Services mails

Sécurité d'email

- l'email est l'un des services de réseau le plus extensivement utilisé
- actuellement le contenu des messages n'est pas sécurisé
  - peut être inspecté durant son transit
  - ou par les utilisateurs privilégiés sur le système de destination
- On souhaite :
  - Confidentialité – authentification – intégrité – non répudiation

Services mails

PGP (Pretty Good Privacy)

PGP

- Développé par Phil Zimmermann
- PGP fournit un service de confidentialité et d'authentification qui peut être employé pour des applications de type courrier électronique et stockage de dossier.
- Apport de Zimmerman :
  - sélection et emploi des meilleurs algos de crypto disponibles
  - intégration dans un programme simple indépendant de l'OS
  - à l'origine libre, dispose également maintenant de versions commerciales

Pourquoi PGP est-il populaire ?

- Disponible librement sur une large variété de plateformes.
- Basé sur des algorithmes robustes et sûrs : RSA,DSS, DH, 3DES, IDEA, CAST-128, SHA1.
- Large éventail d'applicabilité
- Non développé ou commandé par des organismes de normalisation gouvernementaux
- Est maintenant reconnu comme un standard (RFC 3156)

Notation :

K_s : clé de session utilisée dans les schémas symétriques

KR_a : clé privée de A

KU_a : clé publique de A

EP : chiffrement public

DP : déchiffrement public

EC : chiffrement symétrique

DC : déchiffrement symétrique

H = fonction de hachage

|| = concaténation

Z = fonction de compression utilisant l'algorithme ZIP

R64 : conversion au format ASCII Radix 64

Description opérationnelle

- Se compose de cinq services :
  - Authentification
  - Confidentialité
  - Compression
  - Compatibilité E mail
  - Segmentation

Récapitulatif

Fonction	Algorithme utilisé	description
Signature digitale	DSS/SHA ou RSA/SHA	Le condensé du message est créé en utilisant SHA-1 puis chiffré en utilisant DSS ou RSA avec la clé privée de l'expéditeur et inclus au message
Chiffrement de message	CAST ou IDEA ou 3DES avec DH ou RSA	Le message est chiffré en utilisant un algorithme symétrique avec une clé de session temporaire générée par l'expéditeur. Cette clé de session est chiffrée en utilisant la clé publique du destinataire et DH ou RSA. Le résultat est inclus au message.
Compression	ZIP	Compression du message pour stockage ou transmission en utilisant ZIP
Compatibilité au format mail	Conversion Radix64	Afin d'être transparent, la partie chiffrée doit être convertie en ASCII en utilisant la conversion RADIX64
Segmentation	-	Pour correspondre à la taille maximum des messages, on effectue une segmentation

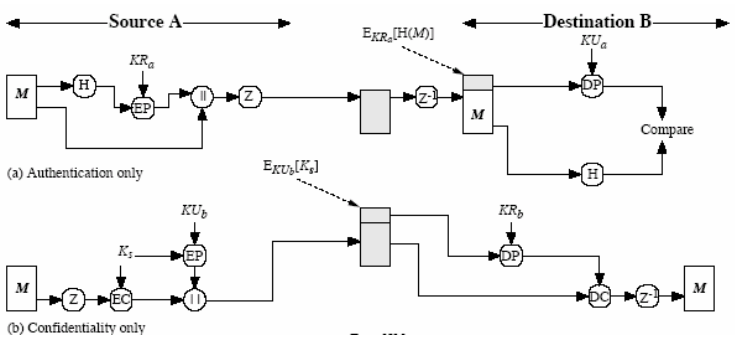
Opération PGP – Authentification

1. L'expéditeur crée un message
2. SHA 1génère un condensé de 160 bits du message
3. Le condensé est chiffré avec RSA ou DSS en utilisant la clé privée de l'expéditeur, et le résultat est attaché au message
4. Le récepteur utilise RSA ou DSS avec la clé publique de l'expéditeur pour déchiffrer et récupérer le condensé
5. Le récepteur produit un nouveau condensé du message et le compare avec le condensé déchiffré, s'ils correspondent, le message est authentique

Opération PGP – Confidentialité

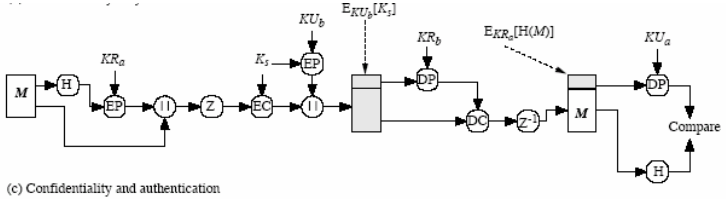
1. L'expéditeur génère un message et un nombre aléatoire de 128 bits à employer comme clef de session pour ce message seulement
2. Le message est chiffré, en utilisant Cast-128/IDEA/3DES avec la clef de session
3. La clé de session est chiffrée en utilisant le RSA avec la clef publique du destinataire, puis attachée au message
4. Le récepteur emploie le RSA avec sa clé privée pour déchiffrer et récupérer la clé de session
5. La clé de session est utilisée pour déchiffrer le message

