3 Cryptographie

Exercice 3.1 Pour $n \in \mathbb{N}^*$, on note $\varphi(n)$ le nombre d'entiers k premier avec n tels que $1 \leq k \leq n$.
Soit $n = pq$, où p et q sont deux nombres premiers p et q distincts.

1. À quoi est égal $\varphi(n)$?
2. Montrer que si l'on connait n et $\varphi(n)$, on peut retrouver facilement p et q.
3. Application : $n = 391 = pq$ et $\varphi(n) = 352$. Calculer p et q.

Exercice 3.2 Dans un cryptosystème utilisant la méthode RSA, déterminer la clé secrète $(\varphi(n), d)$ et le message envoyé $M \in \mathbb{Z}/n\mathbb{Z}$ pour les clés publiques (n, e) et les messages cryptés reçus $C = M^e$ suivants :

1. $n = 35$, $e = 5$, $C = 10$.
2. $n = 265$, $e = 139$, $C = 10$.

Exercice 3.3 Alice et Bob communiquent en utilisant la méthode RSA. Bob cherche donc deux nombres premiers p et q, et calcule leur produit $n = 253$. Il rend public le couple $(n, 13)$.

1. Quelle est la clé secrète de Bob ?
2. Alice veut transmettre le message $M = 2$ à Bob. Quel message crypté C ce dernier va-t-il recevoir ?
3. Bob a reçu d'Alice le message crypté $C = 22$. Quel est le message M qu'Alice lui a envoyé ?

Exercice 3.4 Soit $P = X^4+X+1 \in \mathbb{F}_2[X]$. On note $\mathbb{K} = \mathbb{F}_2[X]/P.\mathbb{F}_2[X]$ et α la classe de X dans $\mathbb{K}$.

1. Montrer P est irréductible dans $\mathbb{F}_2[X]$.
2. Montrez que $\mathbb{K}$ est un corps. Combien possède-t-il d'éléments ?
3. Quel est l'inverse de $1 + \alpha + \alpha^2$ dans $\mathbb{K}$?
4. Montrer α est un générateur de $\mathbb{K}^*$.

Exercice 3.5 On utilise le corps $\mathbb{K}$ et son générateur α construit à l'exercice 3.4.
Alice a choisit un entier e qu'elle a gardé secret et a rendu public l'élément $\alpha^e = \alpha^2 + 1 \in \mathbb{K}$.
Bob envoie des messages à Alice en utilisant l'algorithme de El Gamal.

1. Bob veut coder le message $M = 1+\alpha$ pour l'envoyer à Alice, en utilisant $x = 3$. Que transmet-il à Alice ?
2. Même question avec $M = \alpha^3 + \alpha$ et $x = 4$.
3. Vous decidez de casser le code d'Alice. Ceci fait, vous interceptez le message $(\alpha^3, \alpha^3 + \alpha^2 + \alpha)$ i.e. le couple $(\alpha^x, M\alpha^{xe})$. Quel était le message M de Bob ?

Exercice 3.6 Soit $Q = X^3-X+1 \in \mathbb{F}_3[X]$. On note $\mathbb{L} = \mathbb{F}_3[X]/Q.\mathbb{F}_3[X]$ et β la classe de X dans $\mathbb{L}$.

1. Montrer Q est irréductible dans $\mathbb{F}_3[X]$.
2. Montrez que $\mathbb{L}$ est un corps. Combien possède-t-il d'éléments ?
3. Calculer β^3, β^9 puis β^{12} et montrer enfin que $\beta^{13} = -1$.
4. Montrer β est un générateur de $\mathbb{L}^*$.

Exercice 3.7 On utilise le corps $\mathbb{L}$ et son générateur β construit à l'exercice 3.6.
Alice et Bob décident de fabriquer une clef γ à l'aide du protocole de Diffie-Helman et d'échanger des messages cryptés avec cette clef.
Alice choisit $a = 9$. Bob choisit un entier b et envoie à Alice $\beta^b = -\beta^2 + \beta - 1$.

