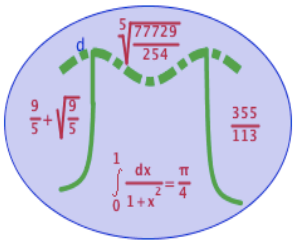

La cryptographie à clés publiques : le système RSA

I Objectifs

Présenter un système de cryptage récent.

Utiliser Python pour aider aux calculs

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.

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) On note x un entier naturel.

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, $x^{cd} \equiv x$ [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 ≡ 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) ≡ x^c [n].

  Le décodage consiste à calculer D(y) ≡ y^d [n].

  On a bien D(C(x)) ≡ x^{cd} ≡ 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 répertoriée 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.

  Par exemple

10 941 738 641 570 527 421 809 707 322 040 357 612 003 732 945 449 205 990 913 842 131 476 349 984 288 934 784 717 997 257 891 267 332 497 625 752 899 781 833 797 076 537 244 027 146 743 531 593 354 333 897

=

102 639 592 829 741 105 772 054 196 573 991 675 900 716 567 808 038 066 803 341 933 521 790 711 307 779

×

106 603 488 380 168 454 820 927 220 360 012 878 679 207 958 575 989 291 522 270 608 237 193 062 808 643

V Application 1

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

Il prend p = 17, q = 11 et donc n = 187

a) Démontrer qu'il peut choisir c = 21 et d = 61 .

b) Les lettres de l'alphabet sont chiffrés, dans l'ordre, par les entiers de 1 à 26

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

"VIVE LA CRYPTOGRAPHIE" et lui envoie.

Quel nombre doit-il chercher pour coder la lettre V ? Et pour la décoder ?

c) Afin de faciliter les calculs de restes dans la division par 187 , on décide d'implémenter un algorithme en langage python pour déterminer le nombre x tel que $x \equiv a^r(n)$

Pour cela, on part du principe suivant :

- si r est pair , x ≡ A^R (n) avec A ≡ a^2 (n) et R = r/2
- si r est impair, x ≡ $A^R \times a$ (n) avec A ≡ a^2 (n) et R = $\frac{r-1}{2}$

Sachant que le reste de la division d'un entier a par n s'écrit en langage python a%n et que l'instruction floor(x) désigne la partie entière de x , compléter le programme python ci-dessous :

```
1  from math import floor
2  def codersa(a,r,n):
3      x=1
4      while r>0:
5          if floor(r/2)==......:
6              r=.....
7              a=.....
8          else:
9              r=.....
10             x=......
11             a=......
12     print(x)
13
14 codersa(37,292,55)
```

d) Quel message Paul envoie-t-il à Alexandre ?

V Application 2

Lise a pour clé publique $(n;c)$ avec n = p q , p = 23 , q = 43.

a) Démontrer qu'elle peut choisir c = 5 et d = 185.

b) Elle reçoit le message crypté suivant de Julie :

632 1 593 520 585 593 698 632 158

Décrypter ce message.