TD5 - RSA

(RSAsharedN) **Exercise 1.** *RSA with shared modulus*

1. Supposons que deux utilisateurs utilisent le même module RSA N. Le premier a une clé publique $PK_1 = (N, e_1)$ et une clé secrète $sk_1 = d_1$, et le second a une clé publique $PK_2 = (N, e_2)$ et une clé secrète $sk_2 = d_2$. Supposons ensuite que le même message $M \in (\mathbb{Z}/N\mathbb{Z})^\star$ est chiffré par chacun des utilisateurs en utilisant le chiffrement *textbook RSA* $C_1 = \text{Enc}(PK_1; M)$; $C_2 = \text{Enc}(PK_2; M)$.
Montrez que si e_1 et e_2 sont premiers entre eux, alors il est facile de retrouver M pour un adversaire qui connait PK_1, PK_2, C_1 et C_2.

(ExRSA) **Exercise 2.** *RSA*

1. On considère les valeurs $p = 53$, $q = 11$ et $e = 3$.
- Calculer la valeur publique N.
- Calculer $\varphi(N)$ la fonction d'Euler.
- Utilisez l'algorithme d'Euclide étendu pour calculer la valeur d de la clé privée.

2. Supposons que pour chiffrer un message avec le chiffrement RSA, la procédure est la suivante :
1. Remplacer chaque lettre par un nombre en prenant son rang dans l'alphabet,
2. Découper le message en blocs de taille 3 représentant un nombre le plus grand possible (inférieur à N) en partant de la droite,
3. Chiffrer chaque bloc B indépendamment en utilisant la formule $C = B^e \bmod N$.
4. Envoyer le message chiffré composé des blocs chiffrés.
Appliquer cette procédure pour renvoyer le chiffré du message "BONJOUR".

(fac) **Exercise 3.** *Factoriser connaissant $\varphi(N)$*

Soient $N = pq$ avec p et q deux premiers distincts de même taille.

1. Montrez que si $\varphi(N)$ et N sont connus, alors il est possible de trouver p et q en temps polynomial en $n = \log(N)$.

2. Pour un module $N = 2782799$ et son indicatrice $\varphi(N) = 2779440$, retrouvez avec la technique précédente les facteurs premiers p et q de N.

(phi) **Exercise 4.** *Factoriser connaissant $\varphi(N)$*

1. Calculez $\varphi(3)$, $\varphi(8)$, $\varphi(21)$.

2. Soit p un nombre premier, montrez que $\varphi(p) = p - 1$.

3. Soient p et q deux nombres premiers distincts $N = pq$, montrez que $\varphi(N) = (p-1)(q-1)$.

4. Soient p un premier et $e \geqslant 1$ un entier. Montrez que :

$$\varphi(p^e) = p^{e-1}(p-1).$$

5. Soient p, q deux premiers deux à deux. Montrez que $\varphi(pq) = \varphi(p)\varphi(q)$.

(ExRSA) **Exercise 5.** *RSA*

1. On considère les valeurs $p = 53$, $q = 11$ et $e = 3$.
- Calculer la valeur publique N.
- Calculer $\varphi(N)$ la fonction d'Euler.
- Utilisez l'algorithme d'Euclide étendu pour calculer la valeur d de la clé privée.

2. Supposons que pour chiffrer un message avec le chiffrement RSA, la procédure est la suivante :
1. Remplacer chaque lettre par un nombre en prenant son rang dans l'alphabet,
2. Découper le message en blocs de taille 3 représentant un nombre le plus grand possible (inférieur à N) en partant de la droite,
3. Chiffrer chaque bloc B indépendamment en utilisant la formule $C = B^e \bmod N$.
4. Envoyer le message chiffré composé des blocs chiffrés.
Appliquer cette procédure pour renvoyer le chiffré du message "BONJOUR".

(RSAb) **Exercise 6.** *RSA*

On rappelle le schéma de chiffrement RSA. Soit $n \geqslant 2$ (par exemple, $n = 512$).

- KeyGen. Choisir $p \neq q$ parmis tous les premiers de taille n-bits; calculer $N = p \cdot q$; choisir $d, e \in [1, \varphi(N) - 1]$ tels que $d \cdot e = 1 \bmod \varphi(N)$. La clé publique est $PK = (N, e)$, et la clé secrète est $sk = d$. *(On rappelle que $\varphi(N) = (p-1)(q-1)$).*
- Enc. Pour $M \in \mathbb{Z}/N\mathbb{Z}$, calculer et retourner $C = M^e \bmod N$.
- Dec. Pour $C \in \mathbb{Z}/N\mathbb{Z}$, calculer et retourner $M = C^d \bmod N$.

1. On veut implémenter l'algorithme de déchiffrement de RSA. Pour calculer C^d modulo $N = pq$, on calcule d'abord C^d modulo q et modulo p et on déduit $C^d \bmod N$ grâce au théorème des restes chinois. Expliquez pourquoi cet algorithm est 4 fois plus rapide que l'algorithme naïf.

2. Supposons que l'utilisateur fasse une erreur pendant le calcul de $C^d \bmod p$, mais $C^d \bmod q$ soit correctement calculé. Montrez comment un attaquant connaissant C et le message erroné $\widetilde{M}$ peut retrouver la factorisation de N.

3. Exploitez la fait que le chiffrement et le déchiffrement soient des homomorphismes multiplicatifs pour en déduire une attaque à chiffrés choisis.