Comparaison : authentification ou confidentialité



Opération PGP – confidentialité & authentification

- emploie les deux services sur le même message
  - créer la signature et l'attacher au message
  - chiffrer le message et la signature
  - attacher la clef de session chiffrée par RSA



(c) Confidentiality and authentication

Opération PGP – Compression

- Par défaut le PGP comprime le message après la signature mais avant le chiffrage
  - ainsi on peut stocker le message et la signature non comprimés pour une vérification postérieure
  - et parce que la compression est non déterministe
- Algorithme de compression : ZIP
- L'emplacement de l'algorithme de compression est critique.

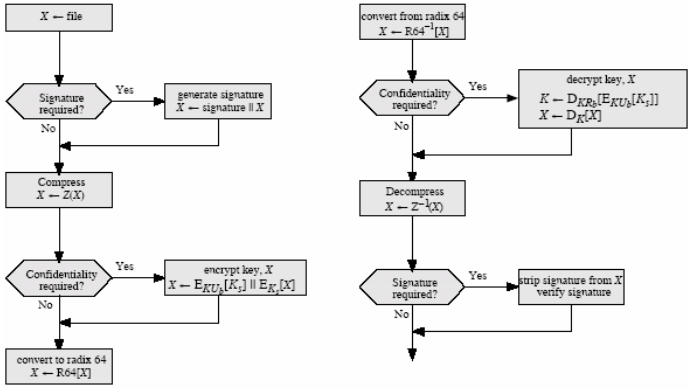
Opération PGP – Compatibilité email

- L'emploi de PGP fournira des données binaires à envoyer (message chiffré etc..)
- Cependant l'email n'a été conçu que pour le texte
- Par conséquent PGP doit coder les données binaires en caractères ASCII imprimables
- Emploi de l'algorithme radix-64
  - Fait correspondre 3 bytes à 4 cars imprimables (↗ taille)
  - Appose également un CRC
- Si nécessaire, segmentation des messages

Segmentation et réassemblage

- Souvent limité à une longueur de message maximum de 50.000 octets.
- Longs messages doivent être cassés en segments.
- Le PGP subdivise automatiquement un message qui est trop grand.
- Le récepteur enlève tous les en-têtes de mail et rassemble le bloc.

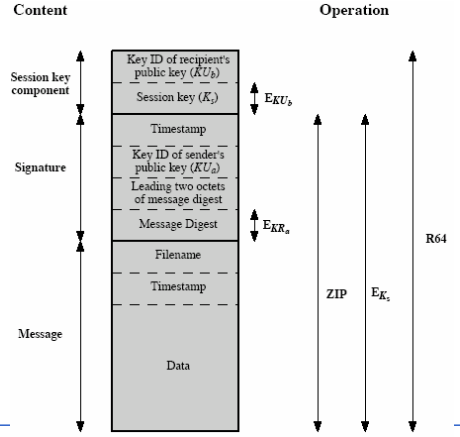
Opération PGP – résumé



(a) Generic Transmission Diagram (from A)

(b) Generic Reception Diagram (to B)

Format d'un message PGP



Clés cryptographiques et anneaux de clés

- Nécessité de générer des clés de session aléatoires
- Possibilité de disposer de plusieurs paires de clés publique/privée
- Obligation de conserver la liste de ses paires de clés mais également la liste des clés publiques de ses correspondants.

Clés de session PGP

- On a besoin d'une clé de session pour chaque message
  - des tailles variables : DES 56 bits, CAST ou IDEA 128 bits, Triple DES 168 bits
- Produit en utilisant la norme ANSI X12.17
- Utilisation de données issues des utilisations précédentes et de la synchronisation de frappe de l'utilisateur

Identifiant de clé

- Comme beaucoup de clefs publique/privée peuvent être en service, il y a nécessité d'identifier quelles sont les clés employées réellement pour chiffrer la clef de session dans un message
  - possibilité envoyer la clé publique complète avec chaque message
  - mais c'est inefficace
- Employer plutôt un identifiant de clé basé sur la clé
  - Prendre les 64 bits les moins significatifs de la clé
  - très probablement unique
- Employer également cet identifiant dans les signatures

Anneaux de clés PGP

- Chaque utilisateur PGP dispose d'une paire d'anneaux :
  - l'anneau de clés publiques contient toutes les clés publiques des autres utilisateurs de PGP connus de cet utilisateur, classé par identifiant de clé
  - l'anneau de clé privée contient les paires de clés publiques/privées de cet utilisateur, classé par key ID
- Remarque :
  - La clé privée n'est pas conservée en tant que telle mais chiffrée (avec CAST ou IDEA ou 3DES) au moyen d'un condensé (SHA1) obtenu à partir d'une passphrase.

