Chiffrement asymétrique : RSA et DH

Dr. Yousfi Souheib

Public Key Infrastructure

Définition

Infrastructure à clef publique qui permet de gérer les clefs et les certificats qui constituent un cadre à l'usage des techniques cryptographiques.

- Certification :
  - E-Commerce : Vendre et acheter des biens ou des services via Internet. Généralement, toute activité relative à l'échange électronique.
  - Nécessité d'une partie tierce pour l'établissement de la confiance.
- Certificat électronique :
  - C'est un document électronique qui prouve qu'une clef publique appartient bien à son propriétaire.
  - Empêcher qu'une personne puisse prendre l'identité d'une autre personne.
  - Intrus ne peut pas se faire passer pour B. A peut vérifier que sa clef ne correspond pas à celle de B grâce au certificat.

- La sécurité de RSA repose sur deux conjectures :
  - L'un des problèmes les plus difficiles en mathématiques : la factorisation des grand nombres, factorisation d'un nombre n en un produit initial des nombres p et q.
  - Avec les algorithmes classiques, le temps que prend cette factorisation croît exponentiellement avec la longueur de la clef.

Le cryptosystème de RSA (Rivest Shamir Adleman)

- Chaque correspondant choisit deux nombres premiers p et q
- On calcule $n = p * q$
- On calcule $\varphi = (p-1) * (q-1)$
- On choisit e de manière à ce qu'il soit relativement premier à φ (Deux nombres relativement premiers entre eux sont deux nombres dont le PGCD (plus grand commun diviseur) est égal à 1)
- On cherche d tel que $d * e = 1 (mod \varphi)$

- Soit M un message à chiffrer, C un message chiffré
- Pour chiffrer un message : $C = M^e mod n$
- Pour déchiffer un message : $M = C^d mod n$
- La clé publique est la paire de nombres (e, n)
- La clé privée est la paire de nombres (d, n)

Le cryptosystème de RSA (Rivest Shamir Adleman)

- Rappel : $n = p * q$; $\varphi = (p-1)*(q-1)$; e relativement premier à φ ; $d * e = 1(mod\varphi)$
  - Exemple :
    - On choisit $p = 3$ et $q = 5$
    - Ce qui nous donne $n = p * q = 15$ et $\varphi = (p-1)*(q-1) = 8$
    - On choisit $e = 3$, il est bien relativement premier à φ (car PGCD(3,8)=1)
    - On trouve $d = 11$ en vérifiant $e * dmod\varphi = 1$ (car 3 * 11 (mod 8) = 33 (mod 8) = 1)

- Nous avons donc :
  - La clé publique $(e, n) = (3, 15)$
  - La clé privée $(d, n) = (11, 15)$
- On prend comme exemple de message $M = 2$
  - Le chiffrement $C = 2^3 (mod 15) = 8$
  - Le déchiffrement $M = 8^{11} (mod 15) = 2$

Le choix des nombres p et q

- Multiplier deux grands nombres est facile
- Décomposer un grand nombre en produit de deux facteurs est plus difficile
- p=1113954325148827987925490175477024844070922844843
  q=1917481702524504439375786268230862180696934189293
- pq=21359870359209100823950227049996287970510953418
  264174064425241650085839577464450884050094308659 99

Example

- On choisit $p = 41, q = 61$ On aura $n = 2501$, $\phi(n) = 2400$
- On choisit $d = 2087$ On aura $e = 23$
- On choisit $d = 2069$ On aura $e=29$
- Si on choisit d'autres valeurs de d on aura d'autres valeurs de e

Prenons ce cas de figure (e=23 and d=2087).

