Mathématiques à l'usage des informaticiens

TP2: Le code RSA.

Salmân M'hammed Abibou & Rodrigo Ferreira Rodrigues

December 14, 2022

Exercice 1

1. (a) Pour déchiffrer ce message 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".

   - Numériquement, le message correspond à 12; 04; 19; 07; 14; 03; 04.
   - Après concaténation on a: 120419071403040.
   - Découpe en paquets de 3 : 120; 419; 071; 403; 040.
   - Chiffrement de chaque paquet : $120^{257} \equiv 589 \bmod 1073$; $419^{257} \equiv 673 \bmod 1073$; $71^{257} \equiv 238 \bmod 1073$; $403^{257} \equiv 308 \bmod 1073$; $40^{257} \equiv 391 \bmod 1073$.
   - Le cryptogramme est **589**; **673**; **238**; **308**; **391**.

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

   - Déchriffrement de chaque paquet : $263^{353} \equiv 21 \bmod 1073$; $115^{353} \equiv 724 \bmod 1073$; $613^{353} \equiv 151 \bmod 1073$; $10^{353} \equiv 914 \bmod 1073$.
   - Message déchiffré : 021; 724; 151; 914.
   - Apres concaténation on a : 021724151914.
   - Découpe en paquets de 2 : 02; 17; 24; 15; 19; 14.
   - Le message est **CRYPTO**.

   (c) Chiffrement du message "AVEZVOUSBIENREUSSI".

   - Numériquement, le message correspond à 00; 21; 04; 25; 21; 14; 20; 18; 01; 08; 04; 13; 17; 04; 20; 18
   - Après concaténation on a: 00210425211420180108041317042018 1808.
   - Découpe en paquets de 3 : 002; 104; 252; 114; 201; 801; 080; 413; 170; 420; 181; 808.
   - Chiffrement de chaque paquet : $2^{257} \equiv 32 \bmod 1073$; $104^{257} \equiv 916 \bmod 1073$; $252^{257} \equiv 546 \bmod 1073$; $114^{257} \equiv 983 \bmod 1073$; $201^{257} \equiv 403 \bmod 1073$; $801^{257} \equiv 1001 \bmod 1073$; $80^{257} \equiv 709 \bmod 1073$; $413^{257} \equiv 857 \bmod 1073$; $170^{257} \equiv 716 \bmod 1073$; $420^{257} \equiv 1034 \bmod 1073$; $181^{257} \equiv 567 \bmod 1073$;$808^{257} \equiv 919 \bmod 1073$.
   - Le cryptogramme est **32**; **916**; **546**; **983**; **403**; **1001**; **709**; **857**; **716**; **1034**; **567**; **919**.

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

- Déchriffrement de chaque paquet : $1019^{353} \equiv 180 \bmod 1073$; $35^{353} \equiv 13 \bmod 1073$; $567^{353} \equiv 181 \bmod 1073$; $36^{353} \equiv 517 \bmod 1073$; $384^{353} \equiv 140 \bmod 1073$; $703^{353} \equiv 111 \bmod 1073$; $99^{353} \equiv 041 \bmod 1073$; $59^{353} \equiv 204 \bmod 1073$.
- Message déchiffré : 180; 013; 181; 517; 140; 111; 041; 204.
- Apres concaténation on a : 18001318151714011104120 4.
- Découpe en paquets de 2 : 18; 00; 13; 18; 15; 17; 14; 01; 11; 04; 12; 04.
- Le message est **SANSPROBLEME**.

(e) Déchiffrement du cryptogramme: 553;813.

- Déchriffrement de chaque paquet : $553^{353} \equiv 50 \bmod 1073$; $813^{353} \equiv 813 \bmod 1073$.
- Message déchiffré : 050; 813.
- Apres concaténation on a : 050813.
- Découpe en paquets de 2 : 05; 08; 13.
- Le message est **FIN**.