ENSIAS 2012-2013

TP : Cryptographie et Maple

Consignes : Préparer un seul fichier texte contenant tous les exercices, l'enregistrer sous la forme "nom-prénom" et l'envoyer à l'adresse `abderrahmane.nitaj@unicaen.fr`

Ex1. On considère l'algorithme suivant :

Algorithme 1 : methode $p-1$

Entrée : Un grand nombre entier n et deux petits entiers k et l.
Sortie : Une liste L.

1: $L = \{\}$.
2: **Pour** j de 1 à l **faire**
3: Prendre un entier a aléatoire de $[2, n-2]$.
4: **Pour** i de 2 à k **faire**
5: $a \equiv a^i \pmod{n}$.
6: $d = \gcd(a-1, n)$.
7: **Si** $d > 1$ et $d < n$ **alors**
8: Ajouter d et $\frac{n}{d}$ à la liste L avec L :=L union $\{d, n/d\}$.
9: **Fin Si**
10: **Fin Pour**
11: **Fin Pour**
12: Return L.

1. Ecrire une procédure dec(n,k,l) qui permet de sortir la liste L.
2. Appliquer cette procedure dans les cas suivants :
   (a) dec(13927189,20,1) ;
   (b) dec(14781543433,1000,5) ;

Ex2. Voici mes paramètre pour le cryptosystème Elgamal où p est le nombre premier, g est le générateur du groupe $(\mathbb{Z}/p\mathbb{Z})^*$ et $ga \equiv g^a \pmod{p}$ pour un exposant a secret :

$$p = 69915935496685949873378903 2469.$$
$$g = 2$$
$$ga \equiv g^a \pmod{p} = 32234300532191484592209654423$$

Le but est de préparer et envoyer un texte crypté.

1. Ecrire dans le même fichier toutes les procédures necessaires.
2. Crypter en envoyer le fichier dans un document text.

Ex3. On considère le module RSA suivant :

$N := 272369241464396505873920220273210867046255976193142655316585465966788231747994015917711233 9.$

On sait que les facteurs premiers p et q de N sont voisins.

1. Ecrire une procédure pour factoriser N.
2. Factoriser N.