1. Calculer la clé secrète γ d'Alice et Bob ?
2. Alice souhaite faire passer à Bob le message $M = \beta^2 - 1$. Elle lui transmet le message crypté $C = M\gamma$. Calculer C.
3. En réponse, Alice reçoit le message crypté $C' = -\beta$. Quel est le message M' de Bob ?

Exercice 3.8 On considère le cryptosystème (sans clé) suivant : un grand nombre entier p est public ; les messages sont des éléments de $(\mathbb{F}_p)^*$ (représentés par des entiers M tels que $1 \leq M \leq p-1$) ; si Alice veut envoyer un message M à Bob, ils procèdent comme suit :

(a) Alice choisit un entier a premier avec $p-1$ et tel que $1 < a < p-1$.
Elle envoie à Bob $C = M^a \in (\mathbb{F}_p)^*$.

(b) Bob choisit un entier b premier avec $p-1$ et tel que $1 < b < p-1$.
Il envoie à Alice $D = C^b \in (\mathbb{F}_p)^*$

(c) Alice calcule l'inverse a' de a dans $\mathbb{Z}/(p-1)\mathbb{Z}$.
Elle renvoie à Bob $E = D^{a'} \in (\mathbb{F}_p)^*$.

(d) Bob calcule l'inverse b' de b dans $\mathbb{Z}/(p-1)\mathbb{Z}$.
Il calcule enfin $F = E^{b'} \in (\mathbb{F}_p)^*$.

On admettra (cf. le cours) que si $a \in (\mathbb{F}_p)^*$, alors $a^{p-1} = 1$.

1. Montrer que $F = M$.
2. Faire les calculs pour $p = 47$, $a = 5$, $b = 11$ et $M = 10$.
(La table de multiplication de $\mathbb{F}_{47}$ est donnée en annexe.)

Table de multiplication de $\mathbb{F}_{47}$

×	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
2	4	6	8	10	12	14	16	18	20	22	24	26	28	30	32	34	36	38	40	42	44	46	1	3	5	7	9	11	13	15	17	19	21	23	25	27	29	31	33	35	37	39	41	43	45
3	6	9	12	15	18	21	24	27	30	33	36	39	42	45	1	4	7	10	13	16	19	22	25	28	31	34	37	40	43	46	2	5	8	11	14	17	20	23	26	29	32	35	38	41	44
4	8	12	16	20	24	28	32	36	40	44	1	5	9	13	17	21	25	29	33	37	41	45	2	6	10	14	18	22	26	30	34	38	42	46	3	7	11	15	19	23	27	31	35	39	43
5	10	15	20	25	30	35	40	45	3	8	13	18	23	28	33	38	43	1	6	11	16	21	26	31	36	41	46	4	9	14	19	24	29	34	39	44	2	7	12	17	22	27	32	37	42
6	12	18	24	30	36	42	1	7	13	19	25	31	37	43	2	8	14	20	26	32	38	44	3	9	15	21	27	33	39	45	4	10	16	22	28	34	40	46	5	11	17	23	29	35	41
7	14	21	28	35	42	2	9	16	23	30	37	44	4	11	18	25	32	39	46	5	12	19	26	33	40	1	8	15	22	29	36	43	3	10	17	24	31	38	45	6	13	20	27	34	40
8	16	24	32	40	1	9	17	25	33	41	2	10	18	26	34	42	3	11	19	27	35	43	4	12	20	28	36	44	5	13	21	29	37	45	6	14	22	30	38	7	15	23	31	39	46
9	18	27	36	45	7	16	25	34	43	6	15	24	33	42	5	14	23	32	41	4	13	22	31	40	3	12	21	30	39	2	11	20	29	38	1	10	19	28	37	9	18	27	36	45	8
10	20	30	40	3	13	23	33	43	6	16	26	36	46	9	19	29	39	2	12	22	32	42	5	15	25	35	45	8	18	28	38	1	11	21	31	41	4	14	24	34	44	7	17	27	37

