Code No: **R1641051** **R16** **Set No. 1**

IV B.Tech I Semester Regular/Supple Examinations, March - 2021

CRYPTOGRAPHY AND NETWORK SECURITY

(Common to Computer Science and Engineering and Information Technology)

Time: 3 hours **Max. Marks: 70**

Question paper consists of Part-A and Part-B
Answer ALL sub questions from Part-A
Answer any FOUR questions from Part-B
****

PART–A *(14 Marks)*

1.	a)	List passive attack from active attack.		[3]
	b)	Write the difference between public key and private key cryptosystem.		[2]
	c)	Mention any one technique of attacking RSA.		[2]
	d)	What are the two approaches of Digital Signature?		[2]
	e)	List the transfer encodings used by S/MIME.		[3]
	f)	Write the applications of IPSec.		[2]

PART–B *(4x14 = 56 Marks)*

2.	a)	Write and discuss the relation between security mechanisms and attacks?		[7]
	b)	Discuss briefly about transposition ciphers		[7]
3.	a)	i.	What are the different modes of operation in DES?	[7]
		ii.	Write down the purpose of S-Boxes in DES?	
	b)	Give the structure of AES. Explain how Encryption/Decryption is done in AES.		[7]
4.	a)	Briefly discuss about Diffie-Hellman Key Exchange algorithm?		[7]
	b)	Is RSA an asymmetric encryption algorithm? Explain with an example.		[7]
5.	a)	Give the structure of CMAC. What is the difference between CMAC and HMAC?		[7]
	b)	Define hash? List the variants in SHA by explaining SHA-1 in detail.		[7]
6.	a)	Explain TLS functions and alert codes of Transport Layer Security.		[7]
	b)	Explain various PGP cryptographic functions and services in detail.		[7]
7.	a)	With a neat sketch explain the IPSec scenario and IPSec Services.		[7]
	b)	Explain IP security architecture and also explain basic combinations of security associations with a neat diagram.		[7]

Code No: **R1641051** **R16** **Set No. 2**

IV B.Tech I Semester Regular/Supple Examinations, March - 2021

CRYPTOGRAPHY AND NETWORK SECURITY

(Common to Computer Science and Engineering and Information Technology)

Time: 3 hours **Max. Marks: 70**

Question paper consists of Part-A and Part-B
Answer ALL sub questions from Part-A
*****

PART–A *(14 Marks)*

1.	a)	Compare the terms attack and threat	[3]
	b)	Write about cipher block chaining mode of operation	[2]
	c)	Mention any one technique of attacking RSA.	[2]
	d)	What is Birthday Attack on Digital Signatures?	[2]
	e)	What are the keys used by PGP?	[2]
	f)	How is replay attack prevented by IPSec?	[3]
	g)		

PART–B *(4x14 = 56 Marks)*

2.	a)	Draw the model for Network Security and show that there are four basic tasks in designing a particular security service.	[7]
	b)	Explain the following mathematical terms and their role in Cryptography i) Prime numbers ii) The Modulus operator iii) The modular inverse	[7]
3.	a)	Mention the strengths and weakness of DES algorithm.	[7]
	b)	Explain in detail the key generation in AES algorithm and its expansion format.	[7]
4.	a)	Explain about Euclidean algorithm for Greatest Common Divisor	[7]
	b)	Describe about public and private keys in ECC system and explain about security of ECC.	[7]
5.	a)	Discuss about the objectives of HMAC and it security features.	[7]
	b)	What is the purpose of digital signature? Explain its properties and requirements.	[7]
6.	a)	What are the environmental shortcomings of Kerberos4? How does Kerberos 5 address them?	[7]
	b)	List and explain the PGP services and explain how PGP message generation is done with a neat diagram	[7]
7.	a)	Explain the scenario of IP security and its Policy	[7]
	b)	Elaborate the below i) Classes of Intruders ii) Intruders Behavior Pattern iii) Intrusion Techniques	[7]

