MATH 233: ASSIGNMENT 5

DUE: **MONDAY, MARCH 4**, 11:59PM ON GRADESCOPE
UNIVERSITY OF ROCHESTER, SPRING 2024

Problem 1 (9.8.5, modified)**.** The ciphertext 6856 was obtained using RSA with $n = 11111$ and $e = 257$. Show that $m = 10$ cannot be the corresponding plaintext, without factoring n. (*Hint.* $11111 \cdot 9 = 99999$. You will not need a calculator.)

Solution. Since $10^5 = 100000 \equiv 1 \pmod{11111}$ and $257 = 5 \cdot 51 + 2$,

$$10^{257} \equiv (100000)^{51} 10^2 \equiv 1^{51} \cdot 100 \equiv 100 \pmod{11111}.$$

Therefore, 10 cannot be the plaintext. □

Problem 2 (9.8.13)**.** Naive Nelson uses RSA to receive a single ciphertext c, corresponding to the message m. His public modulus is n and his public encryption exponent is e. Since he feels guilty that his system was used only once, he agrees to decrypt any ciphertext that someone sends him, as long as it is not c, and return the answer to that person. Evil Eve sends him the ciphertext $2^e c \pmod{n}$. Show how this allows Eve to find m.

Solution. Suppose that Nelson sends m' back to Eve. If d is the decryption exponent, we have

$$m' \equiv (2^e c)^d \equiv 2^{de} c^d \equiv 2^{de} m \pmod{n}.$$

Since $2^{de} \equiv 2 \pmod{n}$ by Euler's Theorem, we have

$$m' \equiv 2m \pmod{n}.$$

Now Eve can find m as

$$m \equiv 2^{-1} m' \pmod{n},$$

using the multiplicative inverse 2^{-1} of 2 mod n which can be obtained easily. □

Problem 3 (9.8.31, modified)**.** Suppose two users Alice and Bob have the same RSA modulus n and suppose that their encryption exponents e_A and e_B are relatively prime. Charles wants to send the message m to Alice and Bob, so he encrypts to get $c_A \equiv m^{e_A}$ and $c_B \equiv m^{e_B} \pmod{n}$. Suppose that $\gcd(m, n) = 1$. Show how Eve can find m if she intercepts c_A and c_B. (*Hint.* Use Bezout's identity.)

Solution. Since e_A and e_B are relatively prime, one can find two integers f_A and f_B such that

$$e_A f_A + e_B f_B = 1.$$

Then

$$c_A^{f_A} c_B^{f_B} \equiv (m^{e_A})^{f_A} (m^{e_B})^{f_B} \equiv m^{e_A f_A + e_B f_B} \equiv m \pmod{n},$$

and Eve is able to calculate this from intercepted ciphertexts and public information e_A, e_B. □

Problem 4 (9.8.26)**.** Suppose you want to factor an integer n. You have found some integers x_1, x_2, x_3, x_4 such that

$$x_1^2 \equiv 2 \cdot 3 \cdot 7, \quad x_2^2 \equiv 3 \cdot 5 \cdot 7, \quad x_3^2 \equiv 3^9, \quad x_4^2 \equiv 2 \cdot 7 \pmod{n}.$$

Describe how you might be able to use this information to factor n. (Indicate explicitly what might be a factor of n.) Why might the method fail?

Solution. We have

$$(x_1 x_3 x_4)^2 \equiv 2^2 \cdot 3^{10} \cdot 7^2 \equiv (2 \cdot 3^5 \cdot 7)^2 \pmod{n}.$$

Therefore, If $x_1 x_3 x_4 \not\equiv 2 \cdot 3^5 \cdot 7 \pmod{n}$, then $\gcd(x_1 x_3 x_4 - 2 \cdot 3^5 \cdot 7, n)$ is a factor of n. However, if $x_1 x_3 x_4 \equiv 2 \cdot 3^5 \cdot 7$ or $x_1 x_3 x_4 \equiv -2 \cdot 3^5 \cdot 7 \pmod{n}$, then the method fails. □

Problem 5. Let $n(= pq), d, e$ be the RSA modulus, the decryption exponent, and the encryption exponent, respectively, of the RSA cryptosystem. Show that

$$\left\lceil \frac{de-1}{n} \right\rceil = \frac{de-1}{\phi(n)}$$

if

$$e \le \frac{n}{p+q-1}.$$

(*Hint.* Observe that $(de-1)/\phi(n)$ is an integer by definition, and $(de-1)/n$ is always smaller than $(de-1)/\phi(n)$. Therefore, the given equality holds if and only if

$$\frac{de-1}{n} > \frac{de-1}{\phi(n)} - 1.$$

Show that the given inequality on e implies the above inequality. You may have to use the fact that $d < \phi(n)$.)

