RICOTTA Clément p1201800
ROUX Antoine p1409394

MIF30 Cryptologie : TP noté

Exercice (Signature RSA)

Q1 :

On utilise la clé secrète car la personne recevant le message va devoir vérifier que la signature attachée correspond à l'émetteur. Il ne connait pas la clé secrète de l'émetteur, il doit donc utiliser sa clé publique. L'inverse ne pourrait pas être possible.

Q2 :

Vérification (e, N, m, σ) :

- Si $\sigma^e = m[N]$
  - Retourne Vrai
- Sinon
  - Retourne Faux

Q4 :

Signature (d, p, q, m) :

- Calcule $N = p * q$
- Calcule l
- Génère r
- Génère h à l'aide de la fonction *generateh*(m, l, r)
- $\sigma = h^d[N]$
- Retourne σ et r

Vérification (e, N, m, σ, r) :

- Calcule l
- Génère h fonction *generateh*(m, l, r)
- Si $\sigma^e = m[N]$
  - Retourne Vrai
- Sinon
  - Retourne Faux

Exercice (El Gamal « additif »)

Q2 :

On utilise le théorème des restes chinois.

Pour compiler et lancer les programmes

La classe RSA_Signature_Elgamal.java contient les deux exercices.

Pour le compiler et l'executer, lancez les commandes :

javac –d bin –sourcepath ./ RSA_Signature_Elgamal.java
cd bin/
java RSA_Signature_Elgamal