# Cryptography Homework 5

*2024 Spring Semester*

21 CST H3Art

## Exercise 6.3

Use the $\text{EXTENDED EUCLIDEAN ALGORITHM}$ to compute the following multiplicative inverses:

(a) $17^{-1} \bmod 101$

(b) $357^{-1} \bmod 1234$

(c) $3125^{-1} \bmod 9987$

> **Solution**:
>
> (a)
>
> $$\begin{aligned} 101 &= 17 \times 5 + 16 \\ 17 &= 16 \times 1 + 1 \\ \\ 1 &= 17 - 16 \times 1 \\ &= 17 - (101 - 5 \times 17) \\ &= 6 \times 17 - 101 \end{aligned}$$
>
> Therefore, the inverse of $17$ under modulo $101$ is $6$.
>
> (b)
>
> $$\begin{aligned} 1234 &= 357 \times 3 + 163 \\ 357 &= 163 \times 2 + 31 \\ 163 &= 31 \times 5 + 8 \\ 31 &= 8 \times 3 + 7 \\ 8 &= 7 \times 1 + 1 \\ \\ 1 &= 8 - 7 \times 1 \\ &= 8 - (31 - 8 \times 3) \\ &= 4 \times 8 - 31 \\ &= 4 \times (163 - 31 \times 5) - 31 \\ &= 4 \times 163 - 31 \times 21 \\ &= 4 \times 163 - (357 - 163 \times 2) \times 21 \\ &= 46 \times 163 - 357 \times 21 \\ &= 46 \times (1234 - 357 \times 3) - 357 \times 21 \\ &= 46 \times 1234 - 159 \times 357 \end{aligned}$$
>
> Therefore, the inverse of $357$ under modulo $1234$ is $-159$.
>
> (c)

$$\begin{aligned}
9987 &= 3125 \times 3 + 612 \\
3125 &= 612 \times 5 + 65 \\
612 &= 65 \times 9 + 27 \\
65 &= 27 \times 2 + 11 \\
27 &= 11 \times 2 + 5 \\
11 &= 5 \times 2 + 1
\end{aligned}$$

$$\begin{aligned}
1 &= 11 - 5 \times 2 \\
&= 11 - (27 - 11 \times 2) \times 2 \\
&= 11 \times 5 - 27 \times 2 \\
&= (65 - 27 \times 2) \times 5 - 27 \times 2 \\
&= 65 \times 5 - 27 \times 12 \\
&= 65 \times 5 - (612 - 65 \times 9) \times 12 \\
&= 65 \times 113 - 612 \times 12 \\
&= (3125 - 612 \times 5) \times 113 - 612 \times 12 \\
&= 3125 \times 113 - 612 \times 577 \\
&= 3125 \times 113 - (9987 - 3125 \times 3) \times 577 \\
&= 3125 \times 1844 - 9987 \times 577
\end{aligned}$$

Therefore, the inverse of $3125$ under modulo $9987$ is $1844$.

# Exercise 6.4

Compute $\gcd(57, 93)$, and find integers $s$ and $t$ such that $57s + 93t = \gcd(57, 93)$.

**Solution**:

To compute $\gcd(57, 93)$, we use the $\text{EUCLIDEAN ALGORITHM}$ as follows:

$$\begin{aligned}
93 &= 57 \times 1 + 36 \\
57 &= 36 \times 1 + 21 \\
36 &= 21 \times 1 + 15 \\
21 &= 15 \times 1 + 6 \\
15 &= 6 \times 2 + 3 \\
6 &= 3 \times 2 + 0
\end{aligned}$$

So $\gcd(57, 93) = 3$, and to find integers $s$ and $t$ such that $57s + 93t = \gcd(57, 93)$, we use the $\text{EXTENDED EUCLIDEAN ALGORITHM}$:

$$\begin{aligned}
3 &= 15 - 6 \times 2 \\
&= 15 - (21 - 15) \times 2 \\
&= 15 \times 3 - 21 \times 2 \\
&= (36 - 21) \times 3 - 21 \times 2 \\
&= 36 \times 3 - 21 \times 5 \\
&= 36 \times 3 - (57 - 36) \times 5
\end{aligned}$$

$$
\begin{aligned}
&= 36 \times 8 - 57 \times 5 \\
&= (93 - 57) \times 8 - 57 \times 5 \\
&= 93 \times 8 - 57 \times 13
\end{aligned}
$$

Finally we find the corresponding integers for $57s + 93t = \gcd(57, 93)$ are $s = -13, t = 8$.

# Exercise 6.5

Suppose $\mathcal{X} : \mathbb{Z}_{105} \to \mathbb{Z}_3 \times \mathbb{Z}_5 \times \mathbb{Z}_7$ is defined as

$$\mathcal{X}(x) = (x \bmod 3, x \bmod 5, x \bmod 7)$$

Give an explicit formula for the function $\mathcal{X}^{-1}$, and use it to compute $\mathcal{X}^{-1}(2, 2, 3)$.

