Cryptography

Chapter 1

Exercise 1

Prime	Non Prime
101	$111 = 3 \times 37$
131	$121 = 11 \times 11$
151	$141 = 3 \times 47$
181	$161 = 7 \times 23$
191	$171 = 3^2 \times 19$
313	$303 = 3 \times 101$
353	$323 = 17 \times 19$
373	$333 = 3^3 \times 37$
383	$343 = 7^3$
	$363 = 3 \times 11^2$
	$393 = 3 \times 131$

Exercise 2. ☺

We have $792 = 2^3 \times 3^2 \times 11$

So there is $(3+1)(2+1)(1+1) = 4 \times 3 \times 2 = 24$ divisors

Exercise 3

We want $ax = b$ with $b \mid ax$ and x smallest possible

$x = 13^4 11^4 3^5$

Exercise 4

735 and 133

$735 = 133 \times 5 + 70$
$133 = 70 \times 1 + 63$
$70 = 63 \times 1 + 7$
$63 = 7 \times 9 + 0$

r	q	U	V
735	X	0	1
133	X	+1	-0
70	5	-5	+1
63	1	+6	-1
7	1	-11	+2
0	9	+105	-19

Cryptography

Chapter 1

Exercise 1

Prime	Non Prime
101	$111 = 3 \times 37$
131	$121 = 11 \times 11$
151	$141 = 3 \times 47$
181	$161 = 7 \times 23$
191	$171 = 3^2 \times 19$
313	$303 = 3 \times 101$
353	$323 = 17 \times 19$
373	$333 = 3^3 \times 37$
383	$343 = 7^3$
	$363 = 3 \times 11^2$
	$393 = 3 \times 131$

Exercise 2 . ⁂

We have $792 = 2^3 \times 3^2 \times 11$

So there is $(3+1)(2+1)(1+1) = 4 \times 3 \times 2 = 24$ divisors

Exercise 3

We want $ax = b$ with $b \mid ax$ and x smallest possible

$x = 13^4 11^4 3^5$

Exercise 4

735 and 133

$735 = 133 \times 5 + 70$
$133 = 70 \times 1 + 63$
$70 = 63 \times 1 + 7$
$63 = 7 \times 9 + 0$

r	q	U	V
735	X	0	1
133	X	+1	-0
70	5	-5	+1
63	1	+6	-1
7	1	-11	+2
0	9	+105	-19

Exercise 5.

$2160u + 756v = 2160 \wedge 756$

1) $2160 = 756 \times 2 + 648$
$758 = 648 \times 1 + 108$
$648 = 108 \times 6 + 0$

So $2160 \wedge 756 = 108$

2) Using Euclide extended Algorithm

r	q	U	V
2160	x	0	1
758	x	+1	-0
648	2	-2	+1
108	1	+3	-1
0	6	-20	+7

So $(-1, 3)$ is a solution

3) $2160x + 756y = 324$

We know that $2160 \times -1 + 756 \times 3 = 108$

Having: $3 \times (2160 \times -1 + 756 \times 3) = 324$

We have $2160 \times -3 + 756 \times 9 = 324$

Thus $(-3, 9)$ is a solution

Exercise 6

- $\overline{27}^{25}$ in $\mathbb{Z}/11\mathbb{Z}$ $\rightarrow \overline{27} = \overline{5}$

$\overline{5}^2 = \overline{25} = \overline{3}$
$\overline{5}^3 = \overline{125} = \overline{4}$

$\overline{5}^{-2} \times \overline{5}^{-3} = \overline{5}^{5} = \overline{3} \times \overline{4} = \overline{12} = \overline{1}$

$25 = 5 \times 5 = (2+3) \times (2+3)$

So $\overline{27}^{25} = \overline{1}$

- $\overline{6}^{51} = \overline{6}^{50} \times \overline{6} = \overline{6}^{25 \times 2} \times \overline{6}$

