TD 2: Cryptographie

Exercice 1

Un utilisateur vient de perdre sa clé privée, mais dispose encore de la clé publique correspondante.

1. Peut-il envoyer des courriers électroniques chiffrés ? Justifiez votre réponse.
   Oui, car il va chiffrer les messages à l'aide des clés publiques des utilisateurs qu'il va communiquer avec eux.
2. Peut-il recevoir des courriers électroniques chiffrés ? Justifiez votre réponse.
   Non, car il va recevoir des courriers électroniques chiffrés par sa clé publique et il ne peut les déchiffrer qu'avec sa clé privée
3. Peut-il signer des courriers électroniques qu'il envoie ? Justifiez votre réponse.
   Non, car une signature numérique est le *Hash* (résultat de la fonction de hachage) d'un message crypté avec la clé privée de l'émetteur.
4. Peut-il vérifier des signatures des courriers électroniques qu'il reçoit ? Justifiez votre réponse.
   Oui, car il va vérifier la signature des courriers électroniques reçus en utilisant les clés publiques des utilisateurs qui ont envoyé ces courriers.
5. A quoi peut encore servir la clé publique de cet utilisateur ?
   Á rien, car on ne peut absolument pas retrouver la clé privée à partir d'une clé publique
   Il n'a pas d'autre choix que de régénérer une nouvelle clé privée et de distribuer la clé publique correspondante à ses interlocuteurs.

Exercice 2

Un professeur envoie ses notes au secrétariat de l'école par mail. La clé publique du professeur est (e=71, n=1073) (pour $\boldsymbol{p}$ = 29, $\boldsymbol{q}$ = 37), celle du secrétariat (e=7, n=187) (pour $\boldsymbol{p}$= 17; $\boldsymbol{q}$=11).

1. Montrer que 1079 est la clé privée du professeur.

La clé privée est constituée de « d et n », Kpr = {d,n} .
Il faut vérifier que

- e*d mod ((p − 1)(q − 1)) = 1➔71*1079 mod1008=1

donc d=1079 est la clé privée du professeur

2. Montrer que 23 est la clé privée du secrétariat de l'école.

La clé privée est constituée de « d et n », Kpr = {d,n} .
Il faut vérifier que

- e*d mod ((p − 1)(q − 1)) = 1➔7*23mod160=1
- donc d=23 est la clé privée du secrétariat

3. Pour assurer la confidentialité de ses messages, avec quelle clé le professeur chiffre les notes ? Quel est le message chiffré correspond à la note 12 ?

Pour assurer la confidentialité de ses messages, le professeur chiffre les notes avec la clé publique du secrétariat

C = M^e mod n=12 ^{7}mod 187= 35831808mod187
35831808/187=191613,94
191613*187=35831631
35831808-35831631=177

4. Pour assurer l'authenticité de ses messages, avec quelle clé le professeur signe chaque note ?

Avec sa clé privée

5. Le secrétariat reçoit ainsi le message 93. Quelle est la note correspondante ?

M = C^d mod n = 93^{23} mod 187 = 15

Exercice 3

On considère un module RSA, n=p*q, où p et q sont les inconnues.

- Montrer comment la connaissance de φ(n) permet de remonter à la factorisation de n

On a $n = P \times q \implies q = \frac{n}{P}$

$\varphi(n) = (P-1)(q-1) = Pq - q - P + 1 = n - \frac{n}{P} - P + 1$

$\varphi(n) \times P = nP - n - P^2 + P$

$P^2 + (\varphi(n) - n - 1)P + n = 0$

de la forme d'une équation de second degré de la forme $ax^2 + bx + c = 0$

Le discriminant de l'équation est la valeur Δ définie par :

$\Delta = b^2 - 4ac = (\varphi(n) - n - 1)^2 - 4n$

$x_1 = \frac{-b+\sqrt{\Delta}}{2a}$ et $x_2 = \frac{-b-\sqrt{\Delta}}{2a}$

$$P_1 = \frac{n + 1 - \varphi(n) + \sqrt{(\varphi(n) - n - 1)^2 - 4n}}{2}$$

$$P_2 = \frac{n + 1 - \varphi(n) - \sqrt{(\varphi(n) - n - 1)^2 - 4n}}{2}$$

$$q_1 = \frac{n}{P_1} = \frac{2n}{n + 1 - \varphi(n) + \sqrt{(\varphi(n) - n - 1)^2 - 4n}}$$

$$q_2 = \frac{n}{P_2} = \frac{2n}{n + 1 - \varphi(n) - \sqrt{(\varphi(n) - n - 1)^2 - 4n}}$$