Chiffrement RSA

Examen de Python/C++

Année universitaire 2023 - 2024

M. Abdoulaye Déthié Sarr

Le chiffrement RSA est un algorithme de cryptographie asymétrique largement utilisé pour la sécurité des données. Il est nommé d'après ses inventeurs, Ron **Rivest**, Adi **Shamir** et Leonard **Adleman**. Le chiffrement RSA utilise une paire de clés, une publique et une privée, pour chiffrer et déchiffrer les données. Ce projet python/C++ se concentre sur la mise en œuvre de l'algorithme de chiffrement RSA. Ce dernier utilise des opérations mathématiques basées sur l'arithmétique modulaire pour chiffrer un message.

Pour chiffrer un message en utilisant les codes ASCII et l'algorithme RSA, voici les étapes à suivre :

1. Convertir le message à chiffrer en une séquence de nombres en utilisant les codes ASCII. Chaque caractère du message est représenté par un nombre correspondant à sa valeur ASCII.

2. Sélectionner deux nombres premiers $\mathbf{p}$ et $\mathbf{q}$. Le produit de ces deux nombres est appelé $\mathbf{n}$ avec $\mathbf{n} = \mathbf{p} \times \mathbf{q}$.

3. Calculer

   $$\phi(\mathbf{n}) = (\mathbf{p}-\mathbf{1})(\mathbf{q}-\mathbf{1})$$

   ϕ est la fonction d'Euler et elle est utilisée dans le choix de la clé publique et privée.

4. Choisir un entier $\mathbf{e}$ tel que

   $$\mathbf{1} < \mathbf{e} < \phi(\mathbf{n})$$

   et $\mathbf{e}$ soit **premier** avec $\phi(\mathbf{n})$. $(\mathbf{n}, \mathbf{e})$ sera utilisé comme la clé publique.

5. Calculer $\mathbf{d}$ tel que $(\mathbf{d} \times \mathbf{e}) \ \mathbf{mod}\ \phi(\mathbf{n}) = \mathbf{1}$. $(\mathbf{n}, \mathbf{d})$ sera utilisé comme la clé privée.

6. Pour chiffrer le message, pour chaque caractère du message, calculez le nombre correspondant à l'aide de la table ASCII, puis calculez le chiffrement en utilisant la formule suivante :

   $$\mathbf{c} = (\mathbf{caractere})^{\mathbf{e}} \ \mathbf{mod}\ \mathbf{n}$$

   Le résultat obtenu $\mathbf{c}$ est le caractère chiffré.

7. Pour déchiffrer le message, pour chaque caractère chiffré, calculez le caractère d'origine en utilisant la formule suivante :

   $$\mathbf{caractere} = \mathbf{c}^{\mathbf{d}} \ \mathbf{mod}\ \mathbf{n}$$

   Le résultat obtenu est le caractère déchiffré.

Notez que la sécurité de RSA repose sur la difficulté de factoriser des nombres premiers très grands. Plus la taille des nombres premiers utilisés est grande, plus le chiffrement est sûr. Il est également important de garder les clés privées et publiques en sécurité, car toute personne ayant accès à ces clés peut déchiffrer le message.

Prenons l'exemple du message "**bonjour**" que nous allons chiffrer à l'aide de l'algorithme RSA.

1. Tout d'abord, nous devons convertir chaque caractère du message en un nombre correspondant à sa valeur ASCII. Voici les valeurs ASCII pour chaque caractère de "**bonjour**" : **98 111 110 106 111 117 114**.

2. Ensuite, nous choisissons deux nombres premiers $\mathbf{p}$ et $\mathbf{q}$. Pour cet exemple, nous choisissons $\mathbf{p = 17}$ et $\mathbf{q = 23}$. Nous calculons $\mathbf{n = p \times q = 391}$.

3. Nous calculons $\phi(\mathbf{n}) = (\mathbf{p-1})(\mathbf{q-1}) = \mathbf{352}$.

5. Nous choisissons un nombre $\mathbf{e}$ tel que $\mathbf{1 < e < \phi(n)}$ et $\mathbf{e}$ soit premier avec $\phi(\mathbf{n})$. Nous pouvons choisir $\mathbf{e = 5}$.

6. Nous calculons $\mathbf{d}$ tel que $(\mathbf{d \times e}) \ \mathbf{mod}\ \phi(\mathbf{n}) = \mathbf{1}$. Dans ce cas, $\mathbf{d = 141}$.

7. Nous avons donc notre clé publique $(\mathbf{n}, \mathbf{e}) = (\mathbf{391}, \mathbf{5})$ et notre clé privée $(\mathbf{n}, \mathbf{d}) = (\mathbf{391}, \mathbf{141})$.

8. Pour chiffrer le message, nous calculons chaque code ASCII correspondant à chaque caractère du message élevé à la puissance $\mathbf{e}$ modulo $\mathbf{n}$, en utilisant la formule :

$$\mathbf{c = (caractere)^e \ mod\ n}$$

   Voici les résultats pour chaque caractère de "bonjour" :

   b $\longrightarrow$ c $= 98^5 \bmod 391 = 308$
   o $\longrightarrow$ c $= 111^5 \bmod 391 = 107$
   n $\longrightarrow$ c $= 110^5 \bmod 391 = 3$
   j $\longrightarrow$ c $= 106^5 \bmod 391 = 296$
   o $\longrightarrow$ c $= 111^5 \bmod 391 = 107$
   u $\longrightarrow$ c $= 117^5 \bmod 391 = 38$
   r $\longrightarrow$ c $= 114^5 \bmod 391 = 23$

   Le message chiffré est donc : "**308 107 3 296 107 38 23".**

9. Pour déchiffrer le message, nous utilisons la clé privée **d** et la formule :

$$\textbf{caractere} = \textbf{c}^{\textbf{d}} \textbf{ mod n}$$

Voici les résultats pour chaque caractère chiffré :

308 ⟶ caractère = 308^{141} mod 391 = 98 (correspondant à "b")
107 ⟶ caractère = 107^{141} mod 391 = 111 (correspondant à "o")
3 ⟶ caractère = 3^{141} mod 391 = 110 (correspondant à "n")
296 ⟶ caractère = 296^{141} mod 391 = 106 (correspondant à "j")
107 ⟶ caractère = 107^{141} mod 391 = 111 (correspondant à "o")
38 ⟶ caractère = 38^{141} mod 391 = 117 (correspondant à "u")
23 ⟶ caractère = 23^{141} mod 391 = 114 (correspondant à "r")

Le message déchiffré est donc "**bonjour**".

Indications :

1. Faire des recherches sur les chaînes de caractères.
2. Faire des recherches sur les codes ASCII.
3. Deux nombres sont premiers entre eux si leur plus grand commun diviseur est 1.

NB :

1. Faire un controle de saisie pour chaque entrée de l'utilisateur.
2. L'esthétique du programme sera tenu en compte à la correction.
3. Travailler par groupe d'au maximum 3 étudiants ou individuellement.
4. Préciser dans le fichier que vous devez rendre le prénom et le nom des différents membres.
5. Envoyer le projet avant la date limite à l'adresse mail suivant : abdoulayedethie.sarr@uadb.edu.sn en mettant comme objet : **Examen Python/C++ BIG2 IAM 2023-2024**

Dateline : Dimanche 10 mars 2024 à 23h59.

GOOD LUCK!!!