Mathématiques à l'usage des informaticiens

TP2: Le code RSA.

Salmân M'hammed Abibou & Rodrigo Ferreira Rodrigues

December 5, 2022

Exercice 1

1. (a) Pour déchiffrer ce massage Alice va calculer $M' \equiv C^D \bmod N$

   (b)

$$M' \equiv C^D \bmod N$$
$$M' \equiv 17^7 \bmod 391$$
$$M' = 204$$

2. Nombres premiers p et q

   (a) On sait que $p \times q = N$ et $pgcd(p, q) = 1$. On trouve finanlement que $p = 23$ et $q = 17$.

   (b)

$$\varphi(N) = (p-1) \times (q-1)$$
$$\varphi(N) = 22 \times 16$$
$$\varphi(N) = 352$$

3. Relation entre E et D

$$D = E^{-1} \bmod \varphi(N)$$
$$D = 151^{-1} \bmod 352$$
$$D = 7^{*}$$

[*] 7 étant obtenu grâce à l'algorithme d'Euclide étendu qu'on a programmé au TP1

Exercice 2

1. (a) Chiffrement de $M = 112$

$$C = M^E \bmod N$$
$$C = 112^{11} \bmod 221$$
$$C = 2$$

   (b) Déchiffrement du cryptogramme $C = 78$

$$M' = C^D \bmod N$$
$$M' = 78^{35} \bmod 221$$
$$M' = 65$$

2. (a) Calculs de N et $\varphi(N)$

$$N = p \times q \qquad \varphi(N) = (p-1) \times (q-1)$$
$$N = 53 \times 71 \qquad \varphi(N) = 52 \times 10$$
$$N = 3763 \qquad \varphi(N) = 3640$$

   (b) Vérification et calcul de D

   On remarque $E = 307 < 3640 = \varphi(N)$ et que $pgcd(\varphi(N), E) = pgcd(3640, 307) = 1$* donc E est acceptable.

$$D = E^{-1} \bmod \varphi(N)$$
$$D = 307^{-1} \bmod 3640$$
$$D = 83$$

   (c) Elements constitutifs des clés publique et privée

   - Clé publique $= (E, N) = (307, 221)$
   - Clé privée $= D = 83$

   (d) Il faut se débarasser des éléments restants c'est-à-dire de p, q et $\varphi(N)$ puisque leur connaissance ne sera plus utile pour la suite du cryptage/décryptage et limite aussi le risque de pirater le code.

*On l'a vérifié grâce au programme qu'on a fait au TP1

Exercice 3

1. (a) Chiffrement du message "METHODE".

   (b) Déchiffrement du cryptogramme: 263;115;613;10.

   (c) Chiffrement du message "AVEZVOUSBIENREUSSI".

   (d) Déchiffrement du cryptogramme: 1019;35;567;36;384;703;99;59.

   (e) Déchiffrement du cryptogramme: 553;813.