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

Parmi les nombres suivants identifier ceux qui sont des nombres premiers.

1. 103
2. 247
3. 367
4. 539
5. 587
6. 597
7. 683
8. 693
9. 701
10. 787
11. 809
12. 909
13. 989
14. 991
15. 997
16. 1009
17. 1211
18. 1311
19. 1319
20. 1321

Exercice 3

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	
101	139				43
2		202			19
		77		47	
		437			23
			18		5
			16		5
			32	7	
		3599	3480	1001	
		1341517	1339200		433
		n	φ	$n-1$	

Exercice 4

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 5

On considère dans le système RSA, la clef publique $(319, 11)$.

1. Déterminer deux nombres premiers p et q tel que $p < q$ et $319 = pq$.
2. Justifier que $(319, 11)$ est une clef valide du cryptosystème RSA.
3. (a) Déterminer la décomposition de 11 en base 2.
   (b) Calculer 100^{11} modulo 319.
   (c) Quel est le message chiffré de $M = 100$?
4. Déterminer la clef privé associée à $(319, 11)$.
5. Déchiffrer le message $M' = 133$

Exercice 6

On considère dans le système RSA, la clef publique $(2581, 493)$.

1. Déterminer deux nombres premiers p et q tel que $p < q$ et $2581 = pq$.
2. Justifier que $(2581, 493)$ est une clef valide du cryptosystème RSA.
3. (a) Déterminer la décomposition de 493 en base 2.
   (b) Calculer 1421^{493} et 1308^{493} modulo 2581.
   (c) Quel est le message chiffré de *OVNI* ?
4. Déterminer la clef privé associée à $(2581, 493)$.
5. Déchiffrer le message *1972-2032*.

Exercice 7

Un professeur envoie ses notes au secrétariat de l'école par mail. La clef publique du professeur est $(55, 3)$ et celle du secrétariat est $(33, 3)$.

1. Déterminer les clefs privés du professeur et du secrétariat.
2. Pour assurer la confidentialité de ses messages, le professeur chiffre les notes avec la clef publique du secrétariat. Quel message chiffré correspond la note de 12 ?
3. Pour assurer l'authenticité des messages contenants les notes, le professeur signe ses messages pour le secrétariat après les avoir chiffrés. Le secrétariat reçoit le message 23. Quelle est la note correspondante ?

Exercice 8

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

Exercice 9

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 10

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