Solution. Observe that

$$p + q - 1 = n - \phi(n).$$

Therefore, if

$$e \le \frac{n}{p+q-1} = \frac{n}{n-\phi(n)},$$

then

$$de - 1 < \frac{n\phi(n)}{n - \phi(n)} = \frac{1}{\frac{1}{\phi(n)} - \frac{1}{n}} \quad \Rightarrow \quad \frac{de-1}{\phi(n)} - \frac{de-1}{n} < 1$$

(here we used $d < \phi(n)$). This implies the inequality given in the hint. □

Problem 6 (10.6.7, modified)**.** Let $p = 101$, which is a prime number. We know that 2 is a primitive root mod p. It can also be shown that $L_2(3) = 69$.

(a) Evaluate $L_2(72)$ using the fact that $72 = 2^3 \cdot 3^2$.

(b) Evaluate $L_2(11)$ using the fact that $11^{67} \equiv 2^2 \cdot 3 \pmod{101}$.

Solution. (a)

$$L_2(72) \equiv 3L_2(2) + 2L_2(3) \equiv 3 \cdot 1 + 2 \cdot 69 \equiv 141 \pmod{100} \quad \Rightarrow \quad L_2(72) = 41.$$

(b)

$$\begin{aligned} & 67L_2(11) \equiv 2L_2(2) + L_2(3) \equiv 2 \cdot 1 + 69 \equiv 71 \pmod{100} \\ \Rightarrow \quad & L_2(11) \equiv 67^{-1} \cdot 71 \equiv 3 \cdot 71 \equiv 213 \pmod{100} \\ \Rightarrow \quad & L_2(11) = 13. \end{aligned}$$

□

Problem 7. Alice and Bob agree to use the prime $p = 29$ and a primitive root $\alpha = 2$ for a Diffie-Hellman key exchange. Alice sends Bob the value $\alpha^a \equiv 11 \pmod{p}$. Bob asks your assistance, so you tell him to use the secret exponent $b = 9$. What value should Bob send to Alice, and what is their secret shared value? Can you figure out Alice's secret exponent a without solving a discrete logarithm problem? (*Hint.* $2^5 \equiv 3 \pmod{29}$, $11^3 \equiv -3 \pmod{29}$.)

Solution. Bob should send

$$2^9 \equiv 2^5 \cdot 2^4 \equiv 3 \cdot 16 \equiv 19 \pmod{p}$$

to Alice. There shared value is

$$\alpha^{ab} \equiv 11^9 \equiv (11^3)^3 \equiv (-3)^3 \equiv -27 \equiv 2 \pmod{p}.$$

Since the shared value is equal to α itself, we know that

$$ab \equiv 1 \pmod{p-1},$$

i.e., a is the multiplicative inverse of $b = 9$ mod $p - 1(= 28)$, which is 25. □

Problem 8 (10.6.16)**.** In the ElGamal cryptosystem, Alice and Bob use $p = 17$ and $\alpha = 3$. Bob chooses his secret to be $b = 6$, so $\beta = 15$. Alice sends the ciphertext $(r, t) = (7, 6)$. Determine the plaintext m.

Solution. Note that the multiplicative inverse of $r = 7$ mod $p = 17$ is $r^{-1} \equiv 5 \pmod{17}$. Then

$$m \equiv tr^{-b} \equiv 6 \cdot 7^{-6} \equiv 6 \cdot 5^6 \equiv 12 \pmod{p}.$$

Therefore, the plaintext is $m = 12$. □

Problem 9 (10.6.4)**.** Let $p = 19$. Then 2 is a primitive root. Use the Pohlig-Hellman method to compute $L_2(14)$. (For this problem, you may use any method – calculator, Wolframalpha, etc. – to evaluate modular exponentiation. However, you should not use any method other than the Pohlig-Hellman method (e.g. brute-force attack), and you should explicitly indicate every modular exponentiation you used.)

Solution. Let $x = L_2(14)$. Since $p - 1 = 18 = 2 \cdot 3^2$, we need to determine $x \pmod 2$ and $x \pmod{3^2}$. First, we make a list with $\gamma_k \equiv 2^{k(p-1)/2} \pmod p$:

k	0	1
γ_k	1	-1

Then since

$$14^{(p-1)/2} \equiv 14^9 \equiv -1 \pmod p,$$

we can conclude that $x \equiv 1 \pmod 2$.

For mod 3^2, we make a similar list with $\gamma_k \equiv 2^{k(p-1)/3} \pmod p$:

k	0	1	2
γ_k	1	7	11

Now let $x \equiv 3x_1 + x_0 \pmod{3^2}$. From

$$14^{(p-1)/3} \equiv 14^6 \equiv 7 \pmod p,$$

we have $x_0 = 1$. Then

$$14 \cdot 2^{-1} \equiv 7 \pmod p,$$

and

$$7^{(p-1)/3^2} \equiv 7^2 \equiv 11 \pmod p.$$

This implies $x_1 = 2$, therefore

$$x \equiv 3 \cdot 2 + 1 \equiv 7 \pmod{3^2}.$$

Now using the Chinese Remainder Theorem, we can conclude that

$$x \equiv 7 \pmod{p-1} \quad \Rightarrow \quad L_2(14) = 7.$$

$\square$