La signature électronique et les réseaux de confiance

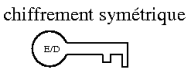
Marc.Schaefer@he-arc.ch

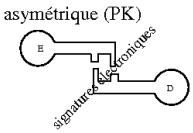
HE-Arc Ingénierie

Institut des systèmes d'information et de communication (ISIC)
Laboratoire de téléinformatique (TINF)

Types de cryptosystèmes

- systèmes à clé secrète ou dits **symétriques**
  - une clé unique (un mot de passe) connue des participants
  - on chiffre et on déchiffre avec cette clé
- systèmes à clé publique ou dits **asymétriques**
  - un couple de clé (clé publique, clé privée) par participant
  - on chiffre avec la clé publique du destinataire (connue, publiée, évt. **Certifiée**)
  - le destinataire déchiffre avec sa clé privée
  - permet la **signature électronique** !





Plan

- la cryptographie en bref et sur Internet, avec un exemple mathématique
- les principes de la signature électronique et des réseaux de confiance, avec mise en pratique (jeu)
- les risques et dangers
- le projet SuisseID

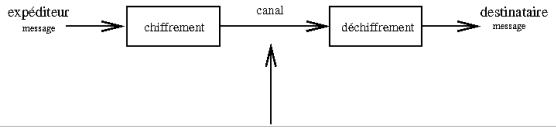
Cryptosystèmes symétriques

- algorithmes efficaces et sûrs même avec des tailles de clés faibles (p.ex. 128 bits)
  - AES, 3-DES, IDEA, ...
- une seule clé chiffre et déchiffre
- comment distribuer ces clés ?
  - avec N participants communiquant entre eux, il y en a :

$$N\frac{N-1}{2}$$

La cryptographie

- cacher l'information: la stéganographie
- la rendre incompréhensible : le **chiffrement**
- les bases mathématiques sont connues, les algorithmes aussi, les implémentations aussi : avantage pour la **confiance**
- le secret réside dans le paramètre de l'algorithme : la **clé** (ou une des clés)



Cryptosystèmes asymétriques

- couple de clé (publique, privée)
  - générées ensemble
  - dépendance mathématique entre elles
  - difficulté de passer d'une clé à l'autre
- principe : fonctions difficilement inversibles en temps « payable »
- on chiffre avec l'une, on déchiffre avec l'autre
  - exemple : Alice envoie un message à Bob en le chiffrant avec la clé publique de Bob

Exemple mathématique : RSA

- clé publique : (e, n)
- clé privée : (d, n) gardée secrète
- les autres valeurs sont jetées
- propriétés
  - difficile de trouver d sans connaître phi
  - difficile de factoriser n en p et q
  - chiffrement de m : $c = m^e \bmod n$
  - déchiffrement de c : $m = c^d \bmod n$

La signature électronique

- buts
  - prouver qu'un message provient bien d'un expéditeur donné
  - basé sur la cryptographie asymétrique
- avez-vous une idée de comment faire pour que Bob puisse vérifier que c'est bien Alice qui lui a envoyé un message ?

La cryptographie sur Internet

- chiffrement des sites Web (HTTPS) – très courant
- chiffrement/signature électronique des e-mails – parfois
- connexion à des services par authentification à clés asymétriques – encore rare
- certificats X.509
- couche logicielle: SSL/TLS
- pour l'e-mail : souvent avec GPG/PGP

Le certificat

- garantit le lien entre une identité et une clé publique
- contient
  - une identité, par exemple :
    - *.alphanet.ch
    - Marc SCHAEFER, habitant à 2053 Cernier
  - la clé publique de cette identité
  - des critères de vérifications de cette identité
  - un estampillage (horodatage), une durée de validité, ...
  - une signature électronique de ce qui précéde, par la clé privée de l'autorité de certification (CA)
- un certificat valide fait partie d'une chaîne de confiance menant à un CA connu

L'attaque de l'intermédiaire

- Alice veut envoyer un message chiffré à Bob
- Charles veut pouvoir lire ce message
- Charles persuade Alice que la clé publique de Bob est en fait la sienne
- Alice utilise la clé publique de Charles (au lieu de celle de Bob) pour chiffrer
- Charles déchiffre avec sa clé privée, puis ré-enchiffre avec la clé publique réelle de Bob
- Bob reçoit le message, le déchiffre, sans se douter que Charles sait tout !
- que faire ?

Partie pratique

- vous avez reçu (mauvais !) une carte avec une clé publique et sa clé privée correspondante
- la 1ère étape est d'essayer de chiffrer un message pour votre voisin, qu'il déchiffrera
- la 2e étape est de faire imprimer un certificat par une autorité de certification
- la 3e étape est de vous connecter sur un système grâce à votre clé privée, un « challenge » et à votre certificat (obtenu sous 2)

Les problèmes des cryptotechniques

- on ne comprend pas toujours ce qu'on fait
- on ne signe pas toujours le message que l'on croit
  - en particulier si la clé privée est stockée sur un ordinateur ou un terminal sans affichage
- les générateurs aléatoires ne sont pas toujours bons
- les logiciels ont des bugs
- les clés doivent être assez longues
- les algorithmes ont des problèmes
- les bases mathématiques peuvent avoir des faiblesses

Réseau de confiance

- la chaîne qui mène d'un certificat présenté par un site Web vers une validation par un certificat reconnu par (stocké dans le) navigateur est une **chaîne de confiance (tout ou rien) –** système hiérarchique
- d'autres systèmes sont basés sur la notion de **réseau de confiance** (p.ex. PGP/PGP)
  - le nombre de certificats qui vous font confiance donne une estimation de la confiance qu'ont vos partenaires en vous (échelle) – système communautaire
- rôle des l**istes de révocations**

La confiance

- la société est basée sur la confiance
  - confiance en la monnaie papier alors qu'il n'y a plus de garantie or depuis longtemps
- la confiance est souvent basée sur des critères subjectifs
  - p.ex. si une compagnie aérienne a un accident d'avion, faut-il l'éviter (faut-il avoir plus ou moins confiance dans sa gestion des prochains vols?)
- utiliser des logiciels de cryptographie ou sa carte bancaire c'est faire confiance tout d'abord à des logiciels qui **agissent** en votre nom !

SuisseID

- initiative de la confédération et de partenaires privés, compatible avec la loi fédérale
- but : délivrer des clés et certificats officiels pour l'usage généralisé de la cryptographie en suisse
- en pratique
  - commander par Internet (p.ex. La Poste) (79.- min.)
  - valider auprès d'une commune ou d'un office postal (25.-)
  - installer ce que La Poste livre
- les clés sont générés par le matériel et devraient donc être sûres
- la sécurité de l'utilisation dépend du traitement (p.ex. qui signe, où la clé privée est stockée, etc)

La confiance appliquée aux logiciels

- en général, plus de bugs sont trouvés, moins on a confiance
- **on a tort** : dans un logiciel, c'est surtout le fait de ne pas (pouvoir?) trouver de bugs qui est un problème !
- tout logiciel a des bugs, l'important est de les trouver, de les corriger, et de diffuser les corrections rapidement !

Références

Merci de votre attention !

Documents et informations

- http://ateliers.wiki.alphanet.ch/TecDays2012