TOTAL PAGES: 2

23ITU526N

PSG COLLEGE OF ARTS & SCIENCE
(AUTONOMOUS)

BSc DEGREE EXAMINATION DECEMBER 2025
(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	Cryptanalysis is used to _____ a) find some insecurity in a cryptographic scheme b) increase the speed c) encrypt the data d) make new ciphers	K1	1
	2	Rail fence technique is an example of _____ a) mono-alphabetic cipher b) poly-alphabetic cipher c) transposition cipher d) additive cipher	K2	1
2	3	How many rounds does the DES algorithm perform? a) 8 b) 16 c) 32 d) 64	K1	2
	4	In AES the 4×4 bytes matrix key is transformed into a keys of size a) 32 words b) 64 words c) 54 words d) 44 words	K2	2
3	5	In the RSA algorithm, select 2 random large values 'p' and 'q'. Which of the following is the property of 'p' and 'q'? a) p and q should be divisible by Φ(n) b) p and q should be co-prime c) p and q should be prime d) p/q should give no remainder	K1	3
	6	The ____ standard defines the structure of a digital certificate. a)X.500 b) TCP/IP c) X.509 d) ASN.1	K2	3
4	7	_____ in SSL is optional. a) Client authentication b) Server authentication c) Application authentication d) Database authentication	K1	4
	8	Determining the identity of a user is called _____. a) authorization b) access control c) confidentiality d) authentication	K2	4
5	9	A packet filter firewall filters at _____. a) Physical layer b) Data link layer c) Network layer or Transport layer d) Application layer	K1	5
	10	IPSec protocol is used to apply security at the ____ a) Network layer b) Session layer c) Application layer d) Transport layer	K2	5

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 types of criminal attacks.	K2	1
		(OR)		
	11.b.	Explain about the simple columnar transposition technique.		
2	12.a.	Organize the algorithm modes in brief.	K3	2
		(OR)		
	12.b.	Construct the details of one round in IDEA.		
3	13.a.	Organize the requirements of the message digest concept.	K3	3
		(OR)		
	13.b.	Build the steps for creation of a digital certificate.		
4	14.a.	Distinguish between SSL and TLS.	K4	4
		(OR)		
	14.b.	Classify the challenge/response authentication tokens.		
5	15.a.	Briefly discuss the header fields inside a TCP segment.	K4	5
		(OR)		
	15.b.	Examine the virtual private networks architecture.		

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 the playfair cipher.	K4	1
2	17	Classify the broad level steps in DES.	K4	2
3	18	Examine the password based encryption standard.	K4	3
4	19	Analyze the handshake protocol.	K4	4
5	20	Categorize the two types of firewalls.	K4	5

Z-Z-Z END