Plaintext: KARLSRUHE

Encoding: 100017111817200704

Comme $10^3 < n < 10^4$, Le texte numérique en clair est subdivisé en blocs de 3 bits, alors 6 nombres obtenus

Chiffrement

100, 017, 111, 817, 200, 704

$100^{23} \bmod 2501$, $17^{23} \bmod 2501$, $111^{23} \bmod 2501$

$817^{23} \bmod 2501$, $200^{23} \bmod 2501$, $704^{23} \bmod 2501$

Les chiffrés obtenus 2306, 1893, 621, 1380, 490, 313

Déchiffrement

$2306^{2087} \bmod 2501 = 100$ $\quad 1893^{2087} \bmod 2501 = 17$

$621^{2087} \bmod 2501 = 111$ $\quad 1380^{2087} \bmod 2501 = 817$

$490^{2087} \bmod 2501 = 200$ $\quad 313^{2087} \bmod 2501 = 704$

La taille de clef dans RSA

- En 2009, une équipe de scientifiques parmi lesquels des chercheurs INRIA (France), NTT (Japon), Université de Bonn (Allemagne) et CWI (Pays-Bas) sont parvenus à "casser" une clef de sécurité RSA de taille 768 bits.
- Grâce à la puissance de traitement des processeurs modernes, ces travaux ont atteint deux ans et demi.
- En 2010, des chercheurs de l'université du Michigan ont réussi à casser une clef RSA de 1024 bits en provoquant des erreurs au niveau du microprocesseur. Par sûreté, NIST recommande une taille des clefs RSA au moins de 2 048 bits.
- En 2020, la clef pourrait avoir comme taille 3072 avec l'évolution de la puissance de calcul.

Signature RSA

- Alice envoie un message M à Bob et veut le signer pour s'identifier
- Elle dispose d'une clef publique e et d'une clef privée d avec $ed = 1 mod (p-1)(q-1)$
- Elle calcule $s = M^d mod n$ et envoie M et s.
- Bob vérifie $M = s^e mod n$

Exemple de signature RSA

- Dans l'exemple on prend n = 33, e=3, d=7
- Si $M = 14$ alors $M^d = 14^7 mod n =$ $105413504 mod 33 = 20 mod 33 = 20 = s$
- Vérification : $s^e = 20^3 mod n = 8000 mod 33 = 14 = M mod 33$

Description du cryptosystème de Diffie-Hellman

- Soit A et B deux terminaux qui veulent communiquer ensemble
- A et B partagent des informations publiques à savoir : p (un nombre premier) et une base g (générateur d'un groupe fini d'ordre p)
- A choisit un nombre aléatoire a et calcule $u = g^a modp$ et envoie u à B
- B choisit aussi un nombre aléatoire b et calcule $v = g^b modp$ et envoie v à A

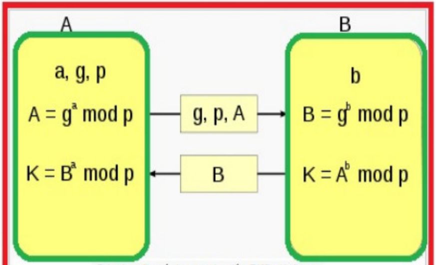
- B calcule sa clé $k = u^b = (g^a)^b mod p$
- A calcule sa clé $k = v^a = (g^b)^a mod p$
- A et B partagent la même clé $K = g^{ab} mod p$

Description du cryptosystème de Diffie-Hellman

- Supposons A et B choisissent comme paramètres publics $p = 47$ et $g = 5$
- A choisit un nombre entre 0 et 46, prenons $a = 18$
- B choisit un nombre entre 0 et 46, prenons $b = 22$
- A publie $g^a mod p$ i.e. $u = 5^{18} mod 47 = 2$
- B publie $g^b mod p$ i.e. $v = 5^{22} mod 47 = 28$
- Si A veut construire la clé de session K avec B, elle prend le message reçu $v = 28$ et elle lui applique son information privée $a = 18$
- A obtient $28^{18} mod 47 = 24 = K$ la clé de session de A

- Si B veut construire sa clé de session, il prend le message reçu de A, $u = 2$ et lui applique son nombre secret $b = 22$.

- B obtient alors $K = 2^{22} mod 47 = 24$: clé de session entre A et B



Principe d'un échange de clés Diffie-Hellman