Total number of printed pages: 02

UG/VII Semester /UECE713C

2023

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 are the different block cipher modes of operations? What are their typical applications?	5
	b)	Explain output feedback mode of operation. What are its advantages and disadvantages?	6+3=9
	c)	What is the meet-in-the-middle attack that happens in double DES?	6
2.	a)	Explain the steps of RSA algorithm.	6
	b)	Perform encryption and decryption using RSA algorithm for the following: p=5, q=31, e=13, M=5.	5
	c)	What is public key cryptography? How does it provide both authentication and confidentiality?	2+4=6
	d)	What is a replay attack? How can it be dealt with?	3
3.	a)	What are the web security challenges? Name some web traffic security approaches.	5
	b)	What is secure socket layer (SSL)? Explain the SSL record protocol operation.	2+6=8
	c)	What is PGP? How does it provide both authentication and confidentiality?	2+5=7
4.	a)	Describe Diffie-Hellman key exchange algorithm.	5
	b)	What is the purpose of the S-boxes in DES? What are their design criteria?	2+6=8
	c)	Explain the various SSL specific protocols.	7
5.	a)	What is a digital signature? What are its requirements?	6
	b)	Explain two possible digital signature schemes using cryptographic hash function	7

	c)	Establish the fact that "at every round the intermediate value of decryption process is equal to the corresponding value of the encryption process with the two halves being swapped" for Feistel cipher.	7
6.	a)	What is a message authentication code (MAC)? Differentiate between a cryptographic hash function and a MAC.	5
	b)	What do you mean by message integrity? How does MAC ensure authentication?	7
	c)	What is IPSec? What are the services it provides? Explain the transport mode of IPSec.	8
7.		Write short notes on -i) OSI security architecture, ii) Counter mode, iii) One-time pad, iv) Encapsulating security payload.	5*4=20

*****