1 Protocole RSA

Génération de clefs

Alice effectue les opérations suivantes :

- Choisir deux entiers premiers p et q, calculer $n = pq$.
- Calculer $\varphi(n) = (p-1)(q-1)$ et un entier e premier avec $\varphi(n)$.
- Calculer d tel que $de = 1 \mod \varphi(n)$

Elle publie ensuite la clef publique $pk = (n, e)$ et garde secret la clef privée $sk = d$.

Exercice 1

On considère les valeurs $p = 53$, $q = 11$ et $e = 3$.

1. Calculez la valeur publique n.
2. Calculez la fonction d'Euler $\varphi(n)$.
3. Utilisez l'algorithme étendu d'Euclide pour calculer la valeur d de la clef privée.

Chiffrement

Bob veut envoyer un message à Alice. Il cherche dans l'annuaire la clef de de chiffrement qu'elle a publiée. Il sait maintenant qu'il doit utiliser le système RSA avec les deux entiers n et e. Il transforme en nombres son message en remplaçant par exemple chaque lettre par son rang dans l'alphabet. (Exemple : "JEVOUSAIME" donne 10 05 22 15 21 19 01 09 13 05) Puis il découpe son message chiffré en blocs de même longueur (en partant de la droite) représentant chacun un nombre le plus grand possible tout en restant plus petit que n.

Exercice 2

1. Que devient le message ?
2. Pourquoi ne pas garder des blocs de taille 2 ?
3. Un bloc B est chiffré par la formule $C = B^e \mod n$. Quel message obtient Bob après avoir chiffré chaque bloc ?

Déchiffrement

Alice utilise sa clef privée d.Chacun des blocs C du message chiffré sera déchiffré par la formule $B = C^d \mod n$.
Quel message retrouve Alice ?

2 Applications

Exercice 3

Connaissant la clef publique $(n = 119, e = 5)$ de ce cryptogramme RSA 7 bits (090 086 036 067 032 001 003 031 059 031)

1. Calculez (par tous les moyens à votre disposition) p et q.
2. Calculez la clef secrète d.
3. Déchiffrez le cryptogramme.

Exercice 4

Bob choisit comme nombre premier $p = 17$ et $q = 19$, comme exposant $e = 5$. Alice et lui se fixent un protocole RSA dans lequel les messages sont des nombres en base 10 que l'on code par bloc de 2 chiffres. Alice veut envoyer le message "462739".

1. Donnez la clef publique de Bob.
2. Donnez la clef secrète d de Bob.
3. Écrivez le message chiffré que Alice envoie à Bob.
4. Déchiffrez le message qu'a reçu Bob et vérifiez que c'est bien celui qu'a envoyé Alice.

3 Devoir maison

Devoir à rendre avant le 22 mars, soit au début du cours, soit par mail à quentin.deschamps@univ-lyon1.fr. Ne pas oublier les questions au verso.

Encore du RSA

Bob utilise le protocole RSA et publie sa clef publique $n = 187$ et $e = 3$.

1. Encodez le message $m = 15$ avec la clef publique de Bob.
2. En utilisant le fait que $\varphi(n) = 160$, retrouvez la factorisation de n.
3. Retrouvez la clef privée d de Bob.

Algorithme de Pollard-Rho

On étudie dans cet exercice un algorithme de factorisation d'entiers RSA. La fonction f est une fonction pseudo-aléatoire de $\mathbb{Z}/N\mathbb{Z}$ dans $\mathbb{Z}/N\mathbb{Z}$, on pourra considérer dans la suite que f est la fonction $x \to x^2 + 1$.

Input : N, f où f est une fonction pseudo-aléatoire

$a \xleftarrow{\$} \mathbb{Z}/N\mathbb{Z}$ Élément aléatoire de $\mathbb{Z}/N\mathbb{Z}$
$(a, b) \leftarrow (a, a)$
while do
  $(a, b) \leftarrow (f(a), f(f(b))$
  $d \leftarrow pgcd(a - b, n)$
  if $1 < d < n$ **then**
    Output : d
  if $d = n$ **then**
    Output : erreur

---

1. Exécuter l'algorithme pour factoriser $N = 99$ en prenant pour f la fonction $x \to x^2 + 1$ (et un élément a aléatoire).
2. Prouver que la suite u des valeurs $a, f(a), f(f(a))...$ est périodique. En déduire que l'exécution de l'algorithme s'arrête toujours.
3. Supposons que l'algorithme renvoie une valeur (le cas d'erreur n'arrive pas). Que représente cette valeur ?

4. La fonction f étant une fonction pseudo-aléatoire, les éléments de la suite u peuvent être considérés comme aléatoires. En utilisant le paradoxe des anniversaires, en déduire l'espérance de la longueur de la période.

5. On note p et q les facteurs de n, en considérant la suite $u \mod p$, donner une estimation de la complexité de l'algorithme.

6. Quelle est la condition pour tomber dans le cas d'erreur ? Donner une estimation de sa probabilité ?