**Solution**:

According to the problem description, we suppose $m_1 = 3$, $m_2 = 5$, $m_3 = 7$, and $M = 3 \times 5 \times 7 = 105$, so:

$$
\begin{aligned}
M_1 &= \frac{105}{3} = 35 \\
M_2 &= \frac{105}{5} = 21 \\
M_3 &= \frac{105}{7} = 15
\end{aligned}
$$

Finally we can find the inverse factors are:

$$
\begin{aligned}
y_1 &= 35^{-1} \bmod 3 = 2 \\
y_2 &= 21^{-1} \bmod 5 = 1 \\
y_3 &= 15^{-1} \bmod 7 = 1
\end{aligned}
$$

Therefore, the explicit formula for the function $\mathcal{X}^{-1}$ is:

$$
\begin{aligned}
\mathcal{X}^{-1}(a_1, a_2, a_3) &= (35 \times 2a_1 + 21 \times 1a_2 + 15 \times 1a_3) \bmod 105 \\
&= (70a_1 + 21a_2 + 15a_3) \bmod 105
\end{aligned}
$$

and for $\mathcal{X}^{-1}(2, 2, 3)$, the result is as follows:

$$
\begin{aligned}
\mathcal{X}^{-1}(2, 2, 3) &= (70 \times 2 + 21 \times 2 + 15 \times 3) \bmod 105 \\
&= 227 \bmod 105 \\
&= 17
\end{aligned}
$$

# Exercise 6.7

Solve the following system of congruences:

$$
\begin{aligned}
13x &\equiv 4 (\bmod 99) \\
15x &\equiv 56 (\bmod 101)
\end{aligned}
$$

**HINT**: First use the $\text{EXTENDED EUCLIDEAN ALGORITHM}$, and then apply the Chinese remainder theorem.

**Solution**:

Firstly we compute the $13^{-1} \bmod 99$ and $15^{-1} \bmod 101$ using the $\text{EXTENDED EUCLIDEAN ALGORITHM}$.

For $13^{-1} \bmod 99$:

$$\begin{aligned}
99 &= 13 \times 7 + 8 \\
13 &= 8 \times 1 + 5 \\
8 &= 5 \times 1 + 3 \\
5 &= 3 \times 1 + 2 \\
3 &= 2 \times 1 + 1 \\
\\
1 &= 3 - 2 \times 1 \\
&= 3 - (5 - 3) \\
&= 3 \times 2 - 5 \\
&= (8 - 5) \times 2 - 5 \\
&= 8 \times 2 - 5 \times 3 \\
&= 8 \times 2 - (13 - 8) \times 3 \\
&= 8 \times 5 - 13 \times 3 \\
&= (99 - 13 \times 7) \times 5 - 13 \times 3 \\
&= 99 \times 5 - 13 \times 38
\end{aligned}$$

So the inverse of $13$ under modulo $99$ is $-38$, for $15^{-1} \bmod 101$:

$$\begin{aligned}
101 &= 15 \times 6 + 11 \\
15 &= 11 \times 1 + 4 \\
11 &= 4 \times 2 + 3 \\
4 &= 3 \times 1 + 1 \\
\\
1 &= 4 - 3 \times 1 \\
&= 4 - (11 - 4 \times 2) \\
&= 4 \times 3 - 11 \\
&= (15 - 11) \times 3 - 11 \\
&= 15 \times 3 - 11 \times 4 \\
&= 15 \times 3 - (101 - 15 \times 6) \times 4 \\
&= 15 \times 27 - 101 \times 4
\end{aligned}$$

So the inverse of $15$ under modulo $101$ is $27$.

Nextly, since $13 \times (-38) \equiv 1 \bmod 99$, we can multiply $4$ on both sides, then we get:

$$13 \times (-38) \times 4 \equiv 4 \bmod 99$$

So for $13x_1 \equiv 4 \pmod{99}$, $x_1 = -38 \times 4 \bmod 99 = 46$.

Similarly, since $15 \times 27 \equiv 1 \bmod 101$, we multiply $56$ on both sides then get:

$$15 \times 27 \times 56 \equiv 56 \bmod 101$$

For $15x_2 \equiv 56 \pmod{101}$, $x_2 = 27 \times 56 \bmod 101 = 98$.

Finally, by applying the Chinese remainder theorem, suppose $M = 99 \times 101 = 9999$, $M_1 = \dfrac{9999}{99} = 101$, $M_2 = \dfrac{9999}{101} = 99$.

