Homework 7

Question 1

The congruence

$$x^e \equiv c \mod p$$

has a unique solution congruence modulo prime p when $\gcd(e, p-1) = 1$.

In this question, you are asked to explore what happen when $\gcd(e, p-1) \neq 1$.

Consider p prime. $c \not\equiv 0 \mod p$. $e \geq 1$.

(1) Give an example of p (prime), $c \not\equiv 0 \mod p$, $e \geq 1$ such that $x^e \equiv c \mod p$ has no solution.

(2) Give an example of p (prime), $c \not\equiv 0 \mod p$, $e \geq 1$ such that $\gcd(e, p-1) \neq 1$ and $x^e \equiv c \mod p$ has at least two solutions.

Prove that if $x^e \equiv c \mod p$ has a solution, then it has exactly $\gcd(e, p-1)$ distinct solutions.

① $e=2,\ p=5$

$$x^2 \equiv c \mod p$$

Find c in $\mathbb{Z}_p^*$ st
c is not a square / quadratic residue

② $e=2$, odd prime p

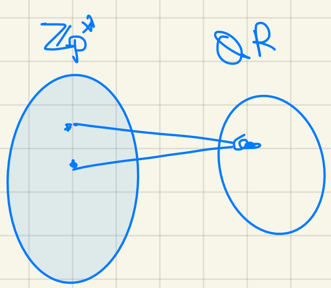
$$x^2 \equiv c \mod p$$

where c in $\mathbb{Z}_p^*$ st c is a square / quadratic residue.

$QR \subseteq \mathbb{Z}_p^*$ p odd prime

$QR = \{ g^2,\ g \in \mathbb{Z}_p^* \}$

$$|QR| = \frac{|\mathbb{Z}_p|^*}{2}$$



2 to 1 function

Bob	Alice
Key creation	
Choose secret primes p and q. Choose encryption exponent e with $\gcd(e, (p-1)(q-1)) = 1$. Publish $N = pq$ and e.	
Encryption	
	Choose plaintext m. Use Bob's public key (N, e) to compute $c \equiv m^e \pmod{N}$. Send ciphertext c to Bob.
Decryption	
Compute d satisfying $ed \equiv 1 \pmod{(p-1)(q-1)}$. Compute $m' \equiv c^d \pmod{N}$. Then m' equals the plaintext m.	

Table 3.1: RSA key creation, encryption, and decryption

Question 2

Section. The RSA public key cryptosystem

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

(a) Bob wants to send Alice the message $m = 892383$. What ciphertext does Bob send to Alice?

(b) 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.

(c) Alice receives the ciphertext $c = 317730$ from Bob. Decrypt the message.

Question 3

3.8. Bob's RSA public key has modulus $N = 12191$ and exponent $e = 37$. Alice sends Bob the ciphertext $c = 587$. Unfortunately, Bob has chosen too small a modulus. Help Eve by factoring N and decrypting Alice's message. (*Hint.* N has a factor smaller than 100.)

Question 4

3.13. 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

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

Assuming that Eve also knows N and the two encryption exponents e_1 and e_2,

Can Eve find out the plaintext without finding p, q?

Question 2 For RSA, if you know $\phi(N) = (p-1)(q-1)$, then you can compute d.

Section. The RSA public key cryptosystem

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

(a) Bob wants to send Alice the message $m = 892383$. What ciphertext does Bob send to Alice?

(b) 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.

(c) Alice receives the ciphertext $c = 317730$ from Bob. Decrypt the message.

(a) $m^e \bmod N$

(b) $q = N/p$

compute $\phi(N) = (p-1)(q-1)$

compute d such that

$ed \equiv 1 \bmod \frac{\phi(N)}{g}$ $g = \gcd(p-1, q-1)$

(c) $m = c^d \bmod N$

Question 3

3.8. Bob's RSA public key has modulus $N = 12191$ and exponent $e = 37$. Alice sends Bob the ciphertext $c = 587$. Unfortunately, Bob has chosen too small a modulus. Help Eve by factoring N and decrypting Alice's message. (*Hint.* N has a factor smaller than 100.)

for p from 3 to $\sqrt{N}$:

check if p divides N, break

Once p is found, use strategy in Question 2

Question 4

3.13. 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

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

Assuming that Eve also knows N and the two encryption exponents e_1 and e_2,

Can Eve find out the plaintext without finding p, q?

$$c_1 \equiv m^{e_1} \bmod N$$

$$c_2 \equiv m^{e_2} \bmod N$$

$$\gcd(e_1, e_2) = 1$$

Using Extended Euclidean algorithm to find u, v s.t

$$e_1 u + e_2 v = 1$$

$$c_1^u c_2^v = m^{e_1 u} m^{e_2 v} = m^{e_1 u + e_2 v} = m \bmod N$$

Question 5

The following question is an experiment for the following statement:

> If $N = pq$ is a product of two distinct odd primes. If $e = 3$ and d is given such that $3d \equiv 1 \mod \phi(N)$. then we can find $\phi(N)$ easily.

For each of the following values, find $\phi(N)$:

(a) $N = 17693317$, $e = 3$, $d = 11789931$

(b) $N = 61853041$, $e = 3$, $d = 41224875$

Hint ① $\varphi(N) \mid 3d-1$

Let $N' = 3d-1$

We know $\varphi(N)$ is a factor of N'.

N' is a small multiple of N.

$\varphi(N)$ is $\frac{(p-1)(q-1)}{pq}$ of $N \rightarrow \varphi(N) \simeq N$.

N' is a "small" multiple of $\varphi(N)$.

Find k s.t k divides N', and compute $N'//k$, which is a potential value of $\varphi(N)$. Use ② to check if $N'//k$ is actualy equal to $(p-1)(q-1)$ for some pimes p and q.

② Given N and $\varphi(N)$, find p, q.

(a) compute $p+q$ using

$$\varphi(N) = (p-1)(q-1) = pq - (p+q) + 1$$

(b) compute p, q by finding roots of

$$x^2 - (p+q)x + pq = 0$$

Additional Questions

① Double encryption RSA.

Public parameters: N, e_1, e_2

private parameters: d_1, d_2, p, q

To encrypt: $C_1 = m^{e_1} \mod N$

$C_2 = C_1^{e_2} \mod N$

To decrypt: [TODO]

[TODO] Argue whether Double encryption RSA is equal / less / more secure than RSA.

2) Multi prime RSA

$N = pqr$ where p, q, r are distinct odd primes.

public parameters : N, e

private parameters : d, p, q

To encrypt : $m^e \bmod N$

To decrypt : $c^d \bmod N$

How to find d?

$ed \equiv 1 \bmod ??$

Argue whether multiprime RSA is equal / more / less secure than RSA.

Argue whether there is an advantage of using multiprime.