

Midterm

Duration: 30 minutes

Documents and calculators are prohibited. Problems are independent from each other. Make sure to show your work and to justify each answer with care. The back of this sheet provides computations that may or may not be useful.

Problem I (7.5 points)

We consider a variant of the one-time-pad cipher based on two keys (or pads). Let K_1 and K_2 be the keys, consider

$$K = K_1 \oplus K_2$$

and C the one-time-pad cipher based on K . (We note \oplus the xor operator).

1. Is the cipher C secure if K_1 and K_2 are chosen randomly?
2. Let r be the fonction reversing the order of the bits of a pad (*e.g.* $r(10110)=01101$). Is the cipher C secure if K_1 is chosen randomly and $K_2 = r(K_1)$?
3. Is the cipher C secure if K_1 is chosen randomly and $K_2 = K_1$?

Problem II (12.5 points)

We consider $n = 77$, $e = 13$, $d = 37$ and we note:

$$K_{\text{PUBLIC}} = (n, e)$$

$$K_{\text{PRIVATE}} = (n, d)$$

1. Encrypt the message $M = 26$, using RSA, with key K_{PUBLIC} .
2. Decrypt the ciphered message you obtained in the previous question with key K_{PRIVATE} .
3. The numbers involved in the keypair are incredibly small. Recover K_{PRIVATE} from K_{PUBLIC} .

13^{13}	mod 13	=	0	13^{13}	mod 37	=	19	13^{13}	mod 60	=	13
13^{13}	mod 66	=	19	13^{13}	mod 70	=	13	13^{13}	mod 75	=	28
13^{13}	mod 77	=	41	13^{13}	mod 80	=	13	13^{13}	mod 88	=	85
20^{13}	mod 13	=	7	20^{13}	mod 37	=	2	20^{13}	mod 60	=	20
20^{13}	mod 66	=	14	20^{13}	mod 70	=	20	20^{13}	mod 75	=	50
20^{13}	mod 77	=	69	20^{13}	mod 80	=	0	20^{13}	mod 88	=	80
26^{13}	mod 13	=	0	26^{13}	mod 37	=	26	26^{13}	mod 60	=	56
26^{13}	mod 66	=	20	26^{13}	mod 70	=	26	26^{13}	mod 75	=	26
26^{13}	mod 77	=	75	26^{13}	mod 80	=	16	26^{13}	mod 88	=	64
37^{13}	mod 13	=	11	37^{13}	mod 37	=	0	37^{13}	mod 60	=	37
37^{13}	mod 66	=	31	37^{13}	mod 88	=	53	37^{13}	mod 85	=	12
37^{13}	mod 70	=	37	37^{13}	mod 77	=	9	37^{13}	mod 80	=	37
75^{13}	mod 13	=	10	75^{13}	mod 37	=	1	75^{13}	mod 60	=	15
75^{13}	mod 66	=	3	75^{13}	mod 88	=	3	75^{13}	mod 85	=	40
75^{13}	mod 70	=	5	75^{13}	mod 77	=	47	75^{13}	mod 80	=	75
77^{13}	mod 13	=	12	77^{13}	mod 37	=	30	77^{13}	mod 60	=	17
77^{13}	mod 66	=	11	77^{13}	mod 88	=	77	77^{13}	mod 85	=	42
77^{13}	mod 70	=	7	77^{13}	mod 77	=	0	77^{13}	mod 80	=	77
13^{37}	mod 13	=	0	13^{37}	mod 37	=	13	13^{37}	mod 60	=	13
13^{37}	mod 66	=	7	13^{37}	mod 70	=	13	13^{37}	mod 75	=	58
13^{37}	mod 77	=	62	13^{37}	mod 80	=	13	13^{37}	mod 88	=	29
20^{37}	mod 13	=	7	20^{37}	mod 37	=	20	20^{37}	mod 60	=	20
20^{37}	mod 66	=	26	20^{37}	mod 70	=	20	20^{37}	mod 75	=	50
20^{37}	mod 77	=	48	20^{37}	mod 80	=	0	20^{37}	mod 88	=	48
26^{37}	mod 13	=	0	26^{37}	mod 37	=	26	26^{37}	mod 60	=	56
26^{37}	mod 66	=	38	26^{37}	mod 88	=	16	26^{37}	mod 85	=	76
26^{37}	mod 70	=	26	26^{37}	mod 77	=	5	26^{37}	mod 80	=	16
37^{37}	mod 13	=	11	37^{37}	mod 37	=	0	37^{37}	mod 60	=	37
37^{37}	mod 66	=	49	37^{37}	mod 88	=	5	37^{37}	mod 85	=	22
37^{37}	mod 70	=	37	37^{37}	mod 77	=	16	37^{37}	mod 80	=	37
75^{37}	mod 13	=	10	75^{37}	mod 37	=	1	75^{37}	mod 60	=	15
75^{37}	mod 66	=	15	75^{37}	mod 88	=	59	75^{37}	mod 85	=	45
75^{37}	mod 70	=	5	75^{37}	mod 77	=	26	75^{37}	mod 80	=	75
77^{37}	mod 13	=	12	77^{37}	mod 37	=	3	77^{37}	mod 60	=	17
77^{37}	mod 66	=	11	77^{37}	mod 88	=	77	77^{37}	mod 85	=	42
77^{37}	mod 70	=	7	77^{37}	mod 77	=	0	77^{37}	mod 80	=	77
13^{77}	mod 13	=	0	13^{77}	mod 37	=	35	13^{77}	mod 60	=	13
13^{77}	mod 66	=	7	13^{77}	mod 70	=	13	13^{77}	mod 75	=	58
13^{77}	mod 77	=	62	13^{77}	mod 80	=	13	13^{77}	mod 88	=	29
20^{77}	mod 13	=	11	20^{77}	mod 37	=	18	20^{77}	mod 60	=	20
20^{77}	mod 66	=	26	20^{77}	mod 70	=	20	20^{77}	mod 75	=	50
20^{77}	mod 77	=	48	20^{77}	mod 80	=	0	20^{77}	mod 88	=	48
26^{77}	mod 13	=	0	26^{77}	mod 37	=	10	26^{77}	mod 60	=	56
26^{77}	mod 66	=	38	26^{77}	mod 88	=	16	26^{77}	mod 85	=	76
26^{77}	mod 70	=	66	26^{77}	mod 77	=	38	26^{77}	mod 80	=	16
37^{77}	mod 13	=	7	37^{77}	mod 37	=	0	37^{77}	mod 60	=	37
37^{77}	mod 66	=	49	37^{77}	mod 88	=	5	37^{77}	mod 85	=	12
37^{77}	mod 70	=	67	37^{77}	mod 77	=	60	37^{77}	mod 80	=	37
75^{77}	mod 13	=	4	75^{77}	mod 37	=	1	75^{77}	mod 60	=	15
75^{77}	mod 66	=	15	75^{77}	mod 88	=	59	75^{77}	mod 85	=	40
75^{77}	mod 70	=	45	75^{77}	mod 77	=	59	75^{77}	mod 80	=	75
77^{77}	mod 13	=	12	77^{77}	mod 37	=	21	77^{77}	mod 60	=	17
77^{77}	mod 66	=	11	77^{77}	mod 88	=	77	77^{77}	mod 85	=	42
77^{77}	mod 70	=	7	77^{77}	mod 77	=	0	77^{77}	mod 80	=	77