NOM :
PRENOM :
GROUPE :

Contrôle final
Cryptographie

Février 2019

La qualité de la rédaction ainsi que la propreté de la copie seront pris en compte dans l'évaluation.

Le but de ce problème est de déchiffrer le message `M3` suivant :

$$717 - 1695^* - 2287 - 1411 - 644 - 1158$$

Il a été obtenu par le processus suivant :

- Le message claire `M0` a été crypté en suivant le protocole RSA. On a fait des paquets de 2 lettres puis on a utilisé la clef $(3998, 631)$. On a obtenu le message `M1`. Lors de ce calcul si l'un des chiffres obtenu est supérieur à 2526 on le marque d'une étoile. Il conservera ce marquage tout au long du processus.
- Le message `M1` a été crypté en suivant la méthode de Hill avec la matrice $A = \begin{pmatrix} 43 & 45 \\ 0 & 47 \end{pmatrix}$ comme clef. On a obtenu le message `M2`.
- Le message `M2` a été crypté par un chiffrement affine de clef $(2521, 1)$. Le résultat a donné le message `M3`

Première partie. Calculs préliminaires.

1. Appliquer l'algorithme d'Euclide et l'algorithme d'Euclide étendu. 1

a	b	r	q	u	v
2521	2526				

2. Appliquer l'algorithme d'Euclide et l'algorithme d'Euclide étendu. 1

a	b	r	q	u	v
2021	2526				

3. Appliquer l'algorithme d'Euclide et l'algorithme d'Euclide étendu. 1

a	b	r	q	u	v
631	1998				

Seconde partie. Détermination des clefs de déchiffrement.

1. La clef RSA.
   (a) Montrer que 3998 est le produit de deux nombres premiers p et q. Vous justifierez précisément que p et q sont des nombres premiers. 2

   (b) Montrer que $(3998, 631)$ est une clef valide du cryptosystème RSA. 1.5

   (c) Déterminer la clef privé associé à la clef publique $(3998, 631)$. 1

2. La clef de Hill.
   (a) Calculer $\det(\mathsf{A})$ le déterminant de A. 1

   (b) Expliquer pourquoi A est une clef de chiffrement valide du chiffrement de Hill. 0.5

   (c) Déterminer la matrice A^{-1} inverse modulaire de la matrice A. 1

3. La clef affine.
   (a) Expliquez pourquoi $(2521, 1)$ est une clef valide du cryptosystème affine. 1

(b) Déterminer la clef de déchiffrement associé à $(2521, 1)$. 1

Troisième partie. Déchiffrement.

1. De `M3` à `M2`.

   (a) Appliquer la clef de déchiffrement affine pour passer de `M3` à `M2`. 1

2. De `M2` à `M1`.

   (a) Expliquer comment réaliser le produit $A^{-1} \times \begin{pmatrix} 362 \\ 1682 \end{pmatrix}$. 0.5

   (b) Appliquer la clef de déchiffrement de Hill pour passer de `M2` à `M1`. 1

3. De `M1` à `M0`.

   (a) Déterminer L'écriture binaire de 19. 0.5

   (b) On a appliqué l'algorithme d'exponentiation modulaire rapide et on a obtenue les tableaux suivants. Déduire de ces tableaux 2162^{19}, 2938^{19}, 1476^{19}, 1636^{19} et 769^{19} modulo 3998. 2.5

k	0	1	2	3	4
2162^{2^k}	2162	4674244	338724	8363664	14791716
	2162	582	2892	3846	3114

k	0	1	2	3	4
2938^{2^k}	2938	8631844	26244	5089536	6724
	2938	162	2256	82	2726

k	0	1	2	3	4
1476^{2^k}	1476	2178576	13424896	13032100	6853924
	1476	3664	3610	2618	1352

k	0	1	2	3	4
1636^{2^k}	1636	2676496	3363556	1532644	1988100
	1636	1834	1238	1410	1094

k	0	1	2	3	4
769^{2^k}	769	591361	13359025	2913849	10923025
	769	3655	1707	3305	489

(c) Appliquer l'algorithme d'exponentiation modulaire rapide et calculer 2520^{19}. 1.5

(d) Déterminer `M0`. 1