MATH 470.502
Examination 2 Solutions
November 26, 2014

1. Alice and Bob are using RSA to communicate.

(a) Alice's public encryption key is $(n, e) = (133, 5)$. Bob wants to encrypt the plaintext message '8' to send to Alice. What is the ciphertext that he sends?

(b) What is Alice's decryption exponent?

Solution: (a) Bob calculates $c \equiv 8^5 \equiv 50 \pmod{133}$, and so $\boxed{c = 50}$.

(b) We factor $133 = 7 \cdot 19$, and so $\phi(133) = 6 \cdot 18 = 108$. We then calculate $\frac{1}{5}$ mod 108. Since $3 \cdot 108 = 324$, we see that $5 \cdot 65 = 325 \equiv 1 \pmod{108}$. So $\frac{1}{5} \equiv \boxed{65} \pmod{108}$.

2. Bob's ElGamal public key is $(p, \alpha, \beta) = (31, 3, 19)$, and his private key is $a = 4$.

(a) Alice wants to encrypt the message '9' and send it do Bob. She first picks $k = 5$. What does she send to Bob?

(b) In a separate communication, Alice has sent Bob the encrypted ciphertext $(r, t) = (25, 28)$. What is the decrypted message?

Solution: (a) Alice calculates two quantities: $r \equiv \alpha^k \pmod{p}$, and so $r \equiv 3^5 \equiv 26 \pmod{31}$; and $t \equiv \beta^k m \pmod{p}$, and so $t \equiv 19^5 \cdot 9 \equiv 14 \pmod{31}$. Therefore $\boxed{(r, t) = (26, 14)}$.

(b) To decrypt Bob calculates $m \equiv t \cdot r^{-a} \pmod{p}$, thus $m \equiv 28 \cdot 25^{-4} \equiv \boxed{16} \pmod{31}$.

3. The following congruences hold:

$$1334^{3826} \equiv 1 \pmod{3827} \qquad 2493^{3826} \equiv 1 \pmod{3827} \tag{1}$$
$$3826^{3826} \equiv 1 \pmod{3827} \qquad 2495^{3826} \equiv 1592 \pmod{3827} \tag{2}$$

$$147^{885} \equiv 6352 \pmod{7081} \qquad 147^{1770} \equiv 366 \pmod{7081} \tag{3}$$
$$147^{3540} \equiv 6498 \pmod{7081} \qquad 147^{7080} \equiv 1 \pmod{7081} \tag{4}$$

Answer the following primality test questions. Be sure to **mention the primality test you are using and describe how it applies**.

(a) What do lines (1)–(2) tell you about the primality of 3827? Explain.

(b) What do lines (3)–(4) tell you about the primality of 7081? Explain.

Solution: (a) We apply the $\boxed{\text{Fermat's Little Theorem primality test}}$. The first three pieces of data are not useful, but the last one shows that $2495^{3827-1} \equiv 1592 \not\equiv 1 \pmod{3827}$. Therefore, $\boxed{\text{3827 must be composite}}$.

(b) Here we apply the $\boxed{\text{Miller-Rabin primality test}}$. In this case $7080 = 8 \cdot 885$. From the data provided, we see that

$$\begin{aligned} 147^{885} &\equiv 6352 \not\equiv \pm 1 \pmod{7081}, \\ 147^{2\cdot 885} &\equiv 366 \not\equiv -1 \pmod{7081}, \\ 147^{4\cdot 885} &\equiv 6498 \not\equiv -1 \pmod{7081}. \end{aligned}$$

Therefore, the Miller-Rabin test implies that $\boxed{\text{7081 is composite}}$. (Note that the final piece of data, that $147^{7080} \equiv 1 \pmod{7081}$, is not used, but it also indicates that the Fermat's Little Theorem primality test will not apply here.)

4. The number 2 is a primitive root modulo 13. Use the Pohlig-Hellman algorithm to find $L_2(7)$.

Solution: Since $13 - 1 = 12 = 2^2 \cdot 3$, we have to apply the algorithm for the primes 2 and 3.

For $q = 2$, we first find x_0 such that $2^{6x_0} \equiv 7^6 \equiv 12 \pmod{13}$. We see that $x_0 = 1$. We then calculate that $\beta_1 \equiv \alpha^{-x_0}\beta \equiv 2^{-1} \cdot 7 \equiv 10 \pmod{13}$. We look for x_1 so that $2^{6x_1} \equiv 10^3 \equiv 12 \pmod{13}$, and so $x_1 = 1$. From this we see that $y_1 = 1 + 1 \cdot 2 = 3$.