Structure des anneaux

Private Key Ring

Timestamp	Key ID*	Public Key	Encrypted Private Key	User ID*
. . .	. . .	. . .	. . .	. . .
T_1	KU_i mod 2^{64}	KU_i	$E_{H(P)}[KR_i]$	User i
. . .	. . .	. . .	. . .	. . .

Public Key Ring

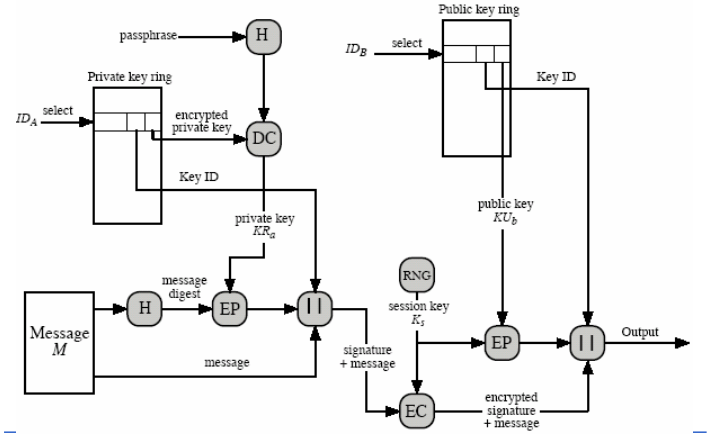
Timestamp	Key ID*	Public Key	Owner Trust	User ID*	Key Legitimacy	Signature(s)	Signature Trust(s)
. . .	. . .	. . .	. . .	. . .	. . .	. . .	. . .
T_1	KU_i mod 2^{64}	Ku_i	trust_flag$_i$	User i	trust_flag$_i$		
. . .	. . .	. . .	. . .	. . .	. . .	. . .	. . .

* = field used to index table

Utilisation des anneaux

- ENVOI
  1. Signature du message
     - Obtention de la clé privée dans l'anneau ad hoc
     - Utilisation de la passphrase pour déchiffrer la clé
     - Construction du composant signature
  2. Chiffrement du message
     - Génération d'une clé de session et chiffrement du message
     - Obtention de la clé publique du correspondant dans l'anneau ad hoc
     - Création du composant de la clé de session

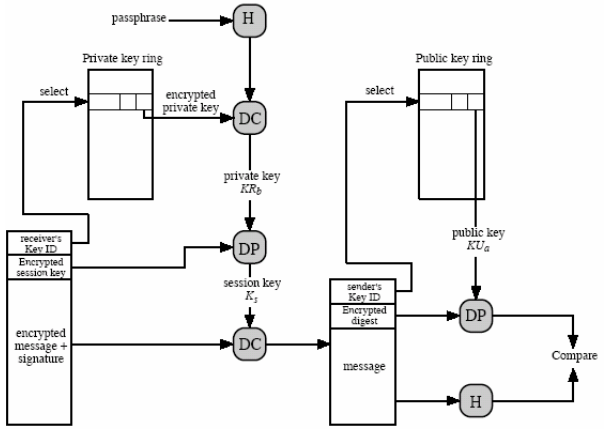
Génération d'un message PGP



Utilisation des anneaux

- RECEPTION
  1. Déchiffrement du message
     - Récupération de la clé privée dans l'anneau ad hoc (obtention de l'ID de la clé dans le composant de la clé de session)
     - Utilisation de la passphrase pour déchiffrer la clé
     - Récupération de la clé de session et déchiffrement du message
  2. Authentification du message
     - Récupération de la clé publique de l'expéditeur dans l'anneau ad hoc (utilisant l'ID de la clé dans le composant de la signature)
     - Récupération du condensé transmis
     - Calcul du condensé du message reçu et comparaison.

