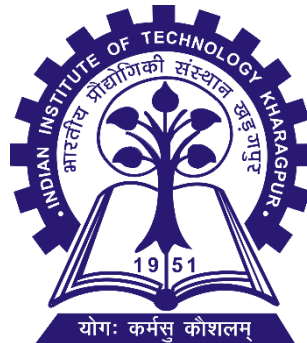


Cryptography and Network Security (CS60065)

AUTUMN, 2021-2022

TA: Tapadyoti Banerjee

Course Instructor: Prof. Dipanwita Roy Chowdhury
Department of Computer Science & Engineering
Indian Institute of Technology, Kharagpur
West Bengal 721302, India



TUTORIAL: 5
DATE: 29th October 2021

QUESTION : 1 (Quadratic Residue)

p is an odd prime

a is an int

a is not congruent to 0 (mod p)

y^2 is congruent to a (mod p) ... y belongs to \mathbb{Z}_p

Find the quadratic residues and quadratic non-residues in \mathbb{Z}_{11}

$$1^2 = 1$$

$$2^2 = 4$$

$$3^2 = 9$$

$$4^2 = 5$$

$$5^2 = 3$$

$$6^2 = 3$$

$$7^2 = 5$$

$$8^2 = 9$$

$$9^2 = 4$$

$$10^2 = 1$$

1, 3, 4, 5, 9

QUESTION : 2 (Congruence)

Let g be a primitive root for \mathbb{F}_p . Suppose that $x = a$ and $x = b$ are both integer solutions to the congruence $g^x \equiv h \pmod{p}$. Prove that $a \equiv b \pmod{p-1}$.

$g^a = g^b \pmod{p}$, since they are both congruent to h .

$$g^{a-b} = 1 \pmod{p}$$

But, g is a primitive root, so its order is $p-1$,
which imply that $p-1$ divides $a-b$.

$$a \equiv b \pmod{p-1}$$

QUESTION : 3 (RSA Crypto System)

Alice uses the RSA Crypto System to receive messages from Bob. She chooses $p=13$, $q=23$, and her public exponent $e=35$. Alice published the product $n=pq=299$ and $e=35$.

- (i) Check that $e=35$ is a valid exponent for the RSA algorithm. **Valid**
- (ii) Compute d , the private exponent of Alice **83**

Bob wants to send to Alice the (encrypted) plaintext $P=15$.

- (iii) What does he send to Alice ?
- (iv) Verify she can decrypt this message

$$p, g, a, A = g^a \pmod{p}$$

$$b, B = g^b \pmod{p}$$

$$s = B^a \pmod{p}$$

$$s = A^b \pmod{p}$$

QUESTION : 4 (Diffie-Hellman key exchange)

Alice and Bob agree to use the prime $p = 1373$ and the base $g = 2$ for a Diffie-Hellman key exchange. Alice sends Bob the value $A = 974$. Bob asks your assistance, so you tell him to use the secret exponent $b = 871$. What value B should Bob send to Alice, and what is their secret shared value? Can you figure out Alice's secret exponent?

QUESTION : 5 (The ElGamal public key cryptosystem)

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

(i) 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 ephemeral key $k = 877$. What is the cipher text (c_1, c_2) that Alice sends to Bob?

Key Generation: G, q, g, e

$x \in \{1, \dots, q-1\}$

$h = g^x$

$\text{PUBK}(G, q, g, h), \text{PRIVK}(x)$

Encryption: M

$y \in \{1, \dots, q-1\}$

$s = h^y$

$c_1 = g^y, c_2 = m \cdot s; (c_1, c_2)$

Decryption: $s = c_1^x = h^y$

$s^{-1}, m = c_2 s^{-1}$

QUESTION : 6 (Rabin Cryptosystem)

Suppose we want to decrypt the cipher text $y = 23$ by using the Rabin Cryptosystem. Illustrate the procedure with this toy example by considering by considering the public key, $n = 77$.