CRYPTOGRAPHY AND NETWORK SECURITY

(Code : CST-603)

Full Marks : 70 *Time* : 3 hours

Answer any **five** questions

Figures in the right-hand margin indicate marks

1.	(*a*)	Distinguish between Plain text and Cipher text with example.	2
	(*b*)	Write the compression between Symmetric and Asymmetric key cryptography.	5
	(*c*)	What do you mean by Secure Electronic Transaction ? Explain the Set process.	7
2.	(*a*)	Name various types of attack on computer system.	2
	(*b*)	Explain Digital Certificate. What are certificate creations procedures ?	5
	(*c*)	Explain the RSA algorithm. Describe the example of RSA.	7
3.	(*a*)	Define Smart Card.	2
	(*b*)	Describe Biometric Authentication.	5
	(*c*)	Define Authentication Tokens. How does this works ? Explain its type.	7
4.	(*a*)	Define IP security.	2
	(*b*)	Write the compression between Symmetric and Asymmetric key cryptography.	5
	(*c*)	Describe Substitution Technique and transposition technique.	7
5.	(*a*)	Define time stamping protocol.	2
	(*b*)	Explain private key management.	5
	(*c*)	What do you mean by DES ? Explain how DES works ?	7
6.	(*a*)	Distinguish between Encryption and Decryption.	2
	(*b*)	What are different principles of Security explain with example.	5
	(*c*)	Explain Virtual Private Network. Describe VPN Architecture.	7
7.	(*a*)	Define Password. What do you mean by Plain Text password ?	2
	(*b*)	Describe the position of SSL in TCP/IP protocol suite with Diagram.	5
	(*c*)	Write short notes on any *two* :	$3\frac{1}{2}\times 2$
		(*i*) TCP/IP	
		(*ii*) Certificate-based Authentication	
		(*iii*) Firewall	
		(*iv*) Digital Signature.	

VI- SEM /IT/CSE/2019(W)/NEW

