I Objectifs

Présenter un système de cryptage récent.

En faire une implémentation sous le tableur Excel.

II Propriété fondamentale

n = pq est le produit de deux entiers **premiers** p et et q distincts.

On pose m = (p – 1)(q – 1) et on note c un nombre premier avec m.

On note x un entier naturel.

a) Démontrer qu'il existe des entiers d et k tels que :

$$cd = mk + 1 \text{ (c'est-à-dire } cd \equiv 1 \text{ [m])}$$

b) Cas où x est non divisible par p.

Démontrer que $x^{p-1} \equiv 1$ [p].

En déduire que $x^{km} \equiv 1$ [p], puis que $x^{cd} \equiv x$ [p]

Cas où x est divisible par p.

Démontrer que $x^{cd} \equiv x$ [p].

c) Démontrer de façon analogue que pour tout entier naturel x, $x^{cd} \equiv x$ [q].

d) En déduire que pour tout entier naturel x, $\mathbf{x^{cd} \equiv x}$ **[n]**.

III Principe du cryptage

- Pour chiffrer un message (cartes bancaires, internet, …), on choisit deux nombres premiers p et q très grand et on calcule n = pq.

  On pose m = (p – 1)(q – 1).

  On cherche deux entiers naturels c et d tels que $cd \equiv 1$ [m].

- Les messages x seront des entiers naturels appartenant à [0;1;….;n – 1].

  Le codage de ce message consiste à calculer $C(x) \equiv x^c$ [n].

  Le décodage consiste à calculer $D(y) \equiv y^d$ [n].

  On a bien $D(C(x)) \equiv x^{cd} \equiv x$ [n].

- Pour chiffrer un message on a besoin de connaître c et n.

Le couple (n;c) est appelé **la clé publique** car elle est connue de tous et repertoriée dans un annuaire.

- Pour déchiffrer, il faut connaître d et n.

  d est appelé **la clé privée** car elle n'est connue que de la personne qui reçoit le message codé.

IV Notes

- Les trois lettres RSA sont les initiales de Rivest, Shamir, Adleman qui ont mis au point cet algorithme en 1978.
- Les nombres premiers p et q doivent demeurés cachés car leur connaissance entraîne celle de m = (p – 1)(q – 1), puis celle de d en résolvant l'équation de Bézout : cd – km = 1 (ce qui est possible car c est dans l'annuaire).

  Le sytème RSA 1 024 bits correspond à un nombre n = pq de l'ordre de $2^{1024} \approx 10^{308}$ s'écrivant avec 309 chiffres décimaux.

V Application 1

Alexandre veut choisir une clé publique (n;c) et sa clé privée d.

Il prend p = 5, q = 11 et donc n = 55 (p et q sont choisis petits, contrairement à la réalité, pour la simplicité des calculs).

a) Démontrer qu'il peut choisir c = 3 et d = 27.

b) Les lettres de l'alphabet sont chiffrés par :

A	B	C	D	….	Y	Z
01	02	03	04	….	25	26

Paul qui connait la clé publique d'Alexandre, crypte le message :

"VIVE LA CRYPTOGRAPHIE" et lui envoie.

Quel message crypté Alexandre reçoit-il ? Comment le décode-t-il ?

c) A l'aide du tableur Excel, implémenter les fonctionnalités suivantes :

- Vérifier que les couples (c;n) et (d;n) donnés sont corrects.
- A l'aide de formules Excel implémenter le codage et le décodage d'un message.

On pourra utiliser les fonctions Excel suivantes :

- CODE() : codage ASCII d'un caractère
- CAR() : fournit le caractère alphabétique correspondant à un code ASCII
- MOD() : donne le reste de la division euclidienne d'un nombre par un autre.

d) A quel problème est-on confronté lors de l'implémentation du décodage ?

Proposer alors deux algorithmes à implémenter avec deux procédures écrites en Visual-Basic qui contournent le problème : une de codage et une de décodage.

V Application 2

Lise a pour clé publique (n;c) avec n = pq, p = 3, q = 13.

a) Démontrer qu'elle peut choisir c = 29 et d = 5.

b) Elle reçoit le message crypté suivant de Julie :

28 01 12 21 11 12 03 28 05.

Décrypter ce message.