Classical cryptography

Exercise 1.1:
a) 7503 mod 81 = 51
b) -7503 mod 81 = 30
c) 81 mod 7503 = 81
d) -81 mode 7503 = 7422
Lemma: Give $a \in \mathbb{Z}$, $b \in \mathbb{Z}$, $m \in \mathbb{N}\backslash\{0\}$, we have:
i) (a + bm) mod m = a mod m,
ii) ab mod m = (a mod m)(b mod m) mod m.
We will use this lemma many times in these exercises.

Proof

i) We suppose that
(1) (a + bm) mod m = t,
so that $m > t \geq 0$.
(1) ⇒ (a + bm) ≡ t (mod m).
⇒ m divides [(a + bm) – t].
Notice that m devides bm, hence m divides (a – t).
⇒ a ≡ t (mod m),
additionally, $m > t \geq 0$
⇒ t = a mod m
Finally, we attain
(a + bm) mod m = t = a mod m ■

ii) We suppose that
a mod m = c, b mod m = d
⇒ a≡ c (mod m), b ≡ d (mod m)
⇒ m divides (a-c), m divides (b-d)
⇒ $\exists$ p, q $\in \mathbb{Z}$: (a-c) = pm, (b-d) = qm
⇒ a = pm + c, b = qm + d
⇒ ab mod m = (pm + c)(qm + d) mod m
= [(pq + pd + cq)m + cd] mod m
= cd mod m (use (i))
= (a mod m)(b mod m) mod m ■

Exercise 1.2:
We have
a ≢ 0 (mod m)
⇒ $\exists$ c $\in \mathbb{Z}$, $m > c > 0$: a ≡ c (mod m)

⇒ m divides (a-c)
⇒ $\exists$ b $\in \mathbb{Z}$: (a-c) = bm
⇒ a = bm + c
⇒ -a = -bm – c
⇒ (-a) mod m = (-c) mod m = m – c (because m – c > 0)
Finally, we attain
(-a) mod m = m – c = m – (a mod m) ■

Exercise 1.3:
Prove that (a mod m) = (b mod m) if and only if a ≡ b (mod m).
(⇐) Suppose that a mod m = r, b mod m = s
that means a = pm + r, b = qm +s, where p, q $\in \mathbb{N}$.

$a \equiv b \pmod{m}$
$\Rightarrow (a - b) \vdots m$
$\Rightarrow [(pm + r) - (qm + s)] \vdots m$
$\Rightarrow [(p-q)m + (r - s)] \vdots m$
$\Rightarrow (r - s) \vdots m$
together with $m > r \geq 0$, $m > s \geq 0$, we have
$m > r - s > -m$
Hence $r - s = 0$
It means a mod m = b mod m ■
(⇒) Prove that : (a mod m = b mod m) ⇒ $a \equiv b \pmod{m}$
a mod m = b mod m
$\Rightarrow b - a = km$ ($k \in Z$)
$\Rightarrow (b - a) \vdots m$
$\Rightarrow a \equiv b \pmod{m}$ ■
Exercise 1.4:
We suppose that
a mod m = c, where $m > c \geq 0$
$\Rightarrow \exists b \in \mathbb{Z} : a = bm + c$
$\Rightarrow a - bm = c$
Since $m > c \geq 0$, we have
(1) $m > a - bm \geq 0$
Let both sides of (1) are divided by m ($m \in \mathbb{N} \setminus \{0\}$), we have
$a/m \geq b > (a/m) - 1$
$\Rightarrow b = \lfloor a/m \rfloor$
Finally, we attain
a mod m = $c = a - bm = a - \lfloor a/m \rfloor . m$ ■
Exercise 1.5:
Decrypt the ciphertext which encrypted by using a Shift Cipher below:
BEEAKFYDJXUQYHYJIQRYHTYJIQFBQDUYJIIKFUHCQD
The root text is:
LOOK UP IN THE AIR IT'S A BIRD IT'S A PLANE IT'S SUPERMAN
The key k = 16.
Exercise 1.6:
In the Shift Cipher over $\mathbb{Z}_{26}$, we have:
$e_K(x) = (x + K) \bmod 26$
$d_K(y) = (y - K) \bmod 26$
The key K is said to be an involutary key if
$e_K(x) = d_K(x)$,
so that
$(x + K) \bmod 26 = (x - K) \bmod 26$
$\Rightarrow (x + K) \equiv (x - K) \pmod{26}$
$\Rightarrow$ 26 divides $[x + K - (x - K)]$
$\Rightarrow$ 26 divides 2K
$\Rightarrow \exists b \in \mathbb{Z} : 2K = b.26$
$\Rightarrow K = b.13$
Since $0 \leq K \leq 25$, we accept b = 0 and/or b = 1, then K = 0 and/or K = 13.
Therefore,
all the involutary keys in the Shift Cipher over $\mathbb{Z}_{26}$ are 0 and 13 ■
Exercise 1.7:

Determine number of keys in an Affine Cipher over Z_m :

For m = 30:

$30 = 2*3*5$

$\Rightarrow \Phi(30) = (2 - 1)*(3 - 1)*(5 - 1) = 8$

$\Rightarrow$ Number of keys = $\Phi(30)*30 = 240$

For m = 100:

$100 = 2^2 * 5^2$

$\Rightarrow \Phi(100) = (4 - 2)*(25 - 5) = 80$

$\Rightarrow$ Number of keys = $\Phi(100)*100 = 8000$

For m = 1225:

$1225 = 5^2 * 7^2$

$\Rightarrow \Phi(1225) = (25 - 5)*(49 - 7) = 820$

$\Rightarrow$ Number of keys = $\Phi(1225)*1225 = 1004500$

Exercise 1.8:

All the invertible elements in $\mathbb{Z}_{28}$ are:

$1^{-1} = 1$
$3^{-1} = 19$
$5^{-1} = 17$
$9^{-1} = 25$
$11^{-1} = 23$
$13^{-1} = 13$
$15^{-1} = 15$
$27^{-1}=27$ ■

All the invertible elements in $\mathbb{Z}_{33}$ are:

$1^{-1} = 1$
$2^{-1} = 17$
$4^{-1} = 25$
$5^{-1} = 20$
$7^{-1} = 19$
$8^{-1} = 29$
$10^{-1} = 10$
$13^{-1} = 28$
$14^{-1} = 26$
$16^{-1} = 23$
$32^{-1} = 32$ ■

All the invertible elements in $\mathbb{Z}_{35}$ are:

$1^{-1} = 1$
$2^{-1} = 18$
$3^{-1} = 12$
$4^{-1} = 9$
$6^{-1} = 6$
$8^{-1} = 22$
$11^{-1} = 16$
$13^{-1} = 27$
$19^{-1} = 24$
$23^{-1} = 32$
$26^{-1} = 31$
$29^{-1} = 29$
$34^{-1} = 34$ ■

Exercise 1.9:

For $1 \leq a \leq 28$, determine a^{-1} mod 29 by trial and error.

$1^{-1} = 1$
$2^{-1} = 15$
$3^{-1} = 10$
$4^{-1} = 22$
$5^{-1} = 6$
$7^{-1} = 25$
$8^{-1} = 11$
$9^{-1} = 13$
$12^{-1} = 17$
$14^{-1} = 27$
$16^{-1} = 20$
$18^{-1} = 21$
$19^{-1} = 26$
$23^{-1} = 24$
$28^{-1} = 28$

Exercise 1.10:

Suppose that K = (5, 21) is a key in an Affine Cripher over $\mathbb{Z}_{29}$

a)

We have 5^{-1} mod 29 = 6, so the decryption function is

$d_K(y) = 6(y – 21) \bmod 29$ ■

b)

For all element x of $\mathbb{Z}_{29}$, we have:

$d_K(e_K(x))$ = 6([(5x + 21) mod 29]– 21) mod 29
= 6([(5x + 21 – L(5x+21)/29⅃.29) - 21) mod 29 (use exercise 1.4)
= 6(5x – L(5x+21)/29⅃.29) mod 29
= (6.5x – 6.L(5x+21)/29⅃.29) mod 29
= 6.5x mod 29 (use lemma (i))
= (6.5 mod 29)(x mod 29) mod 29 (use lemma (ii))
= x mod 29 (because 6*5 mod 29 = 1)
= x ■

Exercise 1.11:

a)

Suppose that K = (a, b) is a key in an Affine Cripher over $\mathbb{Z}_n$.

First, we must show that if K is an involutary key,
then a^{-1} mod n = a and $b(a + 1) \equiv 0 \pmod n$.
Since K is an involutary key,
for all x of $\mathbb{Z}_n$, we have

$e_K(x) = d_K(x)$,
$\Rightarrow (ax+b) \bmod n = a^{-1}(x-b) \bmod n$
$\Rightarrow (ax+b) \equiv a^{-1}(x-b) \pmod n$
$\Rightarrow$ n divides $ax+b – a^{-1}(x-b)$
$\Rightarrow$ n divides $(a - a^{-1})x + (1+a^{-1})b$

Because the equality above satisfies all x of $\mathbb{Z}_n$,
it must satisfy x = n. Replace x by n in the equality, we have
(1) n divides $(a - a^{-1})n + (1+a^{-1})b$,
then n divides $(1+a^{-1})b$, this means
(2) $(1+a^{-1})b \equiv 0 \pmod n$.

Therefore, together with (1), we attain

(3) n divides $(a - a^{-1})x$.

Now we choose the value for x that is not divided by n, from (3) we have

n divides $(a - a^{-1})$,

this means $a \equiv a^{-1} \pmod n$. Additionally, we got $n - 1 \geq a \geq 0$, so

$a^{-1} \bmod n = a$ ■

Actually, we also got $n - 1 \geq a^{-1} \geq 0$, so $a = a^{-1} \bmod n = a^{-1}$.

Hence we can replace a^{-1} by a in the equality (2) to have the following:

$(1+a)b \equiv 0 \pmod n$ ■

Second, we show that if $a^{-1} \bmod n = a$ and $b(a + 1) \equiv 0 \pmod n$

then K is an involutary key.

