浙江大學

《Big Data Security and Privacy Protection》

Set 3

题　　目：	set 3
上课时间：	August 24th
授课教师：	Rongxing Lu
姓　　名：	杜宗泽
学　　号：	3220105581
组　　别：	个人
日　　期：	9月2日

Set 3

1 Question 8

8. Please answer the following RSA related sub-questions.

   (a) In a public-key system using RSA, you intercept the ciphertext $C = 8$ sent to a user whose public key is $e = 5, n = 35$. What is the plaintext M?

   (b) The reason that you can recover the plaintext M in Question 1(a) is that $n = 35$ is too small, you can factor n and obtain the private key d. However, when we set the length of n is 1024 bits, i.e., $|n| = 1024$, the large integer factoring problem becomes hard. Now, when you intercept a ciphertext $C \equiv M^e \bmod n$, where $M \in \{0,1\}^{160}$, $e = 5$, and $|n| = 1024$, can you recover the message M from C without using the brute force? Why or why not?

My answer:

(a) To find the plaintext M, we can use the RSA decryption formula: M = C^d mod n, where d is the private key exponent. In order to calculate d, we need to know the prime factors of n.

In this case, n = 35, which is a small number. We can easily factorize it as 35 = 5 * 7. Now, we can calculate the private key exponent d using the formula: d = e^(-1) mod φ(n), where φ(n) is Euler's totient function.

φ(n) = (p-1)(q-1) = (5-1)(7-1) = 4 * 6 = 24

To find the modular inverse of e (e^(-1) mod 24), we can use the Extended Euclidean Algorithm. In this case, e = 5, and its modular inverse is 5 itself, as 5 * 5 ≡ 1 mod 24.

Now, we can calculate the plaintext M using the RSA decryption formula:
M = C^d mod n= 8^5 mod 35 = 32768 mod 35 = 8

Therefore, the plaintext M is 8.

(b) When the length of n is set to 1024 bits (|n| = 1024), the large integer factoring problem becomes hard. This means that it is computationally infeasible to factorize n and obtain the private key d.

In this scenario, if we intercept a ciphertext C ≡ Me mod n, where $M \in \{0,1\}^{160}$, $e = 5$, and |n| = 1024, it is not possible to recover the message M without using brute force. The reason is that the encryption exponent e and the modulus n are public information, and without the knowledge of the private key d, it is computationally infeasible to derive the original message M from the ciphertext C.

Above all, the security of RSA relies on the difficulty of factoring large integers, and with a sufficiently large key size, it is currently considered secure against brute force attacks and other known attacks.

2 Question 9

9. Please answer the following ElGamal encryption related sub-questions.

   (a) Consider an ElGamal encryption scheme with a common prime $q = 11$ and a primitive root $\alpha = 2$. If B has public key $Y_B = 3$ and A chooses the random integer $k = 2$, what is the ciphertext of $M = 9$?

(b) As we discussed in class, the message M cannot be 0 in the ElGamal encryption. Then, what strategy can you use to encrypt a message 0 in the ElGamal encryption? Please describe your strategy as detail as possible.

My answer:

(a) In the ElGamal encryption scheme, the ciphertext is generated using the following steps:

- A chooses a random integer k.
- A computes the ephemeral public key YA = α^k mod q.
- A computes the shared secret s = YB^k mod q.
- A encrypts the message M by computing the ciphertext C1 = α^k mod q and C2 = M * s mod q.
- The ciphertext (C1, C2) is sent to B.

Given the parameters q = 11, α = 2, YB = 3, and A chooses k = 2, we can calculate the ciphertext for M = 9 as follows:

1. A chooses k = 2.
2. A computes YA = $\alpha^k \bmod q$.
   YA = $2^2 \bmod 11 = 4 \bmod 11 = 4$.
3. A computes the shared secret s = YB^k mod q.
   s = $3^2 \bmod 11 = 9 \bmod 11 = 9$.
4. A encrypts the message M = 9.
   $C_1 = \alpha^k \bmod q = 2^2 \bmod 11 = 4 \bmod 11 = 4$.
   $C_2 = M * s \bmod q = 9 * 9 \bmod 11 = 81 \bmod 11 = 4$.

Therefore, the ciphertext for M = 9 is (C1, C2) = (4, 4).

(b) In the ElGamal encryption scheme, the message M cannot be 0 because it would result in a ciphertext of (C1, C2) = (α^k mod q, 0 * s mod q) = (α^k mod q, 0), which would leak information about the private key k.

To encrypt a message 0 in the ElGamal encryption, we can use a technique which is adding a random value to the message before encryption, ensuring that the resulting ciphertext is not (α^k mod q, 0).

Here is a strategy to encrypt a message 0 using message padding:

1. Choose a random non-zero value r.
2. Compute the padded message M' = M + r.
3. Encrypt the padded message M' using the regular ElGamal encryption process.
4. Send the ciphertext (C1, C2) to the recipient.

By adding a random non-zero value to the message, we ensure that the resulting ciphertext will not reveal any information about the private key k. The recipient can then subtract the random value r from the decrypted message to obtain the original message M = M' - r, which will be 0 in this case.

It is important to note that the random value r should be chosen carefully to ensure security and prevent any potential attacks.