> Hence, $y_1 = 101^{-1} \bmod 99 = 50$, $y_2 = 99^{-1} \bmod 101 = 50$, the solution of the given system of congruences is:
>
> $$\begin{aligned} x^{-1}(a_1, a_2) &= (50 \times 101 \times a_1 + 50 \times 99 \times a_2) \bmod 9999 \\ &= (5050a_1 + 4950a_2) \bmod 9999 \end{aligned}$$
>
> Substitute $a_1 = 46$, $a_2 = 98$ to the above formula, the solution value is:
>
> $$\begin{aligned} x^{-1}(46, 98) &= (5050 \times 46 + 4950 \times 98) \bmod 9999 \\ &= 717400 \bmod 9999 \\ &= 7471 \end{aligned}$$

# Exercise 6.11

Suppose that $n = pq$, where $p$ and $q$ are distinct odd primes and $ab \equiv 1(\bmod\ (p-1)(q-1))$. The RSA encryption operation is $e(x) = x^b \bmod n$ and the decryption operation is $d(y) = y^a \bmod n$. We proved that $d(e(x)) = x$ if $x \in \mathbb{Z}_n^*$. Prove that the same statement is true for any $x \in \mathbb{Z}_n$.

**HINT**: Use the fact that $x_1 \equiv x_2(\bmod pq)$ if and only if $x_1 \equiv x_2(\bmod p)$ and $x_1 \equiv x_2(\bmod q)$. This follows from the Chinese remainder theorem.

> **Solution**:
>
> Suppose $x \not\equiv 0 \pmod p$. Then, for some integer $k > 0$, it holds that
>
> $$x^{ab} = x^{1+k(p-1)(q-1)} \equiv x \cdot x^{k(p-1)(q-1)} \equiv x \pmod p$$
>
> If $x \equiv 0 \pmod p$, then $x^{ab} \equiv x \equiv 0 \pmod p$. Therefore, $x^{ab} \equiv x \pmod p$ for any $x \in \mathbb{Z}_p$. Similarly, $x^{ab} \equiv x \pmod q$ for any $x \in \mathbb{Z}_q$. Now, applying the Chinese Remainder Theorem, $x^{ab} \equiv x \pmod n$ for any $x \in \mathbb{Z}_n$.

# Exercise 6.15

Prove that the *RSA Cryptosystem* is insecure against a chosen ciphertext attack. In particular, given a ciphertext $y$, describe how to choose a ciphertext $\hat{y} \neq y$, such that knowledge of the plaintext $\hat{x} = d_K(\hat{y})$ allows $x = d_K(y)$ to be computed.

**HINT**: Use the multiplicative property of the *RSA Cryptosystem*, i.e., that

$$e_K(x_1)e_K(x_2) \bmod n = e_K(x_1x_2 \bmod n)$$

> **Solution**:
>
> Suppose we have a random $x_0$, then $y_0 = e_K(x_0)$, let $\hat{y} = y_0 y \bmod n$.
>
> Then we take $e_K(x_0)e_K(x) \bmod n = e_K(x_0 x \bmod n)$, $\hat{x} = d_K(e_K(x_0 x \bmod n)) = x_0 x \bmod n$.
>
> Thus, $x = \hat{x}x_0^{-1} \bmod n$.

# Exercise 6.16

This exercise exhibits what is called a ***protocol failure***. It provides an example where ciphertext can be decrypted by an opponent, without determining the key, if a cryptosystem is used in a careless way. The moral is that it is not sufficient to use a "secure" cryptosystem in order to guarantee "secure" communication.

Suppose Bob has an *RSA Cryptosystem* with a large modulus $n$ for which the factorization cannot be found in a reasonable amount of time. Suppose Alice sends a message to Bob by representing each alphabetic character as an integer between $0$

and $25$ (i.e., $A \leftrightarrow 0$, $B \leftrightarrow 1$, etc.), and then encrypting each residue modulo $26$ as a separate plaintext character.

(a) Describe how Oscar can easily decrypt a message that is encrypted in this way.

(b) Illustrate this attack by decrypting the following ciphertext (which was encrypted using an *RSA Cryptosystem* with $n = 18721$ and $b = 25$) without factoring the modulus:

$$365, 0, 4845, 14930, 2608, 2608, 0.$$

**Solution**:

(a) Oscar can encrypt each of the $26$ possible plaintext characters and record the corresponding ciphertext values in a table. This table would map each plaintext character to its encrypted form. Once this table is precomputed, any given ciphertext string can be decrypted by looking up each character in the table and substituting it with the corresponding plaintext character.

(b) Since $n = 18721$, $b = 25$, by iterating $0$ to $25$ to compute ciphertext, we can get a table:

| a | b | c | d | e | f | g | h | i | j | k | l | m |
|---|---|---|---|---|---|---|---|---|---|---|---|---|
| 0 | 1 | 6400 | 18718 | 17173 | 1759 | 18242 | 12359 | 14930 | 9 | 6279 | 2608 | 4644 |
| n | o | p | q | r | s | t | u | v | w | x | y | z |
| 4845 | 1375 | 13444 | 16 | 13663 | 1437 | 2940 | 10334 | 365 | 10789 | 8945 | 11373 | 5116 |

Thus, we can find the plaintext is:

$$\text{vanilla}$$