (*message digest*) (e.g., MD5)
- Services de sécurité
 - Confidentialité (*privacy*) : prévenir la distribution non autorisée de données
 - Authentification (*authentication*) : vérifier l'identité du participant éloigné
 - Intégrité (*message integrity*) : s'assurer que les données n'ont pas été modifiées



Infrastructures de Communication - Séminaire

2

Algorithme à clé symétrique (DES)

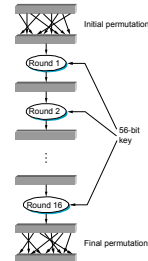


La même clé est partagée par les intervenants.

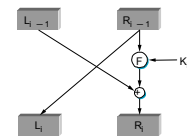
Infrastructures de Communication - Séminaire

3

- Message de 64-bits
- Clé (K) de 64-bits (56-bits + 8-bit parité)
- 16 étapes (rounds)



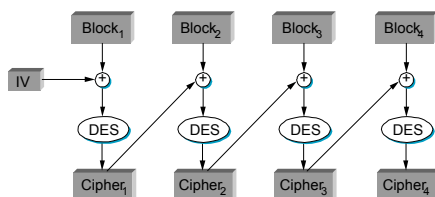
- À chaque étape



Infrastructures de Communication - Séminaire

4

- Les messages longs (>64-bits) sont divisés en blocs de 64-bits.



Infrastructures de Communication - Séminaire

5

Algorithme à clé publique (RSA)



- Les clés publiques sont publiées.
- Le chiffage (*encryption*) utilise la clé publique du destinataire.
- Le destinataire (*decryption*) utilise sa clé privée pour déchiffrer le message.
- Chiffage & Déchiffage

$$c = m^e \bmod n$$

$$m = c^d \bmod n$$

Où la clé publique est (e, n) et la clé privée (d, n)

Infrastructures de Communication - Séminaire

6

RSA (cont)

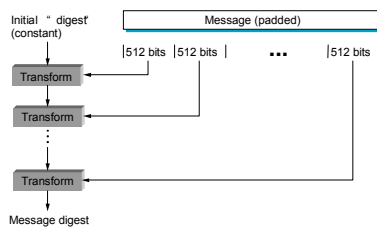
- Choisir deux nombres premiers assez grands p et q (chaque nombre de 256 bits)
- Multiplier p et q pour obtenir n
- Choisir la clé de chiffrement e (encryption key) de sorte que e et $(p-1) \times (q-1)$ soient premiers entre eux
- Deux nombres sont premiers entre eux lorsque le seul facteur commun entre eux est 1
- Calculer la clé de déchiffrement (decryption key) de la manière suivante

$$d = e^{-1} \text{ mod } ((p-1) \times (q-1))$$
- Clé privée (private key) : (d, n)
- Clé publique (public key) : (e, n)

Condensats de messages (Message Digest)

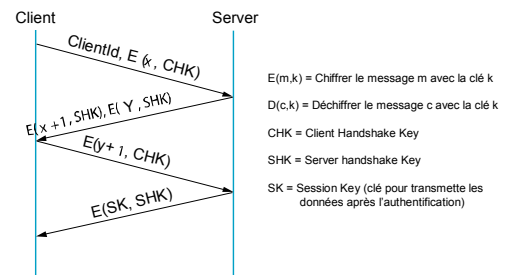
- Checksum cryptographique
 - Protège le destinataire contre les modifications malicieuses du message (checksum protège le destinataire contre les modifications involontaires du message)
- Fonction One-way
 - Étant donné un checksum cryptographique, il est virtuellement impossible de reproduire le message qui donnerait ce checksum. Il n'est pas faisable (complexité) de trouver deux messages ayant le même checksum cryptographique
- Relevance
 - Ayant reçu un message et son checksum, s'il est possible de calculer le checksum du message et ce dernier est le même que celui reçu, il est fort probable que le message ait produit le checksum reçu.

Message Digest 5 (MD5)



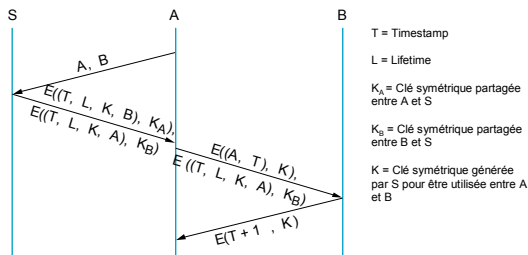
Protocoles d'authentification

- Three-way handshake (clé symétrique, CHK = SHK)



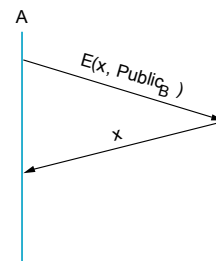
- Trusted third party (Kerberos)

- A et B partagent chacun une clé symétrique, K_A et K_B , avec un serveur S. Pour établir une connexion entre A et B, le serveur S génère une clé K symétrique pour eux sous la demande de A (ou B)



