23ITU526N

PSG COLLEGE OF ARTS & SCIENCE
(AUTONOMOUS)

BSc DEGREE EXAMINATION MAY 2026
(Fifth Semester)

Branch - **INFORMATION TECHNOLOGY**

CRYPTOGRAPHY

Time: Three Hours Maximum: 75 Marks

SECTION-A (10 Marks)
Answer **ALL** questions
ALL questions carry **EQUAL** marks (10 × 1 = 10)

Module No.	Question No.	Question	K Level	CO
1	1	In cryptography, the order of the letters in a message is rearranged by a) transpositional ciphers b) substitution ciphers c) both transpositional ciphers and substitution ciphers d) quadratic ciphers	K1	CO1
	2	In asymmetric key cryptography, the private key is kept by a) sender b) receiver c) sender and receiver d) all the connected devices to the network	K2	CO1
2	3	What is the key size used in the DES algorithm? a) 128 bits b) 56 bits c) 64 bits d) 16 bits	K1	CO2
	4	Which of the following is a valid key size for AES? a) 128, 192, or 256 bits b) 64 or 128 bits c) 128 or 256 bits d) Only 256 bits	K2	CO2
3	5	_____ is a message-digest algorithm. a) DES b) RSA c) IDEA d) MD5	K1	CO3
	6	A digital certificate binds a user with a) the user's public key b) the user's private key c) the user's driving license d) the user's passport	K2	CO3
4	7	PEM allows for _____ security options when sending an email message. a) one b) two c) three d) four	K1	CO4
	8	Biometric devices are based on a) passwords b) PINs c) smart cards d) human characteristics	K2	CO4
5	9	What is the primary role of a firewall? a) To speed up network connections b) To encrypt data for secure communication c) To prevent unauthorized access by filtering network traffic d) To detect viruses and malware on a network	K1	CO5
	10	What does "VPN" stand for? a) Virtual Protocol Network b) Visual Private Network c) Virtual Private Network d) Virtual Protocol Networking	K2	CO5

Cont...

SECTION - B (35 Marks)

Answer **ALL** questions

ALL questions carry **EQUAL** Marks (5 × 7 = 35)

Module No.	Question No.	Question	K Level	CO
1	11.a.	Outline the categories of viruses.	K2	CO1
		(OR)		
	11.b.	Explain about vernam cipher.		
2	12.a.	Construct the details of one round in DES.	K3	CO2
		(OR)		
	12.b.	Identify the key advantages and disadvantages of the algorithm modes.		
3	13.a.	Build the working of MD5.	K3	CO3
		(OR)		
	13.b.	Organize the contents of a digital certificate.		
4	14.a.	Distinguish SSL versus SET.	K4	CO4
		(OR)		
	14.b.	Analyze the two categories of biometric techniques.		
5	15.a.	Categorize the three possible configurations of firewalls.	K4	CO5
		(OR)		
	15.b.	Briefly discuss about the audit records.		

SECTION -C (30 Marks)

Answer **ANY THREE** questions

ALL questions carry **EQUAL** Marks (3 × 10 = 30)

Module No.	Question No.	Question	K Level	CO
1	16	Analyze Diffie-Hellman key exchange algorithm.	K4	CO1
2	17	Classify the advanced encryption standard.	K4	CO2
3	18	Examine the RSA algorithm.	K4	CO3
4	19	Analyze the working of privacy enhanced mail.	K4	CO4
5	20	Classify the TCP segment format.	K4	CO5

Z-Z-Z END