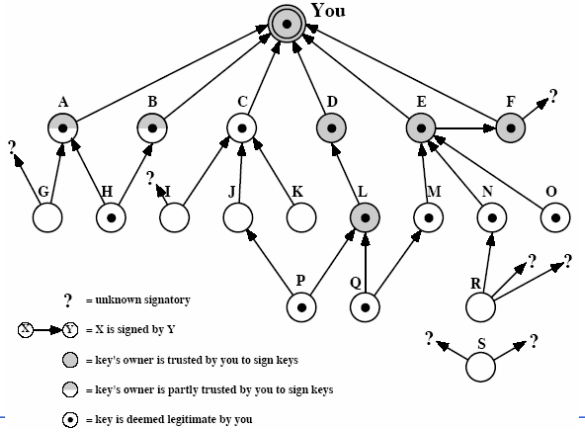
Réception d'un message PGP



Gestion des clés PGP

- plutôt que de compter sur des autorités de certificat
- dans le PGP chaque utilisateur est son propre CA
  - peut signer des clefs pour des utilisateurs qu'ils connaissent directement
- forme une « toile de confiance »
  - les clefs de confiance sont signées
- on peut faire confiance dans les clefs d'autres utilisateurs qui ont une chaîne des signatures à elles
- l'anneau principal inclut des indicateurs de confiance
- les utilisateurs peuvent également révoquer leurs clefs

Utilisation de la toile de confiance



Révocation des clés publiques

- Le propriétaire génère un certificat de révocation de clé
- Certificat normal de signature avec un indicateur de révocation
- La clé privée correspondante est employée pour signer le certificat.

Services mails

S/MIME

(Secure/Multipurpose Internet Mail Extension)

Simple Mail Transfer Protocol (SMTP)

- RFC 822
- limitations de SMTP - ne peut pas transmettre, ou a un problème avec :
  - dossiers exécutables, ou d'autres dossiers binaires (image JPEG)
  - caractères "de langue nationale" (non-ASCII)
  - messages au-dessus d'une certaine taille
  - problèmes de traduction ASCII vers EBCDIC
  - lignes plus longues qu'une certaine longueur (72 à 254 caractères)

En-tête MIME

- **MIME-Version :** Doit être "1.0" → RFC 2045, RFC 2046
- **Content-Type :** Plus de types ont été ajoutés par les réalisateurs (application/word)
- **Content-Transfer-Encoding :** Comment le message a été codé (radix 64)
- **Content-ID :** chaîne d'identification unique.
- **Content Description :** Nécessaire quand le contenu n'est pas un texte lisible (par exemple, MPEG)

S/MIME

- Secure/Multipurpose Internet Mail Extension
- S/MIME va probablement devenir le futur standard de l'industriel
- PGP sera plutôt utilisé pour la sécurité des mails personnels
- S/MIME est reconnu par la plupart des systèmes mails

Fonctions S/MIME

- Données enveloppées
  - Contenu chiffré et clés de session chiffrées pour des destinataires.
- Données signées
  - Condensé chiffré avec la clé privée du “signeur” + texte encodé en base64
- Données signées en clair
  - Texte clair + condensé signé
- Données signées et chiffrées
  - Liaison des entités signées et chiffrées dans des ordres variables

Algorithmes utilisés

- Fonctions de hachage :
  - SHA 1and MDS
- Signatures digitales :
  - DSS
- Chiffrement symétrique :
  - Triple DES, RC2/40 (exportable)
- Chiffrement à clé publique :
  - RSA avec des clés de 512 et 1024 bits, et Diffie Hellman (pour les clés de session).

Diverses procédures pour décider de l’algorithme à utiliser

Manipulation de certificats dans S/MIME

- S/MIME utilise des certificats X.509 v3
- Hybride de gestion entre la hiérarchie de CA X.509 stricte et la toile de confiance PGP
- Chaque client dispose d'une liste de certificats de CA à qui il fait confiance
- Chaque client dispose de sa propre paire de clé et de son certificat
- Ce certificat doit être signé par un des CA's à qui il fait confiance

Autorités de certification

- Il en existe de nombreuses
- Verisign est une des plus utilisées
- Verisign propose différents types de certificats
- Avec des niveaux de confiance et de vérification croissants

Class	Identity Checks	Usage
1	name/email check	web browsing/email
2+	enroll/addr check	email, subs, s/w validate
3+	ID documents	e banking/service access

Rôle de l'agent utilisateur

- Génération de clé - Diffie-Hellman, DSS et RSA.
- Enregistrement - les clés publiques doivent être enregistrée auprès d'une CA X.509 (certificat).
- Stockage du certificat - Local (comme dans un navigateur) pour différents services.
- Données signées et chiffrées – différents ordres pour le chiffrement et la signature

Ressources

- http://www.pgp.com/
- http://web.mit.edu/network/pgp.html
- http://ietf.org/html.charters/openpgp-charter.html
- http://ietf.org/html.charters/smime-charter.html
- [Stallings] – ch 15

Questions

- Expliquer
  - PGP
  - S/MIME