Cryptographie

Solutions

Protocole RSA

Exercice 1 – $\mathsf{p} = 53, \mathsf{q} = 11, \mathsf{e} = 3$.
a) $\mathsf{n} = 583$.
b) $\varphi(\mathsf{n}) = 520$.
c) $\mathsf{d} \equiv 347 \pmod{520}$.

Exercice 2 – $\mathsf{n} = 187$ et $\mathsf{e} = 3$.
1. $\mathsf{c} \equiv \mathsf{m}^{\mathsf{e}} \equiv 15^3 \equiv 9 \pmod{187}$.
2. $\varphi(\mathsf{n}) = 160 = (17-1)(11-1)$, d'où $\mathsf{n} = 11 \times 17$.
3. $\mathsf{d} = 107$.

Exercice 3 – Avec l'algorithme d'Euclide appliqué à 25 et 31 on a l'identité de Bézout :

$$5 \cdot 25 - 4 \cdot 31 = 1.$$

Alice change sa clé aujourd'hui si et seulement si on a la congruence $x \equiv 0 \pmod{25}$. De même, Bob a changé sa clé il y a trois jours si x vérifie la congruence $x \equiv -3 \pmod{31}$. On est donc ramené à résoudre le système

$$\begin{cases} x \equiv 0 \pmod{25}, \\ x \equiv -3 \pmod{31}. \end{cases}$$

En considèrant l'identité de Bézout $5 \cdot 25 - 4 \cdot 31 = 1$, on obtient la solution particulière $x_0 = -3 \times 5 \cdot 25 = -375$ et le théorème des restes chinois affirme que la solution générale est donnée par l'expression $x = (25 \times 31)m - 375 = 775m - 375$, avec m entier. La plus petite valeur positive de x est alors $x = 400$.
La prochaine fois qu'Alice et Bob changeront leur clé le meme jour sera dans 400 jours (une année et 35 jours).

Exercice 4 – $\mathsf{p} = 17, \mathsf{q} = 19, \mathsf{e} = 5$, le message "462739".
1. $\mathsf{n} = 17 \times 19 = 323$.
2. $\varphi(\mathsf{n}) = 288$, d'où $\mathsf{d} \equiv -115 \equiv 173 \pmod{288}$.
3. $\mathsf{c}_1 = 46^5 \equiv 88 \pmod{323}$, $\mathsf{c}_2 = 27^5 \equiv -45 \pmod{323}$, $\mathsf{c}_3 = 39^5 \equiv -37 \pmod{323}$.

Cryptanalyse de RSA et factorisation

RSA avec deux facteurs trop proche

Exercice 5 – Algorithme de Fermat :
(a) Posons $\mathsf{t}_0 = \lceil \sqrt{\mathsf{n}} \rceil,\ \mathsf{z}_0 = 2$
(b) Tant que z_i n'est pas un carré :
i. Augmontons $\mathsf{t}_{\mathsf{i}+1} = \mathsf{t}_\mathsf{i} + 1$
ii. Calculons $\mathsf{z}_{\mathsf{i}+1} = \mathsf{t}_{\mathsf{i}+1}^2 - \mathsf{n}$
(c) Après avoir trouvé un z qui est un carré, posons $\mathsf{p} = \mathsf{t} + \sqrt{\mathsf{z}}$, le factor de n.

RSA avec $\varphi(\mathsf{n})$ connu

Exercice 6 – Supposons que $\mathsf{n}, \varphi(\mathsf{n})$ sont connus. Ainsi, on dispose d'un système de deux équations en p et q :

$$\begin{cases} \mathsf{pq} = \mathsf{n}, \\ \mathsf{p} + \mathsf{q} = \mathsf{n} + 1 - \varphi(\mathsf{n}). \end{cases}$$

qui donnent l'équation du second degré en X :

$$X^2 - (\mathsf{p} + \mathsf{q})X + \mathsf{pq} = 0$$

qui a comme racines p et q :

$$\mathsf{p} = \frac{\mathsf{n} + 1 - \varphi(\mathsf{n}) + \sqrt{(\mathsf{n} + 1 - \varphi(\mathsf{n}))^2 - 4\mathsf{n}}}{2}$$

$$\mathsf{q} = \frac{\mathsf{n} + 1 - \varphi(\mathsf{n}) - \sqrt{(\mathsf{n} + 1 - \varphi(\mathsf{n}))^2 - 4\mathsf{n}}}{2}$$