

**MATH 470: Communications and Cryptography****Homework 5***Due date: 4 October 2023**Name: Huy Lai*

**Problem 1.** Alice publishes her RSA public key: modulus  $N = 2038667$  and exponent  $e = 103$ .

**Subproblem 1.** Bob wants to send Alice the message  $m = 892383$ . What ciphertext does Bob send to Alice?

**Solution:**

Bob sends  $c = m^e \equiv 45293 \pmod{N}$

**Subproblem 2.** Alice knows that her modulus factors into a product of two primes, one of which is  $p = 1301$ . Find a decryption exponent  $d$  for Alice.

**Solution:**

The modulus  $N = 1301 \cdot 1567$ , so  $\phi(N) = 1300 \cdot 1568 = 2035800$ .

A decryption exponent is given by a solution to

$$e \cdot d \equiv 1 \pmod{\phi(N)}$$

The solution is  $d = 810367 \pmod{\phi(N)}$

**Subproblem 3.** Alice receives the ciphertext  $c = 317730$  from Bob. Decrypt the message.

**Solution:**

Alice needs to solve  $m^e \equiv c \pmod{N}$ .

Raising both sides to the power of  $d$  yields

$$m \equiv c^d \pmod{N} \equiv 514407 \pmod{N}$$

**Problem 2.** Let  $N = pq = 352717$  and  $(p - 1)(q - 1) = 351520$ , use the method described in Remark 3.11 to determine  $p$  and  $q$ .

**Solution:**

$p + q = N + 1 - (p - 1)(q - 1) = 1198$ , so

$$X^2 - (p + q)X + N = X^2 - 1198X + 352717 = (X - 677)(X - 521)$$

Hence  $p = 677, q = 521$

**Problem 3.** Alice decides to use RSA with the public key  $N = 1889570071$ . In order to guard against transmission errors, Alice has Bob encrypt his message twice, once using the encryption exponent  $e_1 = 1021763679$  and once using the encryption exponent  $e_2 = 519424709$ . Eve intercepts the two encrypted messages

$$c_1 = 1244183534 \text{ and } c_2 = 732959706$$

Assuming that Eve also knows  $N$  and the two encryption exponents  $e_1$  and  $e_2$ , use the method described in Example 3.15 to help Eve recover Bob's plaintext without finding a factorization of  $N$ .

**Solution:**

With the method described in Example 3.15, we find that

$$u \cdot e_1 + v \cdot e_2 = 1$$

with

$$u = 252426389 \text{ and } v = -496549570$$

Then the plaintext is

$$m \equiv c_1^u \cdot c_2^v \equiv 1054592380 \pmod{N}$$

**Problem 4.** Use the Miller–Rabin test on each of the following numbers. In each case, either provide a Miller–Rabin witness for the compositeness of  $n$ , or conclude that  $n$  is probably prime by providing 10 numbers that are not Miller–Rabin witnesses for  $n$ .

**Subproblem 1.**  $n = 118901509$

**Solution:**

$$n - 1 = 118901508 = 2^2 \cdot 29725377$$

$$2^{29725377} \equiv 7906806 \pmod{n}$$

$$2^{2 \cdot 29725377} \equiv -1 \pmod{n}$$

$$3^{29725377} \equiv -1 \pmod{n}$$

$$3^{2 \cdot 29725377} \equiv 1 \pmod{n}$$

$$5^{29725377} \equiv -1 \pmod{n}$$

$$5^{2 \cdot 29725377} \equiv 1 \pmod{n}$$

$$7^{29725377} \equiv 7906806 \pmod{n}$$

$$7^{2 \cdot 29725377} \equiv -1 \pmod{n}$$

$$11^{29725377} \equiv -1 \pmod{n}$$

$$11^{2 \cdot 29725377} \equiv 1 \pmod{n}$$

Thus 2, 3, 5, 7, and 11 are not Miller–Rabin witnesses for  $n$ .  $n$  is probably prime.

**Subproblem 2.**  $n = 118901521$

**Solution:**

$$n - 1 = 118901520 = 2^4 \cdot 7431345$$

$$2^{7431345} \equiv 45274074 \pmod{n}$$

$$2^{2 \cdot 7431345} \equiv 1758249 \pmod{n}$$

$$2^{4 \cdot 7431345} \equiv 1 \pmod{n}$$

$$2^{8 \cdot 7431345} \equiv 1 \pmod{n}$$

Thus 118901521 is composite. It factors into  $n = 271 \cdot 541 \cdot 811$

**Problem 5.** Show that the Elgamal encryption protocol is insecure against a Chosen Ciphertext Attack. More specifically, suppose Bob has published a prime  $p$ , primitive root  $g \pmod p$ , and his public key  $B$ . Alice has sent Bob a ciphertext  $(c_1, c_2)$ . So far Eve only knows  $p, g, B$ , and  $(c_1, c_2)$ . But suppose now that Eve can somehow make Bob decrypt “random-looking” ciphertexts  $(c'_1, c'_2)$  of Eve’s choice (by “random-looking” we mean that Bob should not be able to tell that  $(c'_1, c'_2)$  or its decryption is related to Alice’s message in any way). Show how Eve can use this ability to decrypt Alice’s message.

