National Taiwan Normal University
CSIE Information Security

Instructor: Po-Wen Chi
Due Date: April 7, 2024, PM 11:59

Assignment 1

Policies:

- Zero tolerance for late submission.
- Please pack all your submissions in one zip file. **RAR is not allowed!!**
- I only accept **PDF**. MS Word is not allowed.
- Hand-writing is not allowed.
- Please use **Chinese.**

1.1 Triple Encryption (10 pts)

In this class, I have shown you why double DES is useless. However, someone argues that an attacker may find one key to simulate three keys. That is,

$$\mathbf{Enc}(k_3, \mathbf{Enc}(k_2, \mathbf{Enc}(k_1, x))) = \mathbf{Enc}(k', x).$$

So the attacker may need to brute force k' instead of k_1, k_2, k_3. Please show that the probability is negligible.

1.2 Hybrid Chosen-Plaintext-Attack Construction (10 pts)

Let (E_0, D_0) be a semantically secure cipher defined over $\{\mathcal{K}_0, \mathcal{M}, \mathcal{C}_0\}$ and (E_1, D_1) be a CPA secure cipher defined over $\{\mathcal{K}, \mathcal{K}_0, \mathcal{C}_1\}$. Define the following hybrid cipher (E, D) as:

$$E(k, m) := \{k_0 \xleftarrow{R} \mathcal{K}_0, c_1 \leftarrow E_1(k, k_0), c_0 \leftarrow E_0(k_0, m), \text{ output } (c_0, c_1)\},$$

$$D(k, (c_0, c_1)) := \{k_0 \leftarrow D_1(k, c_1), m \leftarrow D_0(c_0, k_0), \text{ output } m\}.$$

Prove that (E, D) is CPA secure.

1.3 The malleability of CBC mode (10 pts)

Let c be the CBC encryption of some message $m \in \mathcal{X}^l$, where $\mathcal{X} := 0, 1^n$. You do not know m. Let $\triangle \in \mathcal{X}$. Show how to modify the ciphertext c to obtain a new ciphertext c' that decrypts to m', where $m'[0] = m[0] \oplus \triangle$, and $m'[i] = m[i]$ for $i = 1, \ldots, l$. That is, by modifying c appropriately, you can flip bits of your choice in the first block of the decryption of c, without affecting any of the other blocks.

1.4 Modular Multiplicative Inverse (10 pts)

Please find the modular multiplicative inverse of the following number. Please write down how you find it. If you give the answer directly without the process, you will get zero points.

1. 400 mod 997
2. 472 mod 16651

1.5 Euler's Theorem and RSA (10 pts)

In this class, I have introduced Euler's Theorem to you as follows.

THEOREM 1.1. *For every a and n that are relatively prime, then*

$$a^{\phi(n)} \equiv 1 (mod\ n).$$

However, when we run RSA permutation, m and $N = pq$ may not be relatively prime. When m and $N = pq$ are not relatively prime, will the reverse permutation still work? Why or why not?

1.6 Pseudo Prime (10 pts)

In this class, I have told you that in computer science, we often use pseudo primes instead of real primes. However, when we verify the correctness of RSA, we always assume that p, q are primes. Is there any conflicts? Of course not or RSA will not work. Please show that even p, q are pseudo primes, the correctness of RSA still stands.

Hint: What are pseudo primes?

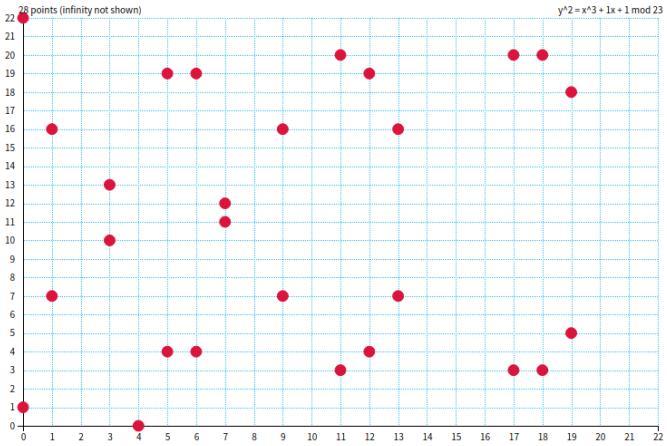

FIGURE 1.1: Elliptic group $E_{23}(1, 1)$.

