CSCI361-2025S1-ClassTest-v2

Question 1

Compute the following by demonstrating the step-by-step calculation correctly.

a. Compute $\gcd(830407, 626303)$ and find integers x and y such that $830407x + 626303y = \gcd(830407, 626303)$

b. Compute $1228^{460} \mod 1147$ using fast exponentiation algorithm discussed in lecture and/or tutorial. Show all steps.

c. For any positive integer n, what does Euler's Totient function $\phi(n)$ measure? What is the value of the Euler Phi function $\phi(n)$ if

   i. $n = 181$

   ii. $n = 250$

Question 2 (3.0 marks)

A message was encrypted using Affine transformation cipher. You have the ciphertext, and it is XQHFE. You also happen to know the plaintext starts with a letter C and ends with a letter N; in other words, the plaintext letter C is encrypted to X, and the plaintext letter N is encrypted to E. Decrypt the ciphertext XQHFE. You can assume the Affine cipher used in this encryption uses only 26 alphabetic characters, and the mapping of the alphabets to its numerical equivalent is as follows:

A	B	C	D	E	F	G	H
0	1	2	3	4	5	6	7
N	O	P	Q	R	S	T	U
13	14	15	16	17	18	19	20

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 Feedback Mode (CFB mode) operation for a block cipher which implements the encryption as $C_i = P_i \oplus S_s[E(k, C_{i-1})]$ for $i > 0$ where $P_1, P_2, P_3, \ldots$ are the messages and $C_1, C_2, C_3, \ldots$ are the ciphertext.

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

ii. Given the plaintext 110101001100, the $key = [1, 0, 1], C_0 = [1, 1, 1]$, and the following cipher:

Input	000	001	010	011	100	101	110
Output	101	100	111	110	001	000	011

Perform a 2-bit shift CFB encryption and show the first **three** two-bit streams of output. You may use schematic diagram or table, as shown in lecture slides or tutorial slides, to present your encryption processes. **(1.0 mark)**

Question 4 (2.0 marks)

i. April chooses an RSA modulus $n = 7 \times 19 = 133$. What are the April's private and public keys? **(1.0 mark)**

ii. Adam and Barbie share the same modulus n for RSA to generate their encryption key e_A and e_B. Charlie sends them (Adam and Barbie) the same message m encrypted with e_A and e_B respectively. The resulting ciphertexts are c_A and c_B. Eve intercepts both c and c_B. Show how Eve can use the common modulus attack to compute the plaintext or the message m sent by Charlie? **(1.0 mark)**

Question 5 (2.0 marks)

a. Explain what is a Feistel structure? **(1.0 mark)**

Question 6 (3.0 marks)

To ensure integrity to its documents, an organization wants a minimum of 3 of its 4 appointed managers to sign a document. The organization decides to take 13 as its secret, and all the 4 manager do not know this secret.

i. You have been appointed as the trusted party. Using Shamir Secret Sharing scheme construct the possible secret shares for the managers.

ii. Suppose managers M1, M2, and M4 want to sign a document, they each supply their secret shares. Find the key so that a manager can sign the document.

Question 7

How can Cipher Block Chaining (CBC) mode of operation of DES be used to protect data integrity via a Message Authentication Code (MAC)? Construct a message authentication code (MAC) using the Cipher Block Chaining mode of operation of DES. **(5.0 marks)**