Homework 9

Question 1:

(a) Consider the Rabin encryption scheme.

Let $N = 34189$.

Let $m = 12013$

What is the ciphertext?

(b) Given $N = 34189$ and ciphertext $c = 400$.

List down all the possible plaintexts. Don't factorize N.

Hint: Use (a) above.

(c) From the possible plaintexts, find p and q, where $N = pq$.

(d) Suppose we are given an extra information that the plaintext is itself a quadratic residue modulo N.

What should be the plaintext for $c = 400$?

Homework 9

Question 1:

(a) Consider the Rabin encryption scheme.

Let $N = 34189$.

Let $m = 12013$

What is the ciphertext? $m^2 \bmod N = 400$

(b) Given $N = 34189$ and ciphertext $c = 400$.

List down all the possible plaintexts. Don't factorize N.

Hint: Use (a) above. Four possible plaintexts. $x_1, x_2 = 20, -20$

$y_1, y_2 \quad 12013, -12013$

(c) From the possible plaintexts, find p and q, where $N = pq$.

$p = \gcd(x_1 - y_1, N)$ $q = \gcd(x_1 + y_1, N)$

(d) Suppose we are given an extra information that the plaintext is itself a quadratic residue modulo N.

What should be the plaintext for $c = 400$?

If $p \equiv 3 \bmod 4$ and $q \equiv 3 \bmod 4$

then there should only be one such plaintext?

For $r \in [x_1, x_2, y_1, y_2]$, check if r is QR_N.

Example $r = 20$.

$r_p = 20 \bmod p$ $r_q \equiv 20 \bmod q$

$r_p^{\frac{p-1}{2}} \equiv 1 \bmod p$ and $r_q^{\frac{q-1}{2}} \equiv 1 \bmod q$

$\Leftrightarrow r$ is QR_N

$$J_N(m) = J_p(m) J_q(m)$$

(e) Suppose we are given the following extra information that m is less than $N/2$ and $J_N(m)$ is 1

What is the plaintext for $c = 400$?

(f) Suppose we are given the following extra information that m is more than $N/2$ and $J_N(m)$ is 1

What is the plaintext for $c = 400$?

(g) Suppose we are given the following extra information that m is less than $N/2$ and $J_N(m)$ is -1

What is the plaintext for $c = 400$?

(h) Suppose we are given the following extra information that m is more than $N/2$ and $J_N(m)$ is -1

What is the plaintext for $c = 400$?

Question 2

11.11 (a) Let N be a Blum integer. Define the function $\mathsf{half}_N : \mathbb{Z}_N^* \to \{0,1\}$ as

$$\mathsf{half}_N(x) = \begin{cases} 0 \text{ if } x < N/2 \\ 1 \text{ if } x > N/2 \end{cases}$$

Show that the function $f : \mathbb{Z}_N^* \to \mathcal{QR}_N \times \{0,1\}^2$ defined as

$$f(x) = [x^2 \bmod N], \mathcal{J}_N(x), \mathsf{half}_N(x)$$

is one-to-one.

(b) Using the previous result, suggest a variant of the padded Rabin encryption scheme that encrypts messages of length n. (All algorithms of your scheme should run in polynomial time, and the scheme should have correct decryption. Although a proof of security is unlikely, your scheme should not be susceptible to any obvious attacks.)

(c) What's the drawback of this scheme?

Question 2

11.11 (a) Let N be a Blum integer. Define the function $\mathsf{half}_N : \mathbb{Z}_N^* \to \{0,1\}$ as

$$\mathsf{half}_N(x) = \begin{cases} 0 \text{ if } x < N/2 \\ 1 \text{ if } x > N/2 \end{cases}$$

Show that the function $f : \mathbb{Z}_N^* \to \mathcal{QR}_N \times \{0,1\}^2$ defined as

$$f(x) = [x^2 \bmod N], \mathcal{J}_N(x), \mathsf{half}_N(x)$$

is one-to-one.