1.7 Elliptic Curve over $\mathbb{Z}_p$ (10 pts)

An elliptic curve is defined by an equation in two variables with coefficients. Elliptic curves are not ellipse. They are named because they are described by cubic equations, similar to those used for calculating the circumference of an ellipse. For cryptography, the variables and coefficients are restricted in a finite field, which results in the definition of a finite abelian group.

For elliptic curves over $\mathbb{Z}_p$, we use the following equation to form a group:

$$y^2 \bmod p = (x^3 + ax + b) \bmod p.$$

Note that all coefficients and variables are belong to $\mathbb{Z}_p$.

For example, given a group E_p where $a = 1, b = 1, x = 9, y = 7, p = 23$, we have

$$\begin{gathered} 7^2 \bmod 23 = (9^3 + 9 + 1) \bmod 23 \\ 49 \bmod 23 = 739 \bmod 23 \\ 3 \bmod 23 = 3 \bmod 23 \end{gathered}$$

So $(9, 7) \in E_p$. We often use $E_p(a, b)$ to represent the group. All points are shown in Fig. 1.1. Note that $(4a^3 + 27b^2) \bmod p \neq 0 \bmod p$ for avoiding repeated factors.

How about the operation and the identity? In a elliptic curve group, the identity is defined at **infinity** O. The operation is defined as follows:

1. For any point P, $P + O = P$.
2. If $P = (x, y)$, then $-P = (x, -y)$.

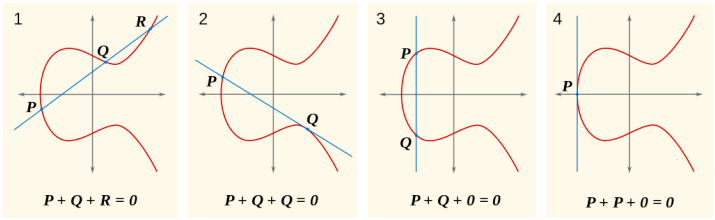

FIGURE 1.2: Elliptic group operation.

3. To "add" (operation) P and Q, draw a straight line $\overline{PQ}$ and find the third intersection R with the curve E_p. We define $P + Q + R = O$. Therefore, $P + Q = -R$. Note that the computation should be in $\mathbb{Z}_p$.

4. For $P + P$, use the tangent line instead.

You can see Figure 1.2 for reference.

Please show that given $P = (x_P, y_P), Q = (x_Q, y_Q), R = P + Q = (x_R, y_r)$,

$$x_R = (\lambda^2 - x_P - x_Q) \bmod p$$
$$y_R = (\lambda(x_P - x_R) - y_P) \bmod p$$

where

$$\lambda = \begin{cases} (\frac{y_Q - y_P}{x_Q - x_P}) \bmod p, \text{if } P \neq Q \\ (\frac{3x_P^2 + a}{2y_P}) \bmod p, \text{if } P = Q \end{cases}$$

1.8 Lab: Secret-Key Encryption (15 pts)

- Lab: https://seedsecuritylabs.org/Labs_20.04/Crypto/Crypto_Encryption/

You need to submit a detailed lab report, with screenshots, to describe what you have done and what you have observed. You also need to provide explanation to the observations that are interesting or surprising. Please also list the important code snippets followed by explanation. Simply attaching code without any explanation will not receive credits.

1.9 Lab: Padding Oracle Attack (15 pts)

- Lab: https://seedsecuritylabs.org/Labs_20.04/Crypto/Crypto_Padding_Oracle/

You need to submit a detailed lab report, with screenshots, to describe what you have done and what you have observed. You also need to provide explanation to the observations that are interesting or surprising. Please also list the important code snippets followed by explanation. Simply attaching code without any explanation will not receive credits.