BCS 2016 - 2017

Exercice 1 - Questions de Cours

1. Chiffrement symétrique:
   - même clé pour chiffrer et déchiffrer;
   - AES, DES;
   - 128 à 256 bits.
2. Chiffrement à clé publique:
   - une clé pour chiffrer et une clé pour déchiffrer;
   - RSA;
   - 2048 à 4096 bits.
3. Propriétés des fonctions de hachage cryptographiques:
   - résistance aux pré-images;
   - résistance aux secondes pré-images;
   - résistance aux collisions;
   - 256 bits.
4. Chiffrement hybride:
   - échange d'une clé par cryptographie à clé publique;
   - communication chiffrée par un chiffrement symétrique.
5. Chiffrement sûr:
   - distinguable d'une fonction aléatoire?
6. Générer de grands nombres premiers:
   - nombres pseudo-premiers $\rightarrow$ pas sûr qu'il est premier;
   - générer à l'aide du petit théorème de Fermat.
7. Chiffrement authentifié:
   - confidentialité, authenticité et intégrité;
   - encrypt then MAC.
8. Chiffrement à la sécurité parfaite:
   - One Time Pad.
9. Le serveur renvoie un message d'erreur lorsque le padding n'est pas bon. Permet de retrouver le premier bloc du chiffré, et ainsi de retrouver tout le message. Afin de s'en prémunir, il faut appliquer les recommendations de sécurité.

Exercice 2 - Serveur de Stockage Sécurisé

CALCUL

Clé secrète $Dsk(Epk(K)) = k$

STOCKAGE

Tout est stocké chiffré.

MAISON

Clé publique Pk

Entre CALCUL et STOCKAGE

$AESk(Data)$

À faire après l'AES:

M $\rightarrow$ C: $Epc(K||\sigma_M(K)) = x$

C: $Dsc(x) = y1||y2$ et vérifie que $y2 = H(y1)$

C $\rightarrow$ S: $Eps(K'||\sigma_C(K')) = x'$

S: $Dss(x') = y1'||y2'$ et vérifie que $y2' = H(y1')$

C $\rightarrow$ S: $Ek'(AESk(Data))$ où E est un chiffrement authentifié

S: Déchiffrer avec la clé K' et vérifier l'intégrité et l'authenticité de la signature.

Entre MAISON et CALCUL

$Epk(K||H(K))$

Chiffrement à clé publique

Exercice 3 - RSA

1. $N = p * q$

   $\varphi(N) = (p-1) * (q-1)$

   e = aléatoire $\in [1, \varphi(N)]$ tel que $pgcd(e, \varphi(N)) = 1$

   d = $emodinv\varphi(N)$

   $\implies ed = 1 \mod \varphi(N)$

2. $55 = pq = 5 * 11$

   $\varphi(N) = 4 * 10$

   $e = 3$

   $3d = 1 \mod 40$

   $d = -13 \mod 40$

   $d = 27 \mod 40$

   $40 = ? * 3$

$1 = 40 - 13 * 3$

3. On connait e, N et $d^4 \leq N$

On a N sur n bits

$\rightarrow$ on cherche d' sur $\frac{N}{4}$ bits car $d^4 \leq N$

$\rightarrow$ de plus d' doit être premier aver $\varphi(N)$ car $ed = 1 \mod \varphi(N)$

$(e, N), (d, p, q)$ clés RSA

$(e' + M, N), (d, p, q)$ clés RSA

$d(e' + M) = 1 \mod \varphi(N)$

$d'e' = 1 \mod \varphi(N)$ avec $d' < N^{\frac{1}{4}}$

On cherche à casser la clé publique.

$(e - M, N) = (e', M)$

- Pour cette clé publique $d'^4 < N$ donc on peut retrouver p et q.
- À partir de p et q on recherche d.

Exercice 4 - Construction de MAC

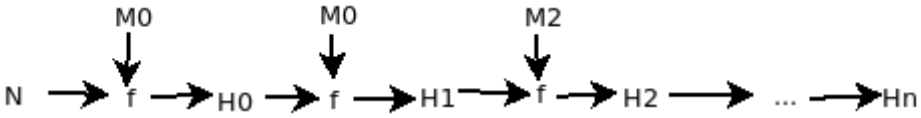

Figure 1: diag_mac

1.

2. a. Soit m, s'il est algorithmiquement difficile de générer un message M et une clé K tels que $MACk(M) = m$

   Il est algorithmiquement dur de trouver M1,M2 et K tels que $MACk(M1) = MACk(M2)$

   b. $MACk(M) = H(K||M)$

3. M0 M1 K0 K1 N -> f -> H0 -> f -> H1 -> f -> H2 -> f -> H3

On cherche une collision sur $H \implies$ algorithmiquement dur

4. $MACk(M) = MACk(H(M))$