×	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
11	22	33	44	8	19	30	41	5	16	27	38	2	13	24	35	46	10	21	32	43	7	18	29	40	4	15	26	37	1	12	23	34	45	9	20	31	42	6	17	28	39	3	14	25	36
12	24	36	1	13	25	37	2	14	26	38	3	15	27	39	4	16	28	40	5	17	29	41	6	18	30	42	7	19	31	43	8	20	32	44	9	21	33	45	10	22	34	46	11	23	35
13	26	39	5	18	31	44	10	23	36	2	15	28	41	7	20	33	46	12	25	38	4	17	30	43	9	22	35	1	14	27	40	6	19	32	45	11	24	37	3	16	29	42	8	21	34
14	28	42	9	23	37	4	18	32	46	13	27	41	8	22	36	3	17	31	45	12	26	40	7	21	35	2	16	30	44	11	25	39	6	20	34	1	15	29	43	10	24	38	5	19	33
15	30	45	13	28	43	11	26	41	9	24	39	7	22	37	5	20	35	3	18	33	1	16	31	46	14	29	44	12	27	42	10	25	40	8	23	38	6	21	36	4	19	34	2	17	32
16	32	1	17	33	2	18	34	3	19	35	4	20	36	5	21	37	6	22	38	7	23	39	8	24	40	9	25	41	10	26	42	11	27	43	12	28	44	13	29	45	14	30	46	15	31
17	34	4	21	38	8	25	42	12	29	46	16	33	3	20	37	7	24	41	11	28	2	19	36	6	23	40	10	27	44	14	31	1	18	35	5	22	39	9	26	43	13	30	47	17	34
18	36	7	25	43	14	32	3	21	39	10	28	46	17	35	6	24	42	13	31	2	20	38	9	27	45	16	34	5	23	41	12	30	1	19	37	8	26	44	15	33	4	22	40	11	29
19	38	10	29	1	20	39	11	30	2	21	40	12	31	3	22	41	13	32	4	23	42	14	33	5	24	43	15	34	6	25	44	16	35	7	26	45	17	36	8	27	46	18	37	9	28
20	40	13	33	6	26	46	19	39	12	32	5	25	45	18	38	11	31	4	24	44	17	37	10	30	3	23	43	16	36	9	29	2	22	42	15	35	8	28	1	21	41	14	34	7	27

×	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
21	42	16	37	11	32	6	27	1	22	43	17	38	12	33	7	28	2	23	44	18	39	13	34	8	29	3	24	45	19	40	14	35	9	30	4	25	46	20	41	15	36	10	31	5	26
22	44	19	41	16	38	13	35	10	32	7	29	4	26	1	23	45	20	42	17	39	14	36	11	33	8	30	5	27	2	24	46	21	43	18	40	15	37	12	34	9	31	6	28	3	25
23	46	22	45	21	44	20	43	19	42	18	41	17	40	16	39	15	38	14	37	13	36	12	35	11	34	10	33	9	32	8	31	7	30	6	29	5	28	4	27	3	26	2	25	1	24
24	1	25	2	26	3	27	4	28	5	29	6	30	7	31	8	32	9	33	10	34	11	35	12	36	13	37	14	38	15	39	16	40	17	41	18	42	19	43	20	44	21	45	22	46	23
25	3	28	6	31	9	34	12	37	15	40	18	43	21	46	24	2	27	5	30	33	36	39	42	45	1	4	7	10	13	16	19	22	25	28	31	34	37	40	43	46	2	5	8	11	14
26	5	31	10	36	15	41	20	46	25	4	30	9	35	14	40	19	45	24	3	29	8	34	13	39	18	44	23	2	28	7	33	12	38	17	43	22	1	27	6	32	11	37	16	42	21
27	7	34	14	41	21	1	28	8	35	15	42	22	2	29	9	36	16	43	23	3	30	10	37	17	44	24	4	31	11	38	18	45	25	5	32	12	39	19	46	26	6	33	13	40	20
28	9	37	18	46	27	8	36	17	45	26	7	35	16	44	25	6	34	15	43	24	5	33	14	42	23	4	32	13	41	22	3	31	12	40	21	2	30	11	39	20	1	29	10	38	19
29	11	40	22	4	33	15	44	26	8	37	19	1	30	12	41	23	5	34	16	45	27	9	38	20	2	31	13	42	24	6	35	17	46	28	10	39	21	3	32	14	43	25	7	36	18
30	13	43	26	9	39	22	5	35	18	1	31	14	44	27	10	40	23	6	36	19	2	32	15	45	28	11	41	24	7	37	20	3	33	16	46	29	12	42	25	8	38	21	4	34	17

