CSCI361-2025S1-ClassTest-v1

Question 1

a. Using your 7-digit UOW student number to form two numbers n_1 and n_2. The number n_1 is formed by taking the last four digits of your 7-digit student number and n_2 is formed by taking the first three digits of your 7-digit student number. For example, student number 6256247 will form $n_1 = 6247$ and $n_2 = 625$. If the last four digits of your student number consists of leading zero, change the first leading 0 to a 1. For example, 6550046 will form $n_1 = 1046$ (change the first leading zero to a 1 to become 1046 instead of leaving it as 46.) and $n_2 = 655$. Make sure your n_1 is a four-digit number. Next, compute the $\gcd(n_1, n_2)$ and find integers x and y such that $(n_1)(x) + (n_2)(y) = \gcd(n_1, n_2)$. **(1.0 mark)**

b. Compute $1022^{218} \mod 1147$ using fast exponentiation algorithm discussed in lecture and/or tutorial session. Show all steps. **(1.0 mark)**

c. What is $(BF \times 03)$ performed in $GF(2^8)$? **(1.0 mark)**

Question 2 (3.0 marks)

Using an affine cipher, the plaintext “plus” encrypts to the ciphertext “tlqm”. What are the decryption keys for this cipher?

Question 3 (2.0 marks)

Encryption of large blocks using TEA (or any fixed size block cipher), as you have done for one of the tasks in your assignment, can be achieved through the means of modes. We consider a Cipher-Block Chaining Mode (CBC mode) for a

block cipher which implements the encryption as $C_i = E(k, N_i \oplus C_{i-1})$ for $i > 0$ where $M_1, M_2, M_3, \ldots$ are the messages and C_0 is a randomly chosen initial vector.

i. Explain how decryption is done and give the mathematical expression for the decryption. **(1.0 mark)**

ii. Given the plaintext 101101000110011, the key $K = [1, 0, 1]$ and $IV = [0, 0, 0]$, generate the five 3-bit blocks of the corresponding ciphertext. **(1.0 marks)**

Question 4 (2.0 marks)

i. Consider the RSA algorithm where $p = 7$, $q = 31$, and $e = 13$. You receive the ciphertext $c = 106$. Find the plaintext or message m. **(1.0 mark)**

ii. RSA is insecure against chosen ciphertext attack. Explain or show by example that RSA is insecure against chosen ciphertext attack. **(1.0 mark)**

Question 5 (2.0 marks)

Alice has a superincreasing knapsack $a = (1, 3, 6, 13, 25, 51)$. She also chooses the modulo $p = 109$ and a multiplier $w = 9$.

i. What is Alice public key?

ii. If Bob sends Alice a message $c = 78$. Alice decrypts this message. What does Alice get? (Note: You can leave the decrypted messages as a series of 0's and 1's.)

Question 6 (3.0 marks)

A secret value s in Z_7^* is shared among 5 parties using Shamir's secret sharing modulo 11 so that any 2 shares are necessary and sufficient to reconstruct it. The share of Alice, the first party, is $y_1 = 4$. The share of Daniel, the fourth party, is $y_4 = 7$.

i. What is the secret? **(2.0 marks)**

ii. What is the share y_2 of Bob, the second party? Show your works. **(1.0 mark)**