Cryptography and Network Security (CS60065)

AUTUMN, 2021-2022

TA: Tapadyoti Banerjee and Rijoy Mukherjee

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

TUTORIAL: 4
DATE: 26th October 2022

QUESTION : 1 (Quadratic Residue)

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

QUESTION : 2 (Congruence)

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

QUESTION : 3 (Z^*_p and cyclic group)

Suppose p = 13. Find how many primitive elements are there in modulo 13. And, examine it for 2.

QUESTION : 4 (RSA Algorithm)

Consider the keys: public key PU = {7,187} and private key PR = {23,187}. Now, use these keys for a plaintext input of M = 88, determine the ciphertext and also decrypt it.

QUESTION : 5 (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.

(ii) Compute d , the private exponent of Alice

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

QUESTION : 6 (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?