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

2022

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)	What is Message Authentication Code (MAC)? Describe how MAC is used to achieve i) confidentiality only and ii) authentication only.	2+6=8
	b)	Differentiate MAC from a cryptographic hash function.	2
	c)	Describe a model of digital signature process. Explain two possible digital signature schemes using cryptographic hash function.	3+7=10
2.	a)	What is IP security (IPSec)? What are its various services? Describe the transport mode of IPSec?	2+3+3=8
	b)	What is PGP? Describe how does PGP provide i) confidentiality only and ii) authentication only?	2+7=9
	c)	What is replay attack? How can it be dealt with?	3
3.	a)	What is public key cryptography? What are its application areas?	5
	b)	Describe how does public key cryptography provide both authentication and confidentiality.	6
	c)	What is secure socket layer (SSL)? Explain the SSL record protocol operation?	9
4.	a)	What are the design criteria of S-boxes?	5
	b)	Explain the functions provided by S/MIME?	6
	c)	What is man-in-the-middle attack taking place in	6

		double DES?	
	d)	Describe triple DES using two keys.	3
5.	a)	Describe the key generation process in RC4 algorithm.	6
	b)	Describe RSA algorithm.	7
	c)	Explain with diagram one single round of DES.	7
6.	a)	Perform encryption and decryption using RSA algorithm for p=5, q=31, e=13, M=5.	5
	b)	Using two-stage columnar transposition technique and key 4312567, encrypt "attack postponed until dawn".	5
	c)	What is the weakness of DES?	3
	d)	Explain the SSL specific protocols.	7
7.		Write short notes on -i) Authentication header (IPSec), ii) Denial of service), iii) Security services as defined in X.800, iv) Security approaches of web traffic.	5*4=20