le cnam

Département de Mathématiques et Statistiques

Algèbre de Boole, probabilités et arithmétique

Devoir 3, à rendre pour la séance numéro 10, mardi 28 novembre 2023

Pratique du code RSA

Cet exercice a pour but de montrer la variété des calculs arithmétiques utilisés lors du codage et du décodage à l'aide du système "RSA". Il est indispensable d'effectuer les opérations arithmétiques à l'aide d'une calculette ou d'un tableur.

On se donne la clef publique $n = 3149$ et $e = 73$ d'un système RSA.

a) Pour coder un entier $m \in \{1, 2, \dots, 3148\}$ quel calcul doit-on effectuer ?

On appelle u le message crypté qui est envoyé à un correspondant qui peut décoder le message.

b) Montrer qu'il suffit de calculer les nombres m^8 et m^{64} modulo un entier qu'on précisera puis de faire deux multiplications pour expliciter $u \in \{1, 2, \dots, 3148\}$.

c) On se donne $m = 421$. Quel est le message u reçu par le correspondant ? Il pourra être utile de vérifier que $421^8 \equiv 773 \pmod{3149}$ et $421^{64} \equiv 1858 \pmod{3149}$.

Compte tenu de la valeur modique de l'entier n, il est possible de casser ce code RSA.

d) De quelle liste de nombres premiers a-t-on besoin pour déterminer deux nombres premiers p et q de sorte que $n = p\,q$?

e) Expliciter cette liste par la méthode de votre choix.

f) Quels sont les deux nombres premiers p et q de sorte que $n = p\,q$?

g) Vérifier que l'exposant utilisé $e = 73$ est bien admissible.

h) Trouver un entier d positif de sorte que $e\,d \equiv 1 \pmod{(p-1)\,(q-1)}$.

i) On reçoit l'entier $v = 2594$. Quel message secret $m' \in \{1, 2, \dots, 3148\}$ a été envoyé ?

Il pourra être utile de vérifier que $2594^8 \equiv 1912 \pmod{3149}$, $2594^{16} \equiv 2904 \pmod{3149}$, $2594^{256} \equiv 1528 \pmod{3149}$ et $2594^{2048} \equiv 1701 \pmod{3149}$ avant d'effectuer quelques multiplications complémentaires *modulo* 3149.

François Dubois, 14 novembre 2023.