$\overline{6}^{2} = \overline{36} = \overline{1}$

$\overline{1}^{25} = \overline{1}$

So $\overline{6}^{51} = \overline{6}$

- $\overline{8}^{47} = \overline{8}^{45+2} = \overline{8}^{45} \times \overline{8}^{2}$

$\overline{8}^{2} = \overline{64} = \overline{4}$

$\overline{8}^{5} = \overline{32768} = \overline{8}$

$\overline{8}^{9} = (\overline{8}^{3})^{3} = (\overline{512}^{3}) = \overline{2}^{3} = \overline{8}$

So $\overline{8}^{47} = \overline{4 \times 8} = \overline{32} = \overline{2}$

- $\overline{15}^{2311} = \overline{15}^{5 \times 462} \times \overline{15}$

$\overline{15}^{5} = \overline{15}$

$\overline{15}^{7} = \overline{15}$

$\overline{15}^{6} = \overline{1}$

$\overline{1}^{11} = \overline{1}$

$\overline{15}^{2310} \times \overline{15} = \overline{1} \times \overline{15} = \overline{15}$

Exercise 7

In $(\mathbb{Z}/24\mathbb{Z}, \oplus, \otimes)$

i) Find all $\overline{a}$ such that $a \wedge 24 = 1$

We are in $\overline{24}$ so we are looking for all the elements in $(\mathbb{Z}/24\mathbb{Z})$ we have $24 = 2^3 \times 3$

So all the numbers divisible by 2 and 3 cannot be a

We have so $\overline{1}, \overline{5}, \overline{7}, \overline{11}, \overline{13}, \overline{17}, \overline{19}, \overline{23}$

- $24 = 5 \times 4 + 4$
  $5 = 4 \times 1 + 1$

r	q	u	v
24	x	0	1
5	x	+1	-0
4	4	-4	+1
1	1	+5	-1

$5 \times \underline{5} - 24$

- $24 = 7 \times 3 + 3$
  $7 = 3 \times 2 + 1$

r	q	u	v
24	x	0	1
7	x	+1	-0
3	3	-3	+1
1	2	+7	-2

$7 \times \underline{7} - 2 \times 24$

- $24 = 11 \times 2 + 2$
  $11 = 2 \times 5 + 1$

r	q	u	v
24	x	0	1
11	x	+1	-0
2	2	-2	+1
1	5	+11	-5

$11 \times \underline{11} - 5 \times 24$

- $24 = 13 \times 1 + 11$
  $13 = 11 \times 1 + 2$
  $11 = 2 \times 5 + 1$

r	q	u	v
24	x	0	1
13	x	+1	-0
11	1	-1	+1
2	1	+2	-1
1	5	-11	+6

$13 \times (\underline{-11}) + 6 \times 24$

- $24 = 17 \times 1 + 7$
  $17 = 7 \times 2 + 3$
  $7 = 3 \times 2 + 1$

r	q	u	v
24	x	0	1
17	x	+1	-0
7	1	-1	+1
3	2	+3	-2
1	2	-7	+5

$17 \times (\underline{-7}) + 5 \times 24$

- $24 = 19 \times 1 + 5$
  $19 = 5 \times 3 + 4$
  $5 = 4 \times 1 + 1$

r	q	u	v
24	x	0	1
19	x	+1	-0
5	1	-1	+1
4	3	+4	-3
1	1	+5	+4

$19 \times (\underline{-5}) + 4 \times 24$

- $24 = 23 \times 1 + 1$

r	q	u	v
24	x	0	1
23	x	+1	-0
1	1	-1	+1

$23 \times (\underline{-1}) + 24$.

