CBCS SCHEME

USN | | | | | | | | | |

BIS703

Seventh Semester B.E./B.Tech. Degree Examination, Dec.2025/Jan.2026
Information and Network Security

Time: 3 hrs. Max. Marks: 100

Note: 1. Answer any FIVE full questions, choosing ONE full question from each module.
2. M : Marks , L: Bloom's level , C: Course outcomes.

		Module – 1	M	L	C
Q.1	a.	Explain the basic terminology of crypto along with its black box.	4	L2	CO1
	b.	Explain simple substitution cipher with an example.	8	L3	CO1
	c.	Discuss double transposition cipher with an example.	8	L3	CO1
		OR			
Q.2	a.	Explain modern crypto history.	6	L2	CO1
	b.	Describe the Taxonomy of cryptography.	7	L2	CO1
	c.	Describe the Taxonomy of cryptanalysis.	7	L2	CO1
		Module – 2			
Q.3	a.	Discuss the requirements of a cryptographic hash function.	6	L2	CO2
	b.	Explain Cryptographic Tiger Hash Algorithm.	10	L3	CO2
	c.	Explain the uses of a hash function.	4	L2	CO2
		OR			
Q.4	a.	Define secret sharing. Explain the concept of secret sharing using key escrow.	10	L3	CO2
	b.	Discuss the usage of random numbers with unpredictability.	6	L2	CO2
	c.	Explain the categorization of water marks.	4	L2	CO2
		Module – 3			
Q.5	a.	Define Randomness. Differentiate between deterministic and non-deterministic generators.	10	L2	CO3
	b.	Explain the freshness mechanism in detail.	10	L2	CO3
		OR			
Q.6	a.	Explain the problems related to passwords.	4	L2	CO3
	b.	Describe the dynamic password schemes based on challenge - response.	8	L2	CO3
	c.	Explain the Diffie-Hellman key agreement protocol.	8	L2	CO3

Module – 4					
Q.7	a.	Explain the key life cycle with a neat diagram.	4	L2	CO4
	b.	Discuss key distribution approaches to acquiring shared keys from a KC.	10	L2	CO4
	c.	Explain the key storage risk factor.	6	L2	CO4
OR					
Q.8	a.	Explain the fields of X.509 version 3 public-key certificate.	8	L2	CO4
	b.	Explain the public-key certificate management models.	12	L2	CO4
Module – 5					
Q.9	a.	Explain simple SSL hand shake protocol.	10	L2	CO5
	b.	Discuss the SSL key management in detail.	10	L2	CO5
OR					
Q.10	a.	Discuss WLAN design issues.	5	L2	CO5
	b.	Explain GSM and UMTS key management.	10	L2	CO5
	c.	Discuss the usage of cryptography in video broadcasting.	5	L2	CO5

* * * * *