

GYANMANJARI INNOVATIVE UNIVERSITY

Gyanmanjari Diploma Engineering College

Diploma Engineering- End Semester Examination (ESE)-Winter-2025

Enrollment No.: _____

Date: 03/12/2025

Subject Code: DETIT15214

Semester: 5

Subject Name: Cryptography and Network Security

Total Marks: 100

Time: 10:30AM To 01:30PM

Instructions:

1. Question No. 1 is Compulsory.
2. Make Suitable Assumptions wherever necessary.
3. Figures to the right indicate full marks.

| | Marks |
|---|-------|
| Q.1 (a) What is cryptography? Explain network security. ક્રિપ્ટોગ્રાફી એટલે શું? નેટવર્ક સિક્યુરિટીની સમજ આપો. | 05 |
| (b) What is Modular Arithmetic? Explain the concept with a simple example. મોડ્યુલર એથમેટિક (Modular Arithmetic) શેને કહે છે? સરળ ઉદાહરણ સાથે તેના ખ્યાલને સમજાવો. | 05 |
| (c) Describe classical encryption techniques : Substitution and Transposition ciphers. Also explain the following with examples: 1. Hill Cipher 2. Caesar Cipher પરંપરાગત એન્ક્રિપ્શન તકનીકો સમજાવો: સબ્સ્ટિટ્યુશન અને ટ્રાન્સપોઝિશન સાઇફર્સ. નીચેના સાઇફર્સને ઉદાહરણ સાથે સમજાવો: 1. હિલ સાઇફર (Hill Cipher) 2. સીઝર સાઇફર (Caesar Cipher) | 10 |
| Q.2 (a) What is GCD (Greatest Common Divisor)? Define it with a simple explanation and example. GCD (મહત્તમ સામાન્ય વિભાજક) શું છે? તેને સરળ શબ્દોમાં વ્યાખ્યાયિત કરો અને ઉદાહરણ સાથે સમજાવો. | 05 |
| (b) Discuss Meet-in-the-Middle Attack. મીટ-ઇન-દ-મિડલ હુમલો સમજાવો. | 05 |
| OR | |
| (b) List any three block cipher modes of operation. બ્લોક સાઇફરના કોઈપણ ત્રણ મોડ ઓફ ઓપરેશન યાદ કરો. | 05 |
| (c) What is the Playfair Cipher? Explain its encryption technique with rules and a suitable example. પ્લેફેર સાઇફર (Playfair Cipher) શું છે? તેનો એન્ક્રિપ્શન તંત્ર સમજાવો, તેના નિયમો અને યોગ્ય ઉદાહરણ સાથે સમજ આપો. | 10 |
| OR | |
| (c) What is Euler's Theorem in number theory? Explain it and solve one example step by step. નંબર થિયરીમાં યૂલરનું સિદ્ધાંત (Euler's Theorem) શું છે? તે સમજાવો અને એક ઉદાહરણ સાથે પગલાંવાર ઉકેલ આપો. | 10 |
| Q.3 (a) Describe the structure and working of block ciphers in detail. બ્લોક સાઇફરની રચના અને કાર્ય વિગતો સાથે સમજાવો. | 05 |

- (b) Compare symmetric and asymmetric cryptography. સમમિત અને અસમમિત ક્રિપ્ટોગ્રાફી વચ્ચે તફાવત સમજાવો. 05
- (c) Write a short note on Data Encryption Standard (DES). ડેટા એન્ક્રિપ્શન સ્ટાન્ડર્ડ (DES) વિષે ટૂંકી નોંધ લખો. 10

OR

- (a) What is public-key cryptography? પબ્લિક-કી ક્રિપ્ટોગ્રાફી શું છે? 05
- (b) Describe the working and security features of public-key cryptography. પબ્લિક-કી ક્રિપ્ટોગ્રાફીનું કાર્ય અને સુરક્ષા લક્ષણો સમજાવો. 05
- (c) Describe the AES algorithm with key features and structure. AES એલ્ગોરિધમની રચના અને મુખ્ય લક્ષણો સમજાવો. 10
- Q.4 (a) What is network security. Why is it important? નેટવર્ક સુરક્ષા શું છે? તે કેમ મહત્વપૂર્ણ છે? 05
- (b) Explain Viruses and its Types. વાયરસ અને તેના પ્રકારો સમજાવો. 05
- (c) What is the Diffie-Hellman key exchange? ડિફી-હેલમેન કી એક્સચેન્જ શું છે? 10

OR

- (a) What is Trojan? Explain How its work. ટ્રોજન શું છે? તે કેવી રીતે કાર્ય કરે છે? 05
- (b) What is penetration testing? પેનેટ્રેશન ટેસ્ટિંગ શું છે? 05
- (c) Write the steps involved in key generation for RSA. RSA માટે કી જનરેશનના પગલાં લખો. 10
- Q.5 (a) Compare and contrast Fermat's Little Theorem and Euler's Theorem. Explain their differences and applications in cryptography. ફર્મેટનું લિટલ થિયોરમ અને યૂલરનું થિયોરમ વચ્ચે તફાવત શું છે? બંનેની તુલના કરો અને ક્રિપ્ટોગ્રાફી ક્ષેત્રે તેમના ઉપયોગો સમજાવો. 05
- (b) explain diffusion and confusion. ડિફ્યુઝન અને કન્ફ્યુઝન શું છે? સમજાવો. 05
- (c) Explain social engineering attacks with types and prevention. સોશિયલ એન્જિનિયરિંગ હુમલાઓ: પ્રકારો અને બચાવ માર્ગ સમજાવો. 10

OR

- (a) What is SSL? How does it help secure data transmission. SSL શું છે? તે ડેટા ટ્રાન્સમિશન કેવી રીતે સુરક્ષિત બનાવે છે? 05
- (b) Differentiate between virus and worm. વાયરસ અને વર્મ વચ્ચેનો તફાવત સમજાવો. 05
- (c) Explain the concept of DoS and DDoS with example. DoS અને DDoS નો અર્થ શું છે? ઉદાહરણ આપો. 10