$\{\bar{1}, \bar{5}, \bar{7}, \bar{11}, \bar{-1}, \bar{-5}, \bar{-7}, \bar{-11}\}$

ii) Solve $\bar{7}x = \overline{15}$

$x = \overline{15} \times \bar{7} = \overline{105} = \bar{9}$

iii) $\bar{3}x = \overline{15} \rightarrow \bar{x} = \bar{5}$ [8] $\rightarrow x = \bar{5}$

$x = \overline{13}$

$x = \overline{21}$

iv) $\bar{3}x = \overline{17} \rightarrow$ no solutions

Exercise 8

i) $\text{Inv}(\mathbb{Z}/28\mathbb{Z}) = \{\bar{1}, \bar{3}, \bar{5}, \bar{9}, \bar{11}, \bar{13}, \bar{15}, \bar{17}, \bar{19}, \bar{23}, \bar{25}, \bar{27}\}$

$28 = 2^2 \times 7$

ii) $\bar{3}x = \bar{17}$

$x = \bar{17} \times \bar{19} = \bar{15}$

$28 = 3 \times 9 + 1$
$4 \times 2 + 0$ } $\gcd(28,3) = 1$

iii) $\bar{4}\dot{x} = \bar{17}$

$28 = 4 \times 7 + 0$

17 not divisible by 4 $\quad \gcd(28;4) = 4$

→ no solutions.

iv) $x \equiv \bar{3}\ [7]$

$x = \bar{3} = \bar{10} = \bar{17} = \bar{24}$

Exercise 9

$$\begin{cases} x \equiv 3\ [7] \\ x \equiv 4\ [11] \end{cases}$$

We have $7 \wedge 11 = 1$ so here

$11 = 7 \times 1 + 4$
$7 = 4 \times 1 + 3$
$4 = 3 \times 1 + 1$

11	x	0	1
7	x	+1	-0
4	1	-1	+1
3	1	+2	-1
1	1	-3	+2

$1 = 7 \times -3 + 2 \times 11$ | x_1

So $x_1 = -21$
$x_2 = 22$

$\begin{cases} x \equiv 1\ [7] \\ x \equiv 0\ [11] \end{cases}$ $\quad \begin{cases} x \equiv 0\ [7] \\ x \equiv 1\ [11] \end{cases}$

So $x = 22 \times 3 - 21 \times 4 = -18$

with $7 \times 11 = 77$

$x = 59 + 77k$

Posons : $x_1 \equiv a\ [n_1]$
$x_2 \equiv b\ [n_2]$
$x_3 \equiv c\ [n_3]$

On pose $n = n_1 \times n_2 \times n_3$

On calcule $Y_1 = \frac{n}{n_1}$; $Y_2 = \frac{n}{n_2}$; $Y_3 = \frac{n}{n_3}$

Ensuite on trouve le n_i pour lequel
$Y_1 \wedge n_i = 1$; $Y_2 \wedge n_i = 1$; $Y_3 \wedge n_i = 1$
Pour chaque Y on calcule son inver
Par rapport à n_i (si negative $+ n_i$)
[Je note chaque inverse I_i]

On a $X = a \times Y_1 \times I_1 + b \times Y_1 \times I_2 + c \times Y_1 \times$

- $\begin{cases} y \equiv 7\ [10] \\ y \equiv 2\ [9] \\ y \equiv 6\ [7] \end{cases}$

On a $\gcd(9;10) = 1$
$\gcd(7;9) = 1$
$\gcd(7;10) = 1$

- $10 \times 9 \times 7 = 630$, $\hat{n}_1 = 63 \rightarrow 63 \wedge 10 = 1$
- $\hat{n}_2 = 70$, $70 \wedge 9 = 1$
- $\hat{n}_3 = 90$, $90 \wedge 7 = 1$

- $63 = 10 \times 6 + 3$
  $10 = 3 \times 3 + 1 \Rightarrow 1 = 10 - 3 \times 3$
  $= 10 - 3(63 - 10 \times 6)$
  $= 10 \times 18 \boxed{-3} \times 63$

$e_1 = \overline{7}$

- $70 = 9 \times 7 + 7$
  $9 = 7 \times 1 + 2$
  $7 = 2 \times 3 + 1$

$1 = 7 - 2 \times 3$
$= 7 - 3 \times (9 - 7)$
$= 7 \times 4 - 3 \times 9$
$= (70 - 9 \times 7) \times 4 - 3 \times 9$
$= 70 \times \boxed{4} - 9 \times 31$