3 Question 10

10. Use the Chinese Remainder Theorem (CRT) to solve x, where

$$\begin{cases} x & \equiv & 1 \bmod 3 \\ x & \equiv & 3 \bmod 5 \\ x & \equiv & 5 \bmod 7 \end{cases}$$

My answer:

To solve the system of congruences using the Chinese Remainder Theorem (CRT), we need to find a solution for x that satisfies all three congruences:

$$\begin{cases} x \equiv 1 (mod 3) \\ x \equiv 3 (mod 5) \\ x \equiv 5 (mod 7) \end{cases}$$

Step 1: Compute the product of the moduli:
N = 3 * 5 * 7 = 105

Step 2: Compute the individual moduli:
N1 = N / 3 = 105 / 3 = 35
N2 = N / 5 = 105 / 5 = 21
N3 = N / 7 = 105 / 7 = 15

Step 3: Compute the modular inverses of the individual moduli:
Since N1 ≡ 35 ≡ 2 (mod 3), the modular inverse of N1 modulo 3 is 2.
Since N2 ≡ 21 ≡ 1 (mod 5), the modular inverse of N2 modulo 5 is 1.
Since N3 ≡ 15 ≡ 1 (mod 7), the modular inverse of N3 modulo 7 is 1.

Step 4: Compute the partial solutions:
a1 = 1 (from the first congruence)
a2 = 3 (from the second congruence)
a3 = 5 (from the third congruence)

Step 5: Compute the sum of the partial solutions multiplied by the respective modular inverses:
x ≡ (a1 * N1 * 2 + a2 * N2 * 1 + a3 * N3 * 1) mod N
≡ (1 * 35 * 2 + 3 * 21 * 1 + 5 * 15 * 1) mod 105
≡ (70 + 63 + 75) mod 105
≡ 208 mod 105
≡ 103

Therefore, the solution to the system of congruences is x ≡ 103 (mod 105).

4 Question 11

11. Please prove the following two results.

    (a) Let $q \geq 7$ be a prime number, prove the number $\underbrace{11 \cdots 1}_{q-1 \;\; 1's}$ can be divisible by q.

    (b) Let $x \geq 1$ be a positive integer, prove $Y = x + \sum_{i=1}^{x} 2^{2i-1}$ can be divisible by 3.

My answer:

(a) To prove that the number 11...1 (q-1) is divisible by q, we can use the fact that 11...1 (q-1) can be expressed as a geometric series.

Let's denote the number 11...1 (q-1) as N. It can be written as:

$N = 10^{q-1} + 10^{q-2} + \ldots + 10^1 + 10^0$

Now, let's consider N modulo q:

$N \equiv (10^{q-1)} + 10^{q-2} + \ldots + 10^1 + 10^0) modq$

We can rewrite each term in the sum using the property of modular arithmetic:

$10^i \equiv 10^i modq$

Now, let's consider the sum of the terms modulo q:

$N \equiv (10^{q-1} modq + 10^{q-2} modq + \ldots + 10^1 modq + 100 modq) \bmod q$

Since q is a prime number, we can use Fermat's Little Theorem, which states that for any prime number p and any integer a not divisible by p, a^(p-1) ≡ 1 mod p.

In this case, since 10 is not divisible by q, we can apply Fermat's Little Theorem:

10^(q-1) ≡ 1 mod q
10^(q-2) ≡ 1 mod q
...
10^1 ≡ 1 mod q
10^0 ≡ 1 mod q

Substituting these congruences back into the sum, we get:

N ≡ (1 + 1 + ... + 1 + 1) mod q

Since there are q-1 terms in the sum, we have:

N ≡ (q-1) mod q

Therefore, N is divisible by q.

(b) To prove that $Y = x + \sum_{i=1}^{x} 2^{2i-1}$ can be divisible by 3, we can use mathematical induction.

Base case: For x = 1, Y = 1 + 2^(2*1-1) = 1 + 2^1 = 1 + 2 = 3, which is divisible by 3.

Inductive step: Assume that for some positive integer k, $Y = k + \sum(2^{2i-1})$ is divisible by 3.

Now, let's consider the case for x = k + 1:

$Y = (k+1) + \sum(2^{2i-1}) = k + \sum(2^{2i-1}) + 1 = k + Y + 1$

We can rewrite Y as:

$Y = k + \sum(2^{2i-1}) = k + (2^{2k-1} + 2^{2(k-1)-1} + \ldots + 2^1 + 2^0)$

Notice that the sum of the terms in the parentheses is a geometric series with a common ratio of 2^2 and a first term of 2^(2k-1).

Using the formula for the sum of a geometric series, we can simplify the sum:

$\sum(2^{2i-1}) = (2^{2k-1} - 1)/(2^2 - 1) = (2^{2k-1} - 1)/3$

Substituting this back into the expression for Y, we get:

$Y = k + (2^{2k-1} - 1)/3 + 1 = (k+1) + (2^{2k-1} - 1)/3$

Since k + 1 is divisible by 3 (by the inductive hypothesis), and $(2^{2k-1} - 1)/3$ is an integer, $Y = (k+1) + (2^{2k-1} - 1)/3$is divisible by 3.

Therefore, by mathematical induction,$Y = x + \sum(2^{2i-1})$can be divisible by 3 for any positive integer x.