(b) Using the previous result, suggest a variant of the padded Rabin encryption scheme that encrypts messages of length n. (All algorithms of your scheme should run in polynomial time, and the scheme should have correct decryption. Although a proof of security is unlikely, your scheme should not be susceptible to any obvious attacks.)

(c) What's the drawback of this scheme?

(a) Domain of f is $\mathbb{Z}_N^*$. $|\mathbb{Z}_N^*| = (p-1)(q-1)$

Codomain of f is $\mathcal{QR}_N \times \{0,1\}^2$. Size is $|\mathcal{QR}_N| \times 2^2$

$$= \frac{|\mathbb{Z}_N^*|}{4} \times 4$$

$$= |\mathbb{Z}_N^*|$$

To show f is one-to-one.

We show that if $f(x_1) = f(x_2)$ then $x_1 = x_2$.

Observations :

Let $y = (y_p, y_q)$ and

$x_p^2 = y_p \mod p$

$x_q^2 = y_q \mod q$

Observation 1: If $x = (x_p, x_q) < N/2$, then $-x \mod N \geq N/2$.

Observation 2 : If $x = (x_p, x_q)$ $J_N(-x) = J_p(-x) J_q(-x)$
$= -J_p(x) \cdot -J_q(x) = J_N(x)$

Because -1 is not a QR mod p

when $p \equiv 3 \mod 4$.

Here $J_p(-1) = -1$.

---

x	$x^2 \mod N$	$J_N(x)$	$half_N(x)$
$x_1 = (x_p, x_q)$	$y = (y_p, y_q)$	c	a
$x_2 = (-x_p, -x_q)$	y	c	$\bar{a}$
$x_3 = (x_p, -x_q)$	y	d	b
$x_4 = (-x_p, x_q)$	y	d	$\bar{b}$

$a \in \{0, 1\}$

$\bar{a}$ = inverse bit of a

If $c \neq d$, then $J_N(x)$ and $\text{half}_N(x)$ uniquely define each of x_1, x_2, x_3, x_4

$x_1 = (x_p, x_q)$

$x_3 = (x_p, -x_q)$

$J_N(x_1) = J_p(x_p)\, J_q(x_q)$

$J_N(x_3) = J_p(x_p)\, J_q(-x_q)$

$= J_p(x_p)\, J_q(-1)\, J_q(x_q)$

$= -J_p(x_p)\, J_q(x_q)$

$= -J_N(x_1)$

Question 3: Elgamal Encryption Scheme

Public parameter creation	
A trusted party chooses and publishes a large prime p and an element g modulo p of large (prime) order.	
Alice	**Bob**
Key creation	
Choose private key $1 \leq a \leq p-1$. Compute $A = g^a \pmod{p}$. Publish the public key A.	
Encryption	
	Choose plaintext m. Choose random element k. Use Alice's public key A to compute $c_1 = g^k \pmod{p}$ and $c_2 = mA^k \pmod{p}$. Send ciphertext (c_1, c_2) to Alice.
Decryption	
Compute $(c_1^a)^{-1} \cdot c_2 \pmod{p}$. This quantity is equal to m.	

Table 2.3: Elgamal key creation, encryption, and decryption

2.8. Alice and Bob agree to use the prime $p = 1373$ and the base $g = 2$ for communications using the Elgamal public key cryptosystem.

(a) Alice chooses $a = 947$ as her private key. What is the value of her public key A?

(b) Bob chooses $b = 716$ as his private key, so his public key is

$$B \equiv 2^{716} \equiv 469 \pmod{1373}.$$

Alice encrypts the message $m = 583$ using the random element $k = 877$. What is the ciphertext (c_1, c_2) that Alice sends to Bob?

(c) Alice decides to choose a new private key $a = 299$ with associated public key $A \equiv 2^{299} \equiv 34 \pmod{1373}$. Bob encrypts a message using Alice's public key and sends her the ciphertext $(c_1, c_2) = (661, 1325)$. Decrypt the message.