×	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
31	15	46	30	14	45	29	13	44	28	12	43	27	11	42	26	10	41	25	9	40	24	8	39	23	7	38	22	6	37	21	5	36	20	4	35	19	3	34	18	2	33	17	1	32	16
32	17	2	34	19	4	36	21	6	38	23	8	40	25	10	42	27	12	44	29	14	46	31	16	1	33	18	3	35	20	5	37	22	7	39	24	9	41	26	11	43	28	13	45	30	15
33	19	5	38	24	10	43	29	15	1	34	20	6	39	25	11	44	30	16	2	35	21	7	40	26	12	45	31	17	3	36	22	8	41	27	13	46	32	18	4	37	23	9	42	28	14
34	21	8	42	29	16	3	37	24	11	45	32	19	6	40	27	14	1	35	22	9	43	30	17	4	38	25	12	46	33	20	7	41	28	15	2	36	23	10	44	31	18	5	39	26	13
35	23	11	46	34	22	10	45	33	21	9	44	32	20	8	43	31	19	7	42	30	18	6	41	29	17	5	40	28	16	4	39	27	15	3	38	26	14	2	37	25	13	1	36	24	12
36	25	14	3	39	28	17	6	42	31	20	9	45	34	23	12	1	37	26	15	4	40	29	18	7	43	32	21	10	46	35	24	13	2	38	27	16	5	41	30	19	8	44	33	22	11
37	27	17	7	44	34	24	14	4	41	31	21	11	1	38	28	18	8	45	35	25	15	5	42	32	22	12	2	39	29	19	9	46	36	26	16	6	43	33	23	13	3	40	30	20	10
38	29	20	11	2	40	31	22	13	4	42	33	24	15	6	44	35	26	17	8	46	37	28	19	10	1	39	30	21	12	3	41	32	23	14	5	43	34	25	16	7	45	36	27	18	9
39	31	23	15	7	46	38	30	22	14	6	45	37	29	21	13	5	44	36	28	20	12	4	43	35	27	19	11	3	42	34	26	18	10	2	41	33	25	17	9	1	40	32	24	16	8
40	33	26	19	12	5	45	38	31	24	17	10	3	43	36	29	22	15	8	1	41	34	27	20	13	6	46	39	32	25	18	11	4	44	37	30	23	16	9	2	42	35	28	21	14	7

×	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
41	35	29	23	17	11	5	46	40	34	28	22	16	10	4	45	39	33	27	21	15	9	3	44	38	32	26	20	14	8	2	43	37	31	25	19	13	7	1	42	36	30	24	18	12	6
42	37	32	27	22	17	12	7	2	44	39	34	29	24	19	14	9	4	46	41	36	31	26	21	16	11	6	1	43	38	33	28	23	18	13	8	3	45	40	35	30	25	20	15	10	5
43	39	35	31	27	23	19	15	11	7	3	46	42	38	34	30	26	22	18	14	10	6	2	45	41	37	33	29	25	21	17	13	9	5	1	44	40	36	32	28	24	20	16	12	8	4
44	41	38	35	32	29	26	23	20	17	14	11	8	5	2	46	43	40	37	34	31	28	25	22	19	16	13	10	7	4	1	45	42	39	36	33	30	27	24	21	18	15	12	9	6	3
45	43	41	39	37	35	33	31	29	27	25	23	21	19	17	15	13	11	9	7	5	3	1	46	44	42	40	38	36	34	32	30	28	26	24	22	20	18	16	14	12	10	8	6	4	2
46	45	44	43	42	41	40	39	38	37	36	35	34	33	32	31	30	29	28	27	26	25	24	23	22	21	20	19	18	17	16	15	14	13	12	11	10	9	8	7	6	5	4	3	2	1