ENSIAS 2014-2015

TP : Cryptographie et Maple

Consignes : Préparer un seul fichier texte contenant tous les exercices, l'enregistrer sous la forme "nom1etnom2" et l'envoyer à l'adresse `abderrahmane.nitaj@unicaen.fr`

Ex1. Let A and B be positive integers with

$$A = \sum_{i=0}^{k-1} a_{k-1-i} b^{k-1-i}, \qquad B = \sum_{i=0}^{l-1} b_{l-1-i} b^{l-1-i}.$$

Suppose that $k \geq l$.

1. Find a formal expression for AB in terms of A and B.
2. Write a maple program to compute AB.

Ex2.

1. Ecrire une procédure maple qui liste tous les nombres pseudo-premiers forts en une base donnée a dans un intervalle $[x, y]$.
2. Appliquer cette procedure avec $a = 5$, $x = 110$ et $y = 210$. Quelle est la liste produite ?

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.

Ex4. 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 :

$$\begin{aligned} p &= 168130353387298588108100600045 3, \\ g &= 2, \\ ga &\equiv g^a \pmod p = 277123080346812480378601199638. \end{aligned}$$

Le but est d'envoyer un texte crypté.

1. Ecrire dans le même fichier toutes les procédures necessaires.
2. Crypter le message suivant "L'ENSIAS est grande".