Total number of printed pages: 01

Programme (PG)/3rd/ PCSE311

2023

Advanced Cryptography and Net. 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 four basic principles related to the security of a particular message? Explain each principle with proper example.	5
	b)	What is the difference between symmetric key encryption and asymmetric key encryption?	5
	c)	Describe a single round of DES with block diagram.	10
2	a)	Show that AES decryption is the inverse of AES encryption.	10
	b)	Explain RSA algorithm with example.	10
3	a)	Describe Diffie-Hellman Symmetric Key Exchange algorithm with an example.	10
	b)	Explain with example how this process might become vulnerable.	10
4	a)	How SHA-1 is differing from MD5?	5
	b)	Why do you use digital signature? What are digital certificates?	3+2=5
	c)	What is SET? Explain with a suitable model.	10
5	a)	What are the services provided by IPSec ?	4
	b)	Briefly describe IPSec Architecture ?	8
	c)	What are the different protocols associated with SSL ?	4
	d)	How is SHTTP different from SSL ?	4
6	a)	What is firewall?	5
	b)	What are different types of firewall? Briefly explain working principle of each.	5
	c)	What are the limitations of firewall?	5
	d)	What are thc differences between authentication and authorization?	5