TD 2 : Le cryptosystème RSA

1 Example de protocole RSA

1.1 Génération des clés

Alice choisit :

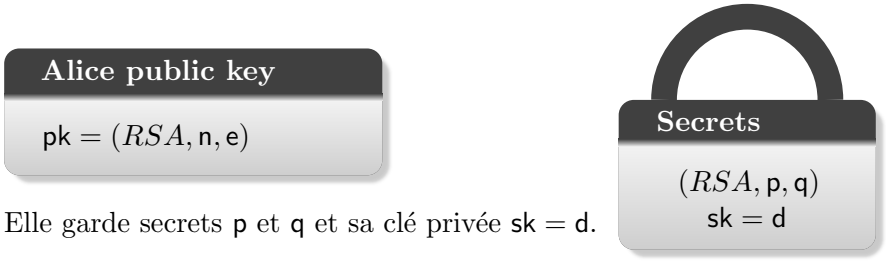
- deux entiers premiers p et q et fait leur produit $\mathsf{n} = \mathsf{p} \cdot \mathsf{q}$.
- un entier e premier avec $\varphi(\mathsf{n}) = (\mathsf{p}-1)(\mathsf{q}-1)$.

Alice calcule :

- la clé d de déchiffrage (c'est sa clef privée) qui doit satisfaire l'équation

$$\mathsf{d} \cdot \mathsf{e} = 1 \pmod{\varphi(\mathsf{n})}$$

Enfin, elle publie dans un annuaire, par exemple sur le web, sa clé publique :



Elle garde secrets p et q et sa clé privée $\mathsf{sk} = \mathsf{d}$.

Exercice 1 On considère les valeurs $\mathsf{p} = 53, \mathsf{q} = 11$ et $\mathsf{e} = 3$.
a) Calculez la valeur publique n.
b) Calculez la fonction d'Euler $\varphi(\mathsf{n}) = (\mathsf{p}-1)(\mathsf{q}-1)$.
c) Utilisez l'algorihtme etendu d'Euclid pour calculer la valeur d de la clé privée.

1.2 Chiffrement

Bob veut envoyer un message à **Alice**.
Il cherche dans l'annuaire la clé 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.

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 a) Son message devient :

010 052 ... ...

b) Pourquoi on ne garde pas la longueur 2 des bloques ?
Sur quoi on retomberait si on laissait des blocs de 2 ?

Indication : Rappellez vous le principe du chiffrement par substitution et l'attaque par l'analyse des fréquences.

Un bloc B est chiffré par la formule
$\mathsf{C} = \mathsf{B}^{\mathsf{e}} \pmod{\mathsf{n}}$

C est un bloc du message chiffré que Bob enverra à Alice.
Exemple : $\mathsf{C}_1 = 010^3 = 1000 = 417 \mod 583$

Exercice 3 Quel message obtient Bob après avoir chiffré chaque bloc ?

417 ... ...

1.3 Déchiffrement

Alice utilise sa clé privée d tq $\mathsf{e} \cdot \mathsf{d} \pmod{(\mathsf{p}-1)(\mathsf{q}-1)} = 1$.

Chacun des blocs C du message chiffré sera déchiffré par la formule

$$\mathsf{B} = \mathsf{C}^{\mathsf{d}} \pmod{\mathsf{n}}$$

Exercice 4 Quel message retrouve Alice ?

010 ... ...

En regroupant les chiffres deux par deux et en remplaçant les nombres ainsi obtenus par les lettres correspondantes, elle sait enfin le secret que Bob lui a transmis, sans que personne d'autre ne puisse le savoir.

2 Applications

Exercice 5 Connaissant la clé publique ($\mathsf{n} = 119, \mathsf{e} = 5$) de ce cryptogramme RSA 7 bits, (on considère des nombres à 7 bits soit inférieurs à $2^7 = 128$) :

090 086 036 067 032 001 003 031 059 031

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

Exercice 6 Bob choisit comme nombre premier $\mathsf{p} = 17$ et $\mathsf{q} = 19$, comme exposant $\mathsf{e} = 5$. 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 clé publique de Bob.
2. Donnez la clé secrète d de Bob.
3. Ecrivez 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.

Exercice 7 Bob utilise le protocole RSA et publie sa clé publique $\mathsf{n} = 187$ et $\mathsf{e} = 3$.
1. Encodez le message $\mathsf{m} = 15$ avec la clé publique de Bob.
2. En utilisant le fait que $\varphi(\mathsf{n}) = 160$, retrouvez la factorisation de n.
3. Retrouvez la clé privée d de Bob.

2.1 RSA avec deux facteurs trop proche

Exercice 8 Supposons que l'entier n soit le produit de deux nombres premiers p et q proches (on peut toujours supposer que $\mathsf{p} > \mathsf{q}$).
On pose $\mathsf{t} = \frac{\mathsf{p}+\mathsf{q}}{2}$ et $\mathsf{s} = \frac{\mathsf{p}-\mathsf{q}}{2}$. Montrez que :

1. L'entier s est petit.
2. $\mathsf{n} = \mathsf{t}^2 - \mathsf{s}^2$.
3. t est légérement supérieur à la racine carrée de n.
4. On peut utiliser ces informations pour factoriser n.
5. Appliquez cet algorithme pour factoriser 899, 110417, puis 364957402.
6. Trouvez la clé secrète d correspondante à $\mathsf{pk} = (RSA, \mathsf{n} = 51983, \mathsf{e} = 17)$.

Algorithme de Fermat

(a) $\mathsf{t} \leftarrow \lceil \sqrt{\mathsf{n}} \rceil$
(b) $\mathsf{z} = 2$
(c) Tant que z n'est pas un carré :
  i. $\mathsf{t} \leftarrow \mathsf{t} + 1$
  ii. $\mathsf{z} \leftarrow \mathsf{t}^2 - \mathsf{n}$
(d) Retourner $\mathsf{p} = \mathsf{t} + \sqrt{\mathsf{z}}$.

Exercice 9 Alice change sa clé RSA tous les 25 jours. Bob change sa propre clé tous les 31 jours. Sachant qu'Alice change sa clé aujourd'hui et que Bob a changé sa clé il y a trois jours, déterminer quand sera la prochaine fois qu'Alice et Bob changeront leur clé le meme jour.