Because $a = a^{-1} \bmod n = a^{-1}$, we have:

$e_K(x) = (ax+b) \bmod n$,

and $d_K(x) = a^{-1}(x-b) \bmod n = (ax - ab) \bmod n$

We do something with $d_K(x)$:

$d_K(x) = (ax - ab) \bmod n$

$= (ax - b(a+1) + b) \bmod n$

Now we use lemma (i) together with the suppose $b(a+1) \equiv 0 \pmod n$ to attain

$d_K(x) = (ax + b) \bmod n = e_K(x)$,

this means K is an involutary key ■

b)

We suppose K =(a, b) is an involutary key in $\mathbb{Z}_{15}$.

The result from 1.11a applies, we have the following conditions:

(4) $a = a^{-1}$ in $\mathbb{Z}_{15}$, and

(5) $b(a+1) \equiv 0 \pmod{15}$.

From (4), the acceptable values of a are 1, 4, 11 and 14.

Then, when a = 1, from (5), we have b = 0;

when a = 4, $b \in \{0, 3, 6, 9, 12\}$;

when a = 11, we have $b \in \{0, 5, 10\}$;

when a = 14, we have $b \in \mathbb{Z}_{15}$.

We listed all keys of $\mathbb{Z}_{15}$ above■

c)

Suppose that L = (e, f) is is an involutary key in $\mathbb{Z}_n$, where n = pq, p, q are distinct odd primes. We will find the properties of L.

The result from 1.11a applies, we have the following:

(6) $e^{-1} = e$

(7) $f(e+1) \equiv 0 \pmod n$

From (6), we have

$e.\ e \equiv 1 \pmod n$

$\Rightarrow e^2 - 1 \equiv 0 \pmod n$

$\Rightarrow (e + 1)(e - 1) \equiv 0 \pmod n$

Because n = pq where p, q are distinct odd primes, there exist two elements r, s of $\mathbb{Z}_n$, 0<r<q, 0<s<p, that are satisfying the following:

(8) e + 1 = rp and e – 1 = sq, or

(9) e + 1 = sq and e – 1 = rp, or

(10) e + 1 = pq (we know e < pq), or

(11) e – 1 = 0

- From (8),

notice that to solve the equaltions (8) (variable e) in $\mathbb{Z}_n$ is more complex than to solve it in $\mathbb{N}$, so we will solve it in $\mathbb{N}$, then transform the result to be the one in $\mathbb{Z}_n$. Now we have to find the solution of this

$e' + 1 = r'p$ and $e' – 1 = s'q$, where $e', r', s' \in \mathbb{N}$

Using subtraction, we have

$r'p – s'q = 2.$

Since p, q are distinct odd primes, there exists a unique pair (u, v), where u, v $\in \mathbb{N}$, $u<q$, $v<p$, satisfying this: $up + vq = 1$, so that

$r'p – s'q = 1 + up + vq$

It follows that

(13) $(r' - u)p + (-s' – v)q = 1 = up + vq$

Since the pair (u, v) is unique, together with (13), we have

$r' – u' = u$ and $-s – v = v$.

It follows that

$r' = 2u$ and $s' = -2v$

Therefore we have

$e' + 1 = 2up$ and $e' – 1 = -2vq$

$\Rightarrow e' = up – vq.$

Now, as we have e', we have $e = e' \bmod n = (up - vq) \bmod n$, so

$e + 1 = [(up - vq) \bmod n] +1$ (notice that we are calculate in $\mathbb{Z}_n$)

$=(up – vq + 1) \bmod n$

$=(up – vq + up +vq) \bmod n$

$= 2up \bmod n$

$= 2up \bmod pq$

$= 2up + mpq$, where $m\in \mathbb{N}$: $2up + mpq \in \mathbb{Z}_n$

$= (2u+mq)p$

Because $(2u+mq)p \in \mathbb{Z}_n$, we have $0<2u+mq < q$

(of course we notice $2u + mq \neq 0$ and $2u + mq \neq q$),

so we suppose $r = 2u+mq$, we have this:

$e = rp$, where $0<r<q$,

together with (7), we have

$frp \equiv 0 \pmod{pq}$.

Because $0<r<q$, so that q divides f, which means we have

$f \in \{0, q, 2q, \ldots (p-1)q\}$

Hence we have $[(p-1) – 0 + 1] = p$ keys.

- From (9), we do similarly to which we did for (8), we have

  $e + 1 = sq$, where $s = 2v + tp$, $t \in \mathbb{N}$: $(2v + tp)q \in \mathbb{Z}_n$, $0<s<p$,

and $f \in \{0, p, 2p, \ldots (q-1)p\}$

Hence we have $[(q-1) – 0 + 1] = q$ keys.

- From (10), explicitly we have $f \in \mathbb{Z}_n$, so there are n keys in this case
- From (11), clearly we have $f = 0$, so there is only 1 key in this case
- Finally, the number of the involutary keys in $\mathbb{Z}_n$ is

  $p + q + n + 1$