Offline Quiz for Advance Security 1

Instruction: Duration 2hrs

Total Marks: 50 Marks

Submission: All submissions should be uploaded before 11:00 AM.

Answer ALL questions.

1 In relation to Feistel Cipher, write a summary of what you have learned in this area no more than one page.

(12 Marks)

2 Using the Hill Cipher, perform the encryption and decryption without using online tools and mention each step details.

PlainText = cashisneeded

$$K = \begin{bmatrix} 17 & 17 & 5 \\ 21 & 18 & 21 \\ 2 & 2 & 19 \end{bmatrix}$$

$$K^{-1} = \begin{bmatrix} 4 & 9 & 15 \\ 15 & 17 & 6 \\ 24 & 0 & 17 \end{bmatrix}$$

(14 Marks)

3 Determine the GCD using the Euclidean algorithm without using online tools and mention each step details.

i) a = 72345, b= 43215
ii) a= 10292, b= 3486

(12 Marks)

4 Consider an online banking system in which users provide an account number and password to access the bank account and transfer money online. Mention example of CIA (confidentiality, integrity, and availability) requirements associated with the system. Also discuss the level of importance (low, medium high) of each requirement on the system.

.

(12 Marks)