Q1a Complete the following Truth Table: F denotes false and T denotes True

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| A | B | C=A or B | D= A xor B | E= A and B |
| F | F |  |  |  |
| F | T |  |  |  |
| T | T |  |  |  |
| T | F |  |  |  |

Q1b In the following Θ denotes one of the following operators: ’or’, ‘xor’ or ‘and’.

Input1 Θ input2 = Result where, input1, 2 are ‘A’ and ‘B’ and Result is one of C, D, or E.

which operation will yield

input1(2) Θ result = input 2(1)

Q2 Using the English alphabet (i.e., mod 26 arithmetic) let plaintext = {p1, p2,… , pn} and corresponding ciphertext = {c1, c2,… , cn}.

Suppose the encryption function is ci = pi + 10 (mod 26). You receive the ciphertext message EWEM SC K QBOKD CMRYYV

What is the decryption function, and the decrypted/recovered plaintext? What type of cipher is this? Show your calculations.

Q3 You are Alice. You have agreed with your friend Bob that you will use the Diffie-Hellman public-key algorithm to exchange secret keys. You and Bob have agreed to use the public base g = 3 and public modulus p = 809.

You have secretly picked the value SA = 17. You begin the session by sending Bob your calculated value of TA. Bob responds by sending you the value TB = 291.

What is the value of your shared secret key? Can you guess Bob’s secret value SB and what it would be? Show steps of your calculations

Q4 Bob believes that he has come up with a nifty hash function. He assigns a numeric value VChar to each letter in the alphabet equal to the letter’s position in the alphabet, i.e., VA = 1, VB = 2, …, VZ = 26. For a message, he calculates the hash value H = (VChar 1 x VChar 2 x VChar 3 …x VChar N) mod(26).

Bob uses this function to send a one-word message, **REGAL**, to his banker Bill, along with his calculated hash value for the message. Alice is able to intercept the message, and generates an alternative message that has a hash value that collides with Bob’s original hash value.

Give definition and properties of the hash function.

Show a message that Alice may have used to spoof Bob’s message, and demonstrate that its hash value collides with Bob’s original hash.

Q5 Consider the following plaintext message: **THE SIXTEENTH PRESIDENT WAS ABRAHAM LINCOLN.**

* 1. (3 pts) If this message is sent unencrypted and successfully received, what is its entropy? And why?
  2. (3 pts) If this message is encrypted with DES using a random 56-bit key, what is the encrypted message’s entropy? And why