Total number of printed pages: **Programme(~~D~~/UG/~~PG~~)/7th / UCSE714(Back)**

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)	Explain substitution, transposition cipher and product cipher.	5
	b)	What is the difference between symmetric key encryption and asymmetric key encryption?	5
	c)	What are the four basic principles related to the security of a particular message? Explain each principle with proper example.	5
	d)	Describe a single round of DES with block diagram.	5
2.	a)	Describe Diffie-Hellman Symmetric Key Exchange algorithm.	5
	b)	Explain how this process might become vulnerable.	5
	c)	How is SHTTP different from SSL?	5
	d)	What protocols contain in SSL? Explain the security handshake pitfalls.	5
3.	a)	What services are provided by IPSec?	5
	b)	What is electronic money?	5
	c)	What is SET? Explain with a suitable model.	5
	d)	What is WEP?	5
4.	a)	Explain RSA algorithm with example.In the public-key system using RSA, you intercept the cipher text CT=10 sent to a user whose public key is E=5, N=35. What is the plain text PT?	10
	b)	How SHA-1 is differing from MD5?	5

	c)	Why do you use digital signature? What are digital certificates?	5
5.	a)	Write short notes on the following. a) PGP b) S/MIME c) PEM	3X5
	b)	What is the difference between MAC and message digest?	5
6.	a)	What are the disadvantages of a Screened host Firewall, single-homed bastion?	5
	b)	"The digital envelope technique combines the best features of both symmetric and asymmetric key cryptography" – Justify this statement.	5
	c)	What are the three main actions of a packet filter?	5
	d)	What are the limitations of a firewall?	5