



Les 17,18,19,20 novembre 2008
Yamoussoukro – CÔTE D'IVOIRE

Cryptographie à clés publiques

Sylvanus KLA



Besoins de cryptographie

- Sécuriser le transfert des documents confidentiels (S/MIME)
- Sécuriser l'accès aux sites confidentiels (SSL)
- Sécuriser le travail à distance (IPSec)
- Crypter les fichiers sur le disque dur (EFS)
- Signer les formulaires (Signatures XML)
 - Authentification: Identité de l'émetteur
 - Intégrité: Le document n'a pas été modifié
 - Non répudiation: L'émetteur ne peut nier l'envoi

Systemes de cryptographie



- Systemes symétriques : la même clé sert à crypter et à décrypter (DES, DESX, RC2, RC4)
- Systemes asymétriques: une clé pour crypter et une autre pour décrypter (RSA)
 - La clé publique est publiée dans un annuaire
 - La clé privée est conservée par l'utilisateur, bien en sécurité
 - Problème de la complexité du cryptage/décryptage

Idée de base

- On va coder 3 en faisant $3^2 = 9$; 9 est le code
- Pour décoder faire $9^{1/2} = 3$
- Ça marche car 2 et $1/2$ sont inverses
- $M^{2 \times 1/2} = M$ $M^{1/2 \times 2} = M$
- Avoir e, son inverse d ($e \times d = 1$) et $(M^e)^d = M$
- e est la clé publique, connue de tous, $d=e^{-1}$ est la clé privée, connue que de l'utilisateur.
- $3^{1/2} = 1,73205$ $1,73205^2 = 2,99982$
- **Question: e et e^{-1} peuvent être entiers ?**

Arithmétique modulaire

- Divisons 14 par 3. Le quotient est 4, **le reste est 2**
- On dit $14 = 2 \pmod{3}$ $(14=2 [3])$
- $28 = 3 [5]$ $63 = 3 [5]$ $28=63 [5]$
- $a = b [n]$ si en divisant a et b par n, on trouve le même reste
- $7 = 2 [5]$ $7 \times 3 = 1 [5]$
- 7 et 3 sont inverses modulo 5. $7^{-1} = 3 [5]$
- **Question: si $d=e^{-1} [?]$, a-t-on $(M^e)^d = M [n]$?**

Exemples

- $3 \times 11 = 1 [8] \quad 3^{-1} = 11 [8]$
- $8^3 = 2 [15] \quad 2^{11} = 8 [15]$
- $7^3 = 13 [15] \quad 13^3 = 7 [15]$
- $16^3 = 1 [15] \quad 1^3 = 1 [15]$
- On peut coder les nombres jusqu'à 15
- Pour coder les autres nombres, les décomposer en blocs
- (15, 3) clé publique, (15, 11) clé privée
- **Pb: La clé privée est facile à deviner**

Le coin des matheux

- Fonction indicative d'Euler
 - Considérons les nombres de 1 à n
 - Ex: 1,2,3,4,5,6,7,8: 4 parmi eux (1,3,5,7) soit 4 nombres, n'ont aucun diviseur commun avec 8
 - $\varphi(8) = 4$
 - $\varphi(2)=1$; $\varphi(3)=2$; $\varphi(4)=2$; $\varphi(5)=4$; $\varphi(6)= 2$; $\varphi(7)=6$
 - Si n est premier, $\varphi(n)=n-1$
 - Si p et q premiers, $\varphi(p \times q) = \varphi(p) \times \varphi(q) = (p-1) \times (q-1)$

Théorème de Fermat

Si e et d sont inverses modulo $\varphi(n)$ alors $(M^e)^d = M [n]$

Notre système de cryptographie

- Prendre n et calculer $\varphi(n)$
- Choisir e premier avec $\varphi(n)$, calculer son inverse d
- (n, e) clé publique; (n, d) clé privée
- En prenant n très grand, les autres ne pourront pas calculer $\varphi(n)$, donc ne pourront pas calculer d
- **Question: comment faire pour que $\varphi(n)$ soit facile à calculer pour nous ?**

Solution

- Construire judicieusement n
- Rappel: $\varphi(p \times q) = \varphi(p) \times \varphi(q) = (p-1) \times (q-1)$ si p et q premiers
- Prendre donc $n = p \times q$, avec p et q de grands nombres premiers
- On aura: $\varphi(n) = (p-1) \times (q-1)$

Algorithme RSA

- Prendre 2 nombres premiers p et q très grands
- Calculer $n = p \times q$
- Calculer $\varphi(n) = (p-1) (q-1)$
- Choisir e premier avec $\varphi(n)$
- Déterminer d l'inverse de e modulo $\varphi(n)$
- Détruire $p, q, \varphi(n)$
- Publier la clé (n, e) dans un annuaire et garder secrètement la clé (n, d)
- Pour coder M , on calcule $M_1 = M^e [n]$
- Pour décoder M_1 on calcule $M_1^d [n]$

Pourquoi c'est sécurisé ?

- Si n est très grand, $\varphi(n)$ est pratiquement impossible à calculer: problème de factorisation des grands nombres
- Questions non résolus
 - N'existe-t-il pas de méthode de factorisation rapide ?
 - N'existe-t-il pas d'autre méthode pour calculer $\varphi(n)$?

Utilisation

- Crypter un texte :
 - Crypter le texte avec une clé symétrique
 - Crypter la clé symétrique en RSA avec la clé publique du destinataire
- Signer un texte :
 - Calculer une empreinte du texte (digest, hash code, condensé)
 - Crypter l'empreinte en RSA avec la clé privée du signataire

Infrastructure à clés publiques (PKI)



- Autorité de certification
- Certificat numérique
- Autorité d'enregistrement
- Autorité de dépôt
- Autorité de séquestre
- Liste des certificats révoqués (CRL)

Mise en place d'une PKI



- L'autorité de certification est un tiers de confiance.
Son capital est la confiance
- Construire cette confiance
 - Déclaration de pratiques de certification:
affirmation publique des pratiques, du niveau de sécurité, des communautés visées, des classes d'applications, des conditions de délivrance, de révocation, de renouvellement des certificats
- 20% de technique, 80% d'organisation