Cryptographie

Énoncés

Protocole RSA

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 qui doit satisfaire l'équation : $\mathsf{d} \cdot \mathsf{e} = 1 \pmod{\varphi(\mathsf{n})}$.

- **Clé publique :** $\mathsf{pk} = (\mathsf{e}, \mathsf{n})$
- **Clé secrète :** $\mathsf{sk} = \mathsf{d}$
- **Chiffrement :** $\mathsf{m} \to \mathsf{c} = \mathsf{m}^{\mathsf{e}} \pmod{\mathsf{n}}$
- **Déchiffrement :** $\mathsf{c} \to \mathsf{m} = \mathsf{c}^{\mathsf{d}} \pmod{\mathsf{n}}$

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.

Exercice 2 – 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.

Exercice 3 – Alice change sa clé publique 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.

Exercice 4 – 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.

Cryptanalyse de RSA et factorisation

RSA avec deux facteurs trop proche

Exercice 5 – 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 $\mathsf{t} = \dfrac{\mathsf{p}+\mathsf{q}}{2}$ et $\mathsf{s} = \dfrac{\mathsf{p}-\mathsf{q}}{2}$. 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, puis 110417.
6. Trouvez la clé secrète d correspondante à $\mathsf{pk} = (RSA, \mathsf{n} = 51983, \mathsf{e} = 17)$.

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

Exercice 6 – Bob utilise le protocole RSA et publie sa clé publique (e, n) où $\mathsf{n} = \mathsf{pq}$.
En utilisant la connaissance de $\varphi(\mathsf{n}) = \mathsf{pq} - \mathsf{p} - \mathsf{q} + 1$, montrez comment retrouver la factorisation de n.

Exercice 7– Montrez que la connaissance d'un couple (e, d) aide à factoriser complétement le modulo n :

1. Un tel couple (e, d) fournit une racine carrée modulaire de 1 :
   (a) Montrez que $\mathsf{ed} - 1$ est pair.
   (b) Montrez que pour tout m premier avec n : $\mathsf{m}^{\mathsf{ed}-1} = 1 \pmod{\mathsf{n}}$.
   (c) Conclure que $\mathsf{m}^{(\mathsf{ed}-1)/2}$ est une racine carrée de 1 $(\mathsf{mod}\ \mathsf{n})$.
2. Montrez que une racine carrée de 1 non triviale donne la factorisation de n en regardant l'équation $\mathsf{x}^2 - 1 = 0 \pmod{\mathsf{n}}$.
3. Appliquez le raisonement antérieur pour factoriser $\mathsf{n} = 2773$ dans le cas du protocol RSA à clé publique $(\mathsf{e}, \mathsf{n}) = (17, 2773)$ et clé privé $\mathsf{d} = 157$.

RSA avec modulo comun

Exercice 8– Bob et Charles utilisent le même modulo n pour leur clés RSA, car ils n'ont pas d'exigence de confidentialité l'un vis-à-vis de l'autre.

Bob et Charles ont pour clé publique RSA respectivement $(\mathsf{n}, \mathsf{e}_1)$ et $(\mathsf{n}, \mathsf{e}_2)$ avec e_1 et e_2 premiers entre eux. Alice envoie le même message m aux deux. Alors, m sera crypté par les clés publiques RSA de Bob et Charles en c_1 et c_2. Expliquer comment Eve, qui intercepte les deux messages cryptés et qui connait les clés publiques de Bob et Charles, peut retrouver le message clair m.