RSA

Exercice 1

Appliquer la méthode du crible d'Eratosthène et entourer les nombres premiers de la liste suivante.

0	1	2	3	4	5	6	7	8	9
10	11	12	13	14	15	16	17	18	19
20	21	22	23	24	25	26	27	28	29
30	31	32	33	34	35	36	37	38	39
40	41	42	43	44	45	46	47	48	49
50	51	52	53	54	55	56	57	58	59
60	61	62	63	64	65	66	67	68	69
70	71	72	73	74	75	76	77	78	79
80	81	82	83	84	85	86	87	88	89
90	91	92	93	94	95	96	97	98	99

Exercice 2

Compléter le tableau suivant sachant que $p < q$ sont deux nombres premiers, $n = pq$, $\varphi = (p-1)(q-1)$ et e et d sont des nombres premiers à φ inverse l'un de l'autre.

p	q	n	φ	e	d
3	13			11	
7	41			13	
139	101				43
2		202			19
		77		47	
		437			23
			32	7	
			16		5
		3599	3480	1001	
		1341517	1339200		433

Exercice 3

Calculer les nombres suivants.

1. 71^{21} modulo 65
2. 33^{19} modulo 130
3. 123^{43} modulo 98
4. 301^{17} modulo 59
5. 1000^{55} modulo 99
6. 2^{666} modulo 2015

Exercice 4

On considère dans le système RSA, la clef publique $(1763, 929)$.

1. Déterminer deux entiers p et q tel que $p < q$ et $1763 = pq$.
2. Justifier que $(1763, 929)$ est une clef publique valide du cryptosystème RSA.
3. (a) Déterminer la décomposition de 929 en binaire.
   (b) Calculer 18^{929} modulo 1763.

(c) Quel est le message chiffré de $M = 18$.

4. Déterminer la clef privé associée à la clef publique $(1763, 929)$.
5. Déchiffrer le message $M' = 884$

Exercice 5

On considère dans le système RSA, la clef publique $(1189, 1031)$.

1. Déterminer deux entiers p et q tel que $p < q$ et $1189 = pq$.
2. Justifier que $(1189, 1031)$ est une clef publique valide du cryptosystème RSA.
3. (a) Déterminer la décomposition de 1031 en binaire.

   (b) Calculer 44^{1031} modulo 1189.

   (c) Quel est le message chiffré de $M = 44$.
4. Déterminer la clef privé associée à la clef publique $(1189, 1031)$.
5. Déchiffrer le message $M' = 583$

Exercice 6

Chiffrer le message suivant en RSA par la clef publique $(4559, 1705)$: CHIFFREMENTRSA.

Exercice 7

Déchiffrer le message suivant chiffrer en RSA de clef publique $(2047, 1931)$ et de clef privée inconnue :
$1141 - 2 - 1878 - 425 - 128 - 64 - 64 - 2 - 1434 - 1516 - 64 - 19 - 128 - 64$.

Exercice 8

Déchiffrer le message suivant chiffrer en RSA de clef publique $(444931, 97919)$ et de clef privée inconnue :
$32755 - 394934 - 234962 - 412077 - 169502 - 187788 - 83769$