**Solution:**

We can generate a “random” cipher text for Bob to decrypt using a second message  $m'$  and Eve’s secret key  $k'$  as follows:

$$c'_1 = c_1 \cdot g^{k'} \equiv g^{k+k'} \pmod p$$

$$c'_2 = c_2 \cdot B^{k'} \cdot m' \equiv (m \cdot m') \cdot B^{k+k'} \pmod p$$

Bob uses this information to calculate the “encrypted” message to send back as follows:

$$m'' = m \cdot m'$$

With this, the original message can be recovered by calculating  $m'' \cdot (m')^{-1}$ .

**Problem 6.** Let  $N = pq$  be a product of two distinct odd primes  $p$  and  $q$ . Show that there are four square roots of 1 modulo  $N$ . In other words, show that there are exactly four integers in  $\{1, 2, 3, \dots, N-1\}$  whose squares are congruent to 1 mod  $N$ .

**Solution:**

Since  $p-1$  and  $q-1$  are both even,  $\exists m, n \in \mathbb{Z}$  such that  $p-1 = 2m, q-1 = 2n$

By Fermat's Little Theorem we know that if  $a \nmid p$  and  $p$  is prime,

$$a^{p-1} \equiv 1 \pmod{p}$$

Substituting  $2m$  for  $p-1$  gives us

$$a^{2m} \equiv 1 \pmod{p}$$

This is equivalent to  $(a^m)^2 \equiv 1 \pmod{p}$

We know from a previous homework question that there exists exactly two solutions to the above equation.

A similar logic can be applied to  $q$ .

This gives two equations as follows

$$\begin{aligned} (a^m)^2 &\equiv 1 \pmod{p} \\ (b^n)^2 &\equiv 1 \pmod{q} \end{aligned}$$

The solution to these equations are  $a_1, a_2, b_1, b_2$ .

Since  $\gcd(p, q) = 1$ , the Chinese Remainder Theorem asserts that pair of solutions,  $(a_1, b_1), (a_1, b_2), (a_2, b_1), (a_2, b_2)$ , there exists a unique solution modulo  $N$ .

Therefore, there are exactly four integers in the set  $\{1, 2, 3, \dots, N-1\}$  whose squares are congruent to 1 mod  $N$ .

These integers correspond to the four combinations of  $(a_1, b_1), (a_1, b_2), (a_2, b_1), (a_2, b_2)$  when using CRT.

**Problem 7.** Suppose that you are given an integer  $N$  and a pair of integers  $e, d$  with the promise that  $N$  is the product of two large primes and that  $ed \equiv 1 \pmod{\phi(N)}$  (but you are not given the factors of  $N$  nor the value of  $\phi(N)$ ). Describe an algorithm that efficiently factors  $N$ .

**Solution:**

Note that since  $ed \equiv 1 \pmod{\phi(N)}$ , by proposition,  $\phi(N) \mid ed - 1$ . This implies that  $k \cdot \phi(N) + 1 = ed, k \in \mathbb{Z}$

1. Compute a random integer  $a$  such that  $1 < a < N$ . This is similar to how the Miller-Rabin primality test selects random witnesses.
2. Calculate the value  $x \equiv a^d \pmod{N}$ . Since  $ed \equiv 1 \pmod{\phi(N)}$ , this means that  $x^e \equiv a^{(d \cdot e)} \equiv a^{(k \cdot \phi(N) + 1)} \equiv a \pmod{N}$ , where  $k$  is an integer.
3. Use the Extended Euclidean Algorithm to find  $g = \gcd(N, x - a)$ . If the  $g > 1$ , then it means that  $N$  has a non-trivial factor in common with  $x - a$ .
4. If  $g = 1$ , repeat steps 1-3 with a different random value of  $a$ . Keep doing this until you find  $g > 1$  or until you've tried a sufficient number of random values of  $a$ .
5. Once you find a  $g > 1$ , you have effectively found one of the prime factors of  $N$ , either  $p$  or  $q$ .