Here $e_2 = \overline{4}$

- $90 = 7 \times 12 + 6$
  $7 = 6 + 1$

$1 = 7 - 6$
$= 7 - (90 - 7 \times 12)$
$= 7 \times 13 \boxed{-} 90$

$e_3 = -\overline{1} = \overline{6}$

$x = 7 \times 7 \times 63 + 4 \times 70 \times 2 + 6 \times 90 \times 6$
$= 587 + 630k$

Chapter 2

Exercise 10

The Enciphering key is $(\bar{5}, \bar{3})$

i) "DECIDE" → 342834

- $ax + b = \bar{5}x + \bar{3}$

$18 = 7$	H
$23 = 1$	B
$13 = 2$	C
$43 = 10$	K
$18 = 7$	H
$23 = 1$	B

ii) So we have $11 = 5 \times 2 + 1$ so $11 - 5 \times 2 = 1$

So $\bar{5} = \overline{-2} = \bar{9}$

So we have $\bar{9} \times \bar{3} = \overline{-27} = \bar{6}$

$\overline{15} = \bar{4}$	E
$\overline{60} = \bar{5}$	F
$\overline{60} = \bar{5}$	F
$\overline{96} = \bar{8}$	I
$\overline{24} = \bar{2}$	C

$\overline{33} = \bar{0} = A$.

$\overline{24} = \bar{2} \cdot C$

$\overline{15} = \bar{4}$ E

EFFICACE

Exercise 11

i) We calculate all the determinants

i) 9 gcd( ) = 1
ii) 104 gcd( ) = 13
iii) 6 gcd( ) = 2
iv) 4 gcd( ) = 4

} f and h are byective

i) $\bar{9}^{-1}$ → $14 = 9 + 5$
$9 = 5 \times 1 + 4$
$5 = 4 \times 1 + 1$

$1 = 5 - 4$
$= 5 \times 2 - 9$
$= 14 \times 2 - 9 \times 3$

$-\bar{3} = \bar{11}$

$$g^{-1}\begin{pmatrix} y_1 \\ y_2 \end{pmatrix} = \begin{pmatrix} \overline{2} & \overline{9} \\ \overline{5} & \overline{7} \end{pmatrix}\begin{pmatrix} \overline{y_1} \\ \overline{y_2} \end{pmatrix} + \begin{pmatrix} \overline{1} \\ \overline{11} \end{pmatrix}$$

Same for iv)

Chapter 3

Exercise 16

$\varphi(51) = \varphi(3 \times 17) = 32$

$\varphi(93) = 60$

$\varphi(135) = \varphi(3^3 \times 5) = 72$

$\varphi(200) = \varphi(2^3 \times 5^2) = 80$

Exercise 17

i) $\varphi(165) = 80$

ii)

$165 = 14 \times 11 + 11$

$14 = 11 \times 1 + 3$

$11 = 3 \times 3 + 2$

$3 = 2 \times 1 + 1$

r	q	u	v
165	x	0	1
14	x	+1	-0
11	11	+11	+1
3	1	+12	-1
2	3	-47	+4
1	1	+59	-5

So : $1 = 59 \times 14 - 5 \times 165$.

So $\overline{59}$

iii) $\overline{15}^{1766} = \overline{15}^{2 \times 883} = \overline{60}^{883}$

$= \overline{60}^3 \times \overline{60}^{880}$

$= \overline{15} \times \overline{45}^{176} = \overline{15} \times \overline{45}^{16 \times 11}$

$= \overline{15} \times \overline{45}^{11} = \overline{15} \times \overline{45} \times \overline{45}^{5}$.

