USTHB/FEI
Dpt Informatique

TD : cryptographie asymétrique

Exercice 1 :

Soit le cryptosystème RSA avec p=43, q=59 et d=937.
(a) Déterminer la clé de chiffrement e.
(b) Chiffrer le message 13487947504.
(c) Déchiffrer le message crypté 175807260375 qui a été envoyé par blocs de 4 chiffres.

Exercice 2 :

Considérons l'algorithme RSA avec un module n=1363, si on a pris connaissance que $\phi(n)=1288$. Utiliser ces informations pour factoriser n.

Exercice3 :

Alice et Bob utilisent le même module RSA mais avec des clés publiques différentes e_A et e_B respectivement tel que pgcg(e_A; e_B) = 1. Charlie récupère deux textes cryptés $c_A = m^{eA}$ (mod n) and $c_B = m^{eB}$ (mod n). Charlie calcule :

$x_1 = e^{-1}_A \bmod n$ et $x2 = (x_1 e_A^{-1})/e_B$

(a) comment Charlie peut calculer m en utilisant c_A, c_B, x_1 and x_2?
(b) utilizer (a) pour calculer m si n=18721, eA=43, eB=7717, cA=12677 et cB=14702

Exercice4 : RSA / CRT

Donner le message clair m correspondant au chiffré c = 133 obtenu à partir de l'opération de chiffrement RSA $c = m^7 \bmod 143$ sachant que n est divisible par 11. Vous donnerez deux méthodes pour calculer m, l'une directe l'autre reposant sur le CRT.

Exercice5 : El Gamal

Soit p = 59, a = 2, et P = 56.
a. Vérifier que s = 21 est la clé privée pour la clé publique ElGamal (p; a; P).
b. Calculer un chiffrement de m = 7 avec (p; a; P). Pourquoi n'est-t-il pas unique ?
c. Montrer les étapes pour déchiffrement de votre texte chiffré

Exercice6 : El Gamal

Soit le cryptosystème El Gamal (p,a,P)

a. Soit c=(a,b) un texte chiffré, suppose que Charlie peut obtenir le déchiffrement d'un texte chiffré c'≠ c, montrer qu'il peut alors déchiffrer c.
b. Soient c1=(a1,b1) c2=(a2,b2) deux chiffrés (avec la même clé publique) des messages m1 et m2 respectivement avec m1≠ m2, montrer qu'on peut chiffrer un autre message m'.