- Authentification utilisant une clé publique

- A demande d'authentifier son identité à B (l'identité de A peut être authentifiée de la même manière)



Signatures numériques (Message Integrity Protocols)

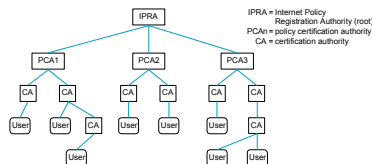
- Signatures numériques utilisant RSA
 - La signature peut être seulement générée par un seul participant (celui qui a la clé privée)
 - Calculer la signature digitale avec la clé privée et vérifier avec la clé publique
- Utilisant MD5
 - Envoie: $m + MD5(m + k) + E(k, \text{private})$
 - Destinataire
 - Récupérer la clé aléatoire k utilisant la clé publique de celui qui envoie
 - Appliquer MD5 à la concaténation du message m et la clé aléatoire k
- Utilisant MD5 avec RSA
 - Envoie: $m + E(MD5(m), \text{private})$
 - Destinataire
 - Déchiffrer la signature avec la clé publique de celui qui envoie
 - Comparer le résultat d'appliquer MD5 au message m avec le checksum déchiffré

Gestion des clés publiques (1/3)

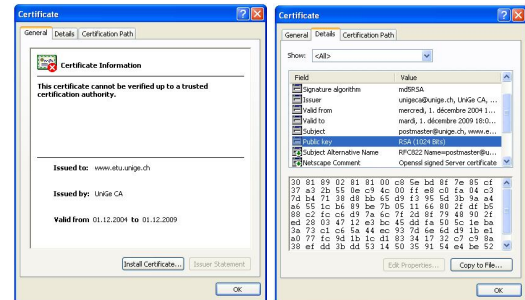
- Certificat
 - Document numérique spécialement signé:
 - "I certify that the public key in this document belongs to the entity named in this document, signed X."
 - Nom de l'entité certifiée
 - Clé publique de l'entité certifiée
 - Nom de l'entité de certification (certified authority)
 - Signature numérique
- Certified Authority (CA)
 - Entité administrative qui octroie des certificats
 - Utile seulement pour qqn qui possède la clé publique du CA

Gestion des clés publiques (2/3)

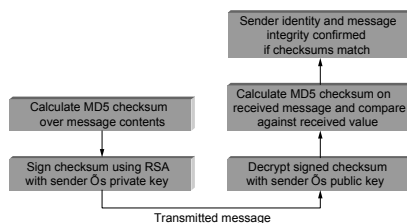
- Chain of Trust
 - Si X certifie qu'une clé publique appartient à Y, et Y certifie qu'une autre clé publique appartient à Z, alors il existe une chaîne de certificats entre X et Z
 - Quelqu'un, qui veut vérifier la clé publique de Z, doit connaître la clé publique de X pour suivre la chaîne de certificats
- Certificate Revocation List
 - Les certificats peuvent avoir une validité limitée



Gestion des clés publiques (3/3)

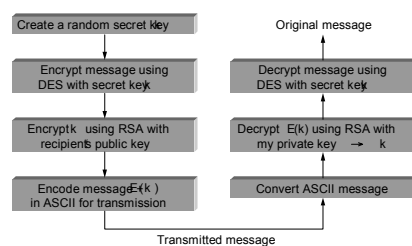


Privacy Enhanced Mail (PEM) (1/2)



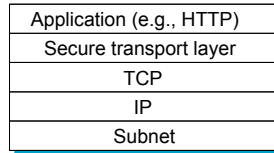
Intégrité du message et authentification

Privacy Enhanced Mail (PEM) (2/2)



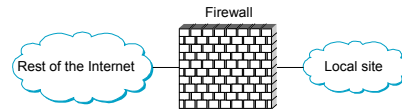
Confidentialité du message

Transport Layer Security (TLS, SSL, HTTPS)



Cette nouvelle couche est vue comme la couche de transport pour les applications, sauf qu'elle établit des connexions sécurisées (p.ex. SSH, HTTPS, etc.)

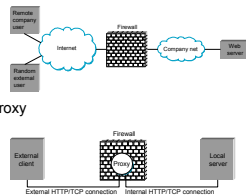
Firewalls



- Filter-Based Solution
 - Example
(192.12.13.14, 1234, 128.7.6.5, 80)
(*.*, 128.7.6.5, 80)
 - Par défaut: laisser passer ou ne pas laisser passer ?
 - Règles dynamiques ?

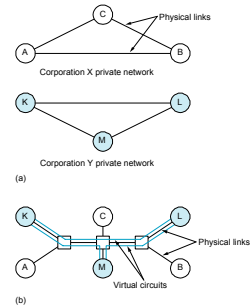
Proxy-Based Firewalls

- Problème: filtrages complexes
- Exemple: web server (permettre l'accès à quelques pages)



- Solution: proxy
- Design: transparent vs. classique
- Limitations: attaques internes

Virtual Private Network (VPN)



VPN et IP tunnel