Code No: **R1641051** **R16** **Set No. 3**

IV B.Tech I Semester Regular/Supple Examinations, March - 2021

CRYPTOGRAPHY AND NETWORK SECURITY

(Common to Computer Science and Engineering and Information Technology)

Time: 3 hours **Max. Marks: 70**

Question paper consists of Part-A and Part-B
Answer ALL sub questions from Part-A
Answer any FOUR questions from Part-B
*****

PART–A *(14 Marks)*

1.	a)	Define the key words i) Confidentiality ii) Integrity	[2]
	b)	Distinguish between diffusion and confusion.	[3]
	c)	Discuss the design principles of block cipher technique?	[2]
	d)	List out the advantages of RC4 algorithm.	[2]
	e)	List the transfer encodings used by S/MIME.	[3]
	f)	What services are provided by IPSec?	[2]

PART–B *(4x14 = 56 Marks)*

2.	a)	List and explain the security mechanisms defined by X.800	[7]
	b)	Justify that substitution and transposition techniques are two basic blocks for all encryption techniques with one example to each?	[7]
3.	a)	Explain the generation of sub keys and S Box from the given 32-bit key in Blowfish algorithm.	[7]
	b)	Explain in detail the key generation in AES algorithm and its expansion format.	[7]
4.	a)	Illustrate ElGamal Encryption and decryption algorithm	[7]
	b)	Perform decryption and encryption using RSA algorithm with p=3, q=11, e=7 and N=5.	[7]
5.	a)	Compare the Features of SHA-1 and MD5 algorithm.	[7]
	b)	How man in middle attack can be performed in Diffie Hellman algorithm.	[7]
6.	a)	Explain the four protocols defined by Secure Socket Layer	[7]
	b)	Discuss the following with respect to PGP: (i) Cryptographic algorithms used by PGP (ii) Compression in PGP	[7]
7.	a)	Explain IP security architecture and also explain basic combinations of security associations with a neat diagram.	[7]
	b)	What are the different types of viruses? How do they get into the systems?	[7]

Code No: **R1641051** **R16** **Set No. 4**

IV B.Tech I Semester Regular/Supple Examinations, March - 2021

CRYPTOGRAPHY AND NETWORK SECURITY

(Common to Computer Science and Engineering and Information Technology)

Time: 3 hours **Max. Marks: 70**

Question paper consists of Part-A and Part-B
Answer ALL sub questions from Part-A
Answer any FOUR questions from Part-B
****

PART–A *(14 Marks)*

1.	a)	Define Brute-force attack.	[2]
	b)	In DES the effective key size of round key is 48 bits long ?	[3]
	c)	Mention any one technique of attacking RSA.	[2]
	d)	How keys are exchanged in Diffie-Hellman algorithm	[2]
	e)	List out the properties of hash function.	[2]
	f)	What is transport mode and tunnel mode in IP sec?	[3]
	g)		

PART–B *(4x14 = 56 Marks)*

2.	a)	Explain the various active attacks? What security mechanisms are suggested to counter the active attacks?	[7]
	b)	Discuss the various principles involved in private and public key cryptography.	[7]
3.	a)	Explain simplified DES with example	[7]
	b)	How AES is used for encryption/decryption? Discuss with example.	[7]
4.		Describe the MD5 message digest algorithm with necessary block diagrams.	[14]
5.	a)	Describe the steps in finding the message digest using SHA-512 algorithm. What is the order of finding two messages having the same message digest?	[7]
	b)	What are the requirements of cryptographic hash functions?	[7]
6.	a)	How does PGP provide authentication and confidentiality for email services ?Discuss	[7]
	b)	Write in detail about Secure Socket Layer protocol stack.	[7]
7.	a)	What are the services provided by IPSec? Where can be the IPSec located on a network?	[7]
	b)	Explain how firewalls help in establishing a security framework for an organization.	[7]