$= \overline{15}$

Exercise 18 ☺

i) We have p, q two prime number, $n = p \times q$

$$\varphi(n) = \varphi(p) \times \varphi(q)$$
$$= (p-1) \times (q-1)$$
$$= pq - p - q + 1$$
$$= pq - (p+q) + 1$$
$$= n - p + q + 1$$

ii) $$p + q = n + 1 = \varphi(n)$$

iii) We have $\begin{cases} p + q = 4112 \\ pq = 2851207 \end{cases}$

$$q = 4112 - p$$
$$p(4112 - p) = 2851207 \iff -p^2 + p \times 4112 = 2851207$$
$$p^2 - 4112p + 2851207 = 0$$
$$(b^2) - 4ac = 5503716 = 2346$$
$$x_1 = \frac{4112 - 2346}{2} = 883$$
$$x_2 = \frac{-4112 - 2346}{2} = -3229$$

So we have $p = 3229$ and $q = 883$

Exercise 19 ☺

i) $x^5 = \overline{41}$ in $\mathbb{Z}/65\mathbb{Z}$

$65 \mid (x^5 - \overline{41})$

$41 = 24 \times 1 + 17$
$24 = 17 \times 1 + 7$
$17 = 7 \times 2 + 3$
$7 = 3 \times 2 + 1$

if $65 \mid x^5 - 41 \Rightarrow x^5 - 41 = p \times 65$

$\overline{41} \times \overline{65} = 1$

$\phi(n) = \overline{48}$

$5d \equiv 1 \ [48]$

$48 = 5 \times 9 + 3$

$5 = 3 \times 1 + 2$

$3 = 2 \times 1 + 1$

$1 = 3 - 2$

$= 3 \times 2 - 5$

$= (48 - 5 \times 9) \times 2 - 5$

$= 48 \times 2 - 5 \times 19$

$-5 \times 29 \equiv 1 \ [48]$.

$x = \overline{41}^{29} = \overline{41}^{5+5+5+5+5+4}$

$= 6 \times 6 \times 6 \times 6 \times 6 \times 16$

$= \overline{6}$

ii) $x^9 = \overline{11}$

$\phi(102) = 32$

$9d = 1 \ [32]$

$32 = 9 \times 3 + 5$

$9 = 5 \times 1 + 4$

$5 = 4 \times 1 + 1$

$1 = 5 - 4$

$= 5 \times 2 - 9.$

$= 32 \times 2 - 9 \times 7$

$9 \times 25 = 1 \ [32]$

So $x = \overline{11}^{25} = 11^{5 \times 5} = \overline{95}^{5} = \overline{23}$

eii) $gcd(6, 16) = 2$

3 no solutions

$8 = 3 \times 2 + 2$

$3 = 2 \times 1 + 1$

$3 \times 3 \equiv 1 \ (8)$

So $x = \overline{6}^{3} = \overline{8}$

Exercise 20

i) $ed \equiv 1 [\varphi(n)] \iff 3d \equiv 1 [\varphi(n)]$ $\qquad 55 = 5 \times 11$

$\varphi(55) = 40$ $\qquad 3 \times (-13) \equiv 1 [\varphi(n)]$

$40 = 3 \times 13 + 1$ $\qquad 3 \times 27 \equiv 1 [\varphi(n)]$

$\gcd(40; 3) = 1$

✓

2) $x = 12$

$y = x^{e_B}$

$= 12^7$

So $\overline{12}^7 = \overline{12}$

3) $y = 50$

$x = y^{d_A} = 50^{27} = \overline{50}^2 \times \overline{50}^{5 \times 5}$

$= 25 \times 10^5 = \overline{250} = \overline{30}$

4) We want to find d_B.

