

BCA 171502

Roll No. of candidate

--	--	--	--	--	--	--	--	--	--

W/3/2021

BINA CHOWDHURY CENTRAL LIBRARY  
(GIMT & GIPS)  
Azara, Hatkhowapara,  
Guwahati - 781017

B.C.A. 5<sup>th</sup> Semester End-Term Examination  
NETWORK SECURITY AND CRYPTOGRAPHY  
(New Regulation)

Full Marks – 70

Time – Three hours

The figures in the margin indicate full marks  
for the questions.

Answer question No. 1 and any *four* from the rest.

1. Answer the following questions : (10 × 1 = 10)
- (i) In cryptography, what is cipher?
- (a) algorithm for performing encryption and decryption
  - (b) encrypted message
  - (c) both algorithm for performing encryption and decryption and encrypted message
  - (d) decrypted message
- (ii) In asymmetric key cryptography, the private key is kept by
- (a) sender
  - (b) receiver
  - (c) sender and receiver
  - (d) all the connected devices to the network
- (iii) In cryptography, the order of the letters in a message is rearranged by \_\_\_\_\_
- (a) transposition ciphers
  - (b) substitution ciphers
  - (c) both transposition ciphers and substitution ciphers
  - (d) quadratic ciphers

[Turn over

- (iv) Cryptanalysis is used —————
- (a) to find some insecurity in a cryptographic scheme
  - (b) to increase the speed
  - (c) to encrypt the data
  - (d) to make new ciphers
- (v) Caesar Cipher is an example of
- (a) Poly-alphabetic Cipher
  - (b) Mono alphabetic Cipher
  - (c) Multi alphabetic Cipher
  - (d) Bi-alphabetic Cipher
- (vi) Monoalphabetic ciphers are stronger than Polyalphabetic ciphers because frequency analysis is tougher on the former
- (a) True
  - (b) False
- (vii) Which of the following is a Passive Attack?
- (a) Masquerade
  - (b) Replay
  - (c) Denial of Service (DoS)
  - (d) Traffic Analysis
- (viii) Which of the following is a component of cryptography?
- (a) Cipher text
  - (b) Cipher
  - (c) Key
  - (d) All of these
- (ix) Which of the following is a Monoalphabetic cipher?
- (a) Caesar cipher
  - (b) Autokey cipher
  - (c) Vigenere cipher
  - (d) All of these
- (x) In the Polyalphabetic cipher, the character in plaintext have a ————— relationship with the character in cipher text
- (a) One-to-One
  - (b) One-to-Many
  - (c) Many-to-One
  - (d) Many-to-Many

DINA GHOWDHURY CENTRAL LIBRARY  
(GIMT & GIPS)  
Azara, Hatkhowapara,  
Guwahati -781017

2. Answer the following questions

- (a) What is die need for network security? Explain its goals. (2+6=8)
- (b) Explain snooping and traffic analysis in terms of Threat to Confidentiality. (2 × 2 =4)
- (c) What are the different types of network security devices? Explain. (3)

3. Answer the following questions"

- (a) What is a firewall? What are the types of firewalls? (4)
- (b) Define the following terms with suitable example. (5 × 1 = 5)
- (i) Plaintext
  - (ii) Cipher text
  - (iii) Encryption
  - (iv) Decryption
  - (v) Cipher.
- (c) Explain Vernam Cipher Encryption and Decryption process considering plaintext as "HELLO" and Key as "GIMTG". (6)

BINA CHOWDHURY CENTRAL LIBRARY  
(GIMT & GIPS)  
Azara, Hatkhowapara,  
Guwahati - 781017

4. Answer the following questions :

- (a) Explain the different network security attack in terms of Threat to Integrity. (4)
- (b) Define a network security attack? Explain passive attacks and active attacks. (2+4=6)
- (c) Differentiate between Symmetric-Key and Asymmetric-Key Cryptography. (5)

5. Answer the following questions

- (a) Explain the encryption and Decryption process of Hill Cipher considering plaintext "ATTACK" and key is  $\begin{bmatrix} 2 & 3 \\ 3 & 6 \end{bmatrix}$ . (2 × 4 = 8)
- (b) What is the relationship between security services and security mechanism? (7)

6. Answer the following questions

- (a) What is Caesar Cipher? Show the encryption and decryption technique of Caesar Cipher taking the plaintext as 'zoo' and key is 3. (2+3+3=8)
- (b) Explain various network security services. (7)

7. Answer the following questions

- (a) Write the Algorithm of Playfair Cipher. (3)
- (b) Considering the plaintext as "GOOD MORNING" and Key is "GIMT". Explain the Encryption and Decryption Technique using PlayFair Symmetric Encryption Technique. (2 × 4 = 8)
- (c) Write a short note on Vigenere Cipher. (4)