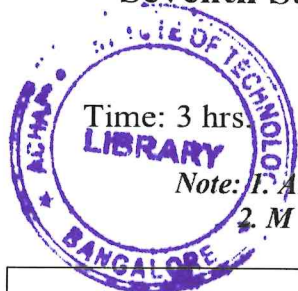


Seventh Semester B.E./B.Tech. Degree Examination, June/July 2026

Information and Network Security



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.	Give an introduction to cryptography and explain “How to speak crypto with standard terminology”.	8	L2	CO1
	b.	Explain classic cryptography and describe the simple substitution cipher with an example.	8	L2	CO1
	c.	Explain the cryptanalysis of a simple substitution cypher and define what is meant by a secure cipher.	4	L2	CO1
OR					
Q.2	a.	Explain the Double Transposition Cipher with an example.	8	L2	CO1
	b.	Explain the One – Time Pad and Project VENONA.	6	L2	CO1
	c.	Explain the code book cipher and the ciphers used in the U.S Election of 1876.	6	L2	CO1
Module – 2					
Q.3	a.	What is a Hash function? Explain the properties of a good cryptographic hash function.	8	L2	CO2
	b.	Explain the Birthday problem and its significance in hash function security.	6	L2	CO2
	c.	Differentiate between cryptographic and non – cryptographic hash functions.	6	L2	CO2
OR					
Q.4	a.	Explain the use of hash functions in real – world applications such as : i) Online bidding systems ii) Spam reduction iii) Other crypto – related applications.	8	L2	CO2
	b.	Explain Random number generation and generating random bits.	6	L2	CO2
	c.	Explain information hiding and its importance in cryptography.	6	L2	CO2
Module – 3					
Q.5	a.	Define Providing freshness. Explain the zero knowledge mechanism.	8	L3	CO3
	b.	Explain the fundamentals of entity authentication.	8	L3	CO3

	c.	Write a short note on further reading in authentication mechanism.	4	L3	CO3
OR					
Q.6	a.	Explain the fundamentals of key management in cryptographic systems.	8	L2	CO3
	b.	Analysis a simple cryptographic protocol , identifying attacks.	6	L2	CO3
	c.	Explain Authentication protocols and key establishment protocols with suitable examples.	6	L2	CO3
Module – 4					
Q.7	a.	Explain the basics of cryptographic protocols.	6	L2	CO4
	b.	Explain the processes of key generation , key establishment , key storage and key usage.	8	L2	CO4
	c.	Define Governing Key Management. Explain key management policies and controls.	6	L2	CO4
OR					
Q.8	a.	Describe the certificate lifecycle in detail.	6	L2	CO4
	b.	Explain different public – key management models.	6	L3	CO4
	c.	Discuss alternative approaches to public key management.	8	L3	CO4
Module – 5					
Q.9	a.	Explain the role of cryptography in securing the internet. Describe SSL / TLS and HTTPS.	8	L2	CO5
	b.	Explain how cryptography is used in Wireless Local Area Networks [WLANs].	8	L2	CO5
	c.	Describe the application of cryptography in mobile telecommunications.	4	L2	CO5
OR					
Q.10	a.	Explain the use of cryptography in secure payment card transactions.	6	L3	CO5
	b.	Describe the role of cryptography in video broadcasting systems.	6	L3	CO5
	c.	Explain how cryptography is applied in identity cards. Such as smart card and e – passports.	8	L2	CO5
