Université MohammedV **Master IPS :S1**

Faculté des sciencesRabat **Module : Sécurité informatique**

Département d'informatique **2021-2022**

Série n°4 : RSA et EL Gamal

Exercice 1

Considérons les deux nombres premiers, p et q, tels que p= 11 et q=13.

1. Calculer les clefs associées au crypto-système RSA défini par les nombres p et q .
2. On suppose que le message à envoyer est une date de naissance : 071290

   -Chiffrer ce message

   - Déchiffrer le.

Exercice 2 :

Considérons le nombre premier n=181. Un générateur de Z/ /nZ/ est g=23.
Prenons a=7 et $A=g^a \pmod{n}$.

3. Déterminer la clé publique et la clé privée du crypto-système Elgamal corrspondant.
4. Chiffrer le message 071290 à l'aide du crypto-système Elgamal défini par les paramètres précédents.
5. Déchiffrer le message chiffré obtenu

Exercice 3:

Soient p et q deux grands nombres premiers qu'on suppose inconnus.
Posons n=p.q et $\varphi(n)= (p-1) (q-1)$.
Montrer que si n et $\varphi(n)$ sont connus, on peut déterminer une factorisation de n.

Exercice 4

Si un message en clair est chiffré 2 fois avec le système RSA en utilisant 2 clés publiques RSA (N, c1) et(N,c2) et si c1 et c2 sont premiers entre eux montrer alors que le message en clair peut être retrouvé à partir des 2 cryptogrammes associés.

Exercice 5

Soit (G,g,p,A) une clé publique ElGamal et a la clé secrète correspondante .

1) Désignons par C1 et C2 les messages chiffrés respectifs des messages clairs m1 et m2 avec la clé ci-dessus. Déterminer en fonction de m1 et m2, le message clair m inconnu qu'un' attaquant peut envoyer (chiffré bien sûr) au destinataire ?de quelle type d'attaque s'agit-il ?
2) Comment peut-on éviter cette attaque ?