Total number of printed pages: **Programme(UG)/Semester VII/UECE713C**

2024

Cryptography and Network Security

Full Marks: 100

Time: Three hours

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

*Answer **any five** questions.*

1.	a)	Name some traditional ciphers used. Describe the working of any one of them. What do you mean by substitution and transposition techniques.	2+3+3= 8
	b)	What is Message Authentication Code (MAC)? Describe with the help of relevant diagram how MAC is used to achieve i) confidentiality only and ii) authentication only.	2+6=8
	c)	What do you mean by cryptography and cryptanalysis?	4
2.	a)	Name the various passive and active attacks. Explain the passive attacks.	8
	b)	Describe a model of digital signature process. Explain two possible digital signature schemes using cryptographic hash function.	3+6=9
	c)	Define confusion and diffusion factors in cryptography.	3
3.	a)	What is secure socket layer (SSL)? Explain the SSL record protocol operation?	2+7=9
	b)	Encrypt the following text using playfair cipher with	5

		the key “gold”- “meet me after dark”.	
	c)	What is double DES? Explain. Mention any weakness of this technique.	6
4.	a)	What is public key cryptography? Describe how does public key cryptography provide both authentication and confidentiality.	2+5=7
	b)	Describe the key generation process in RC4 algorithm.	6
	c)	Describe RSA algorithm.	7
5.	a)	Explain with diagram one single round of DES.	6
	b)	What are the design criteria of S-boxes?	6
	c)	What is PGP? Describe how does PGP provide i) confidentiality only and ii) authentication only?	2+6=8
6.	a)	Perform encryption and decryption using RSA algorithm for p=5, q=7, e=7, M=12.	5
	b)	Draw a neat diagram of Fiestel Cipher.	5
	c)	Describe triple DES using three keys.	5
	d)	What is IP security (IPSec)? What are its various services?	5
7.	a)	Describe symmetric encryption with the help of relevant diagram.	5
	b)	Encrypt the text “defend the east wall” using rail-fence transposition technique with key 3.	5
	c)	What is the weakness of DES?	3
	d)	Explain the SSL specific protocols.	7