GYANMANJARI INNOVATIVE UNIVERSITY

GYANMANJARI DIPLOMA ENGINEERING COLLEGE

Diploma Engineering –Mid Semester Examination (MSE)-W2025

Enrollment No.:_____

Subject Code: DETIT15214 **Date: 10/09/2025**

Subject Name: Cryptography and Network Security **Semester: 5**

Time: 11:00 AM to 1:00 PM **Total Marks: 60**

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)	Explain the main security goals in network security. નેટવર્ક સિક્યુરિટીમાં મુખ્ય સુરક્ષા લક્ષ્યો (Security Goals) શું છે? તેની સમજ આપો.	05
	(b)	Differentiate active attack and passive attack. એક્ટિવ એટેક અને પેસિવ એટેક વચ્ચે તફાવત આપો.	05
	(c)	Explain the working of the DES algorithm with a block diagram. બ્લોક ડાયગ્રામ સાથે DES એલ્ગોરિધમનું કાર્ય સમજાવો.	10
Q.2	(a)	Explain the Euclidean Algorithm. How is it used to find the GCD of two numbers? Show all steps with an example. યૂક્લિડિયન એલ્ગોરિધમ શું છે? તેને કેવી રીતે બે સંખ્યાઓના GCD (મહત્તમ સામાન્ય વિભાજક) શોધવા માટે ઉપયોગમાં લેવામાં આવે છે? તમામ પગલાં ઉદાહરણ સાથે સમજાવો.	05
	(b)	Give difference between stream cipher and block cipher? સ્ટ્રીમ સાઇફર અને બ્લોક સાઇફર વચ્ચેનો તફાવત આપો.	05
		OR	
	(b)	State Fermat's Little Theorem. Explain it with a suitable numerical example. ફર્મેટનું લિટલ થિયોરમ (Fermat's Little Theorem) શું છે? તેને યોગ્ય સંખ્યાત્મક ઉદાહરણ સાથે સમજાવો.	05
	(c)	Encrypt a given plaintext using playfair cipher. Plaintext: INSTRUMENT and Keyword: MONARCHY આપેલા પ્લેઇનટેક્સ્ટને Playfair Cipher વડે એન્ક્રિપ્ટ કરો. Plaintext: INSTRUMENT and Keyword: MONARCHY	10
		OR	
	(c)	Describe the AES algorithm with key features and structure. AES એલ્ગોરિધમની રચના અને મુખ્ય લક્ષણો સમજાવો.	10
Q.3	(a)	Discuss Men-in-the-Middle Attack. મેન -ઈન-ધ-મિડલ હુમલો સમજાવો.	05
	(b)	Discuss the advantages and working of Elliptic Curve Cryptography (ECC). એલિપ્ટિક કર્વ ક્રિપ્ટોગ્રાફી (ECC) ના લાભો અને કાર્ય સમજાવો.	05
	(c)	Explain the RSA algorithm with key generation, encryption, and decryption example. RSA એલ્ગોરિધમને કી જનરેશન, એન્ક્રિપ્શન અને ડિક્રિપ્શનના ઉદાહરણ સાથે સમજાવો.	10

OR

Q.3 (a) Describe Diffie-Hellman key exchange protocol with a neat example. 05
ડિફી-હેલમેન કી એક્સચેન્જ પ્રોટોકોલને ઉદાહરણ સાથે સમજાવો.

(b) Enlist block cipher modes and explain any two. 05
બ્લોક સાઇફર મોડ્સ ની યાદી બનાવો અને કોઇ પણ બે સમજાવો.

(c) Explain digital signature algorithm with its applications. 10
ડિજિટલ Signature એલ્ગોરિધમ અને તેના ઉપયોગો સમજાવો.