$7d \equiv 1 [120]$

$120 = 7 \times 17 + 1$

$7 \times \overline{-17} \equiv 1 [120]$

$7 \times \overline{103} = 1$

So $d = \overline{103}$

Exercise 21.

i) $n_A = 133 = 7 \times 19$

$\varphi(133) = 133\left(1 - \frac{1}{7}\right)\left(1 - \frac{1}{19}\right) = 108$

$41d \equiv 1\ [108]$

$108 = 41 \times 2 + 26$
$41 = 26 \times 1 + 15$
$26 = 15 \times 1 + 11$
$15 = 11 \times 1 + 4$
$11 = 4 \times 2 + 3$
$4 = 3 \times 1 + 1$

r	q	U	V
108	x	0	1
41	x	+1	-0
26	2	-2	+1
15	1	+3	-1
11	1	-5	+2
4	1	+8	-3
3	2	-21	+8
1	1	+29	-11

$29 \times 41 - 11 \times 108 = 1$

$41 \times 29 \equiv 1\ [108]$

✓

ii) $x = 3$

$y = x^{e_B}\ [n_B]$

$= 3^{77}\ [187]$

$= 3^{7 \times 11}\ [187]$

$= \overline{130}^{11}\ [187]$

$= \overline{130}^{4 \times 2} \times \overline{130}^{4} \times \overline{130}^{3}\ [187] = 38 \times 38 \times 124 = \overline{97}$

iii) $y = 10$

$x = y^{d_A} \Rightarrow x = 10^{29} = 10^{5 \times 5} \times 10^{4} = \overline{117}^{5} \times \overline{25}$

$= \overline{123} \times \overline{27} \times \overline{25}$

$= \overline{33}$

iv) $ed \equiv 1\ [160]$

$160 = 77 \times 2 + 6$
$77 = 7 \times 6 \times 12 + 5$

$6 = 5 + 1$

$1 = 6 - (77 - 6 \times 12)$
$= 6 \times 13 - 77$
$= (160 - 77 \times 2) \times 13 - 77$
$= 160 \times 13 - 77 \times 27$

So : $77 \times (\overline{-27}) \equiv 1 [160]$

$77 \times \overline{133} \equiv 1 [160]$

133

Exercise 23

i) $\varphi(209) = 180 \quad \varphi(221) = 192$

$13d \equiv 1 [180]$

$25d \equiv 1 [192]$

So : $180 = 13 \times 13 + 11$

$13 = 11 \times 1 + 2$

$11 = 2 \times 5 + 1$

$1 = 11 - 2 \times 5$

$= 11 - 5 \times (13 - 11)$

$= 11 \times 6 - 5 \times 13$

$= (180 - 13 \times 13) \times 6 - 5 \times 13$

$= 180 \times 6 - 13 \times 83$

So $d = -\overline{83} = 97$

$192 = 25 \times 7 + 17$

$25 = 17 \times 1 + 8$

$17 = 8 \times 2 + 1$

$1 = 17 - 8 \times 2$

$= 17 - (25 - 17) \times 2$

$= 17 \times 3 - 25 \times 2$

$= (192 - 25 \times 7) \times 3 - 25 \times 2$

$= 192 \times 3 - 25 \times 23$

So $d = -\overline{23} = \overline{169}$

ii) We have $n_A < n_B$.

A sends to B

$S = \left((s_A)^{d_A} [n_A] \right)^{e_B} [n_B]$

$= \left((\overline{10}^{97}) [209] \right)^{25} [221]$

$= \left((\overline{10}^{9 \times 10} \times \overline{10}^{7}) [209] \right)^{25} [221]$

$= \overline{186}^{25} [221]$

$= \overline{120} \times \overline{186} = 1 \times \overline{186} = \overline{186}$

(iii) A checked B

$$S_B = \left((y_{BA})^{e_B}\,[n_B]\right)^{d_A}\,[n_A]$$

$$= \left(98^{25}\,[221]\right)^{97}\,[209]$$

$$= \overline{98}^{97}\,[209]$$

$$= \overline{98}^{5\times 19+2}$$

$$= \overline{186}^{19} \times \overline{98}^{2}$$

$$= 186 \times \overline{164}^{6} \times \overline{98}^{2}$$

$$= \overline{186} \times \overline{199}$$

$$= \overline{21}$$

Yes!