(d) Now Bob chooses a new private key and publishes the associated public key $B = 893$. Alice encrypts a message using this public key and sends the ciphertext $(c_1, c_2) = (693, 793)$ to Bob. Eve intercepts the transmission. Help Eve by solving the discrete logarithm problem $2^b \equiv 893 \pmod{1373}$ and using the value of b to decrypt the message.

Question 4 :

2.10. The exercise describes a public key cryptosystem that requires Bob and Alice to exchange several messages. We illustrate the system with an example.

Bob and Alice fix a publicly known prime $p = 32611$, and all of the other numbers used are private. Alice takes her message $m = 11111$, chooses a random exponent $a = 3589$, and sends the number $u = m^a \pmod{p} = 15950$ to Bob. Bob chooses a random exponent $b = 4037$ and sends $v = u^b \pmod{p} = 15422$ back to Alice. Alice then computes $w = v^{15619} \equiv 27257 \pmod{32611}$ and sends $w = 27257$ to Bob. Finally, Bob computes $w^{31883} \pmod{32611}$ and recovers the value 11111 of Alice's message.

(a) Explain why this algorithm works. In particular, Alice uses the numbers $a = 3589$ and 15619 as exponents. How are they related? Similarly, how are Bob's exponents $b = 4037$ and 31883 related?

(b) Formulate a general version of this cryptosystem, i.e., using variables, and show that it works in general.

(c) What is the disadvantage of this cryptosystem over Elgamal? (*Hint.* How many times must Alice and Bob exchange data?) deterministic and multiple transaction

(d) Are there any advantages of this cryptosystem over Elgamal? In particular, can Eve break it if she can solve the discrete logarithm problem? Can Eve break it if she can solve the Diffie–Hellman problem?

$$m = W^{31883} = v^{15619 \cdot 31883}$$

$$= u^{b \cdot 15619 \cdot 31883}$$

$$= m^{a \cdot b \cdot 15619 \cdot 31883}$$

$$a \cdot b \cdot 15619 \cdot 31883 = 1$$

$$15619 = a^{-1} \bmod p-1$$

$$31883 = b^{-1} \bmod p-1$$

Question 4:

2.10. The exercise describes a public key cryptosystem that requires Bob and Alice to exchange several messages. We illustrate the system with an example.

Bob and Alice fix a publicly known prime $p = 32611$, and all of the other numbers used are private. Alice takes her message $m = 11111$, chooses a random exponent $a = 3589$, and sends the number $u = m^a \pmod{p} = 15950$ to Bob. Bob chooses a random exponent $b = 4037$ and sends $v = u^b \pmod{p} = 15422$ back to Alice. Alice then computes $w = v^{15619} \equiv 27257 \pmod{32611}$ and sends $w = 27257$ to Bob. Finally, Bob computes $w^{31883} \pmod{32611}$ and recovers the value 11111 of Alice's message.

(a) Explain why this algorithm works. In particular, Alice uses the numbers $a = 3589$ and 15619 as exponents. How are they related? Similarly, how are Bob's exponents $b = 4037$ and 31883 related?

(b) Formulate a general version of this cryptosystem, i.e., using variables, and show that it works in general.

(c) What is the disadvantage of this cryptosystem over Elgamal? (*Hint*. How many times must Alice and Bob exchange data?) deterministic and multiple transaction

(d) Are there any advantages of this cryptosystem over Elgamal? In particular, can Eve break it if she can solve the discrete logarithm problem? Can Eve break it if she can solve the Diffie–Hellman problem?

For Elgamal, if Eve can solve DHP, Eve breaks Elgamal.

For this system, it appears that it is not easy to break it even we can solve DHP.

DHP: $A = g^a \bmod p$

$B = g^b \bmod p$

Solve $g^{ab} \bmod p$