MATH 233: ASSIGNMENT 5

DUE: **WEDNESDAY, MARCH 6**, 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.)

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.

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.)

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?

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

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

(*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 $d < \phi(n)$.)

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 $11^{67} \equiv 2^2 \cdot 3 \pmod{101}$.

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.* $2^5 \equiv 3 \pmod{29}$, $11^3 \equiv -3 \pmod{29}$.)

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.

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.)