For $q = 3$, we look for x_0 such that $2^{4x_0} \equiv 7^4 \equiv 9 \pmod{13}$. It follows that $x_1 = 2$, and so $y_2 = 2$.

We thus use the Chinese remainder theorem to find x so that $x \equiv 3 \pmod 4$ and $x \equiv 2 \pmod 3$. It follows that $x \equiv 11 \pmod{12}$, and therefore $\boxed{L_2(7) = 11}$.

5. Suppose that Eric and Todd are communicating using a modified version of RSA. Eric's public key is (n_1, e_1), and his private key is d_1, both keys set up exactly as in normal RSA. Similarly Todd's public key is (n_2, e_2), and his private key is d_2. To send the plaintext message m to Todd, Eric first calculates

$$c_1 \equiv m^{d_1} \pmod{n_1},$$

and then he calculates

$$c_2 \equiv c_1^{e_2} \pmod{n_2}.$$

He then sends c_2 to Todd.

(a) Todd receives the ciphertext c_2. How does he decrypt the message? Explain.

(b) How can Todd know for certain that Eric sent him the message, rather than someone else posing as Eric?

Solution: (a) To decrypt the message, Todd must perform two congruences. He calculates $c_2^{d_2} \equiv c_1 \pmod{n_2}$ and then he calculates $c_1^{e_1} \equiv m \pmod{n_1}$.

(b) Since Eric used his decryption exponent d_1 as part of the encryption process (and he is presumably the only person who knows d_1), when Todd calculated $c_1^{e_1} \mod n_1$, he would get a recognizable message only if d_1 was used to encrypt.

6. Let $n = 10057$. We know that 10057 is the product of two distinct primes. Suppose in carrying out the quadratic sieve that you have found that

$$\begin{aligned} 81^2 - n &= -3496 = -2^3 \cdot 19 \cdot 23, & 100^2 - n &= -57 = -3 \cdot 19, \\ 83^2 - n &= -3168 = -2^5 \cdot 3^2 \cdot 11, & 103^2 - n &= 552 = 2^3 \cdot 3 \cdot 23, \\ 99^2 - n &= -256 = -2^8, & 104^2 - n &= 759 = 3 \cdot 11 \cdot 23. \end{aligned}$$

(a) Use this information to find positive integers x and y such that $x^2 \equiv y^2 \pmod{10057}$ but $x \not\equiv \pm y \pmod{10057}$.

(b) Use the information in part (a) to factor 10057.

Solution: (a) By inspection, we can find at least two correct solutions. One was

$$\begin{aligned} x &= \boxed{83 \cdot 99 \cdot 103 \cdot 104} = 88020504, \\ y &= \boxed{\sqrt{3168 \cdot 256 \cdot 552 \cdot 759}} = 582912. \end{aligned}$$

The other was

$$\begin{aligned} x &= \boxed{81 \cdot 83 \cdot 99 \cdot 100 \cdot 104}, \\ y &= \boxed{\sqrt{3496 \cdot 3168 \cdot 256 \cdot 57 \cdot 552 \cdot 759}}. \end{aligned}$$

In both cases $x^2 \equiv y^2 \pmod{10057}$ and $x \not\equiv \pm y \pmod{10057}$.

On the other hand, it was possible to consider

$$\begin{aligned} x &= 81 \cdot 100 \cdot 103, \\ y &= \sqrt{3496 \cdot 57 \cdot 552}. \end{aligned}$$

In this case $x^2 \equiv y^2 \pmod{10057}$, but $x \equiv -y \pmod{10057}$.

(b) We calculate $\gcd x - y, 10057$ to find a non-trivial factor. In the first case in (a), we can simplify a little by finding that

$$\begin{aligned} x = 88020504 &\equiv 1640 \pmod{10057}, \\ y = 582912 &\equiv 9663 \pmod{10057}. \end{aligned}$$

We then calculate that

$$\gcd(x - y, 10057) = \gcd(1640 - 9663, 10057) = \gcd(8023, 10057) = 113.$$

We then find that $\boxed{10057 = 113 \cdot 89}$. (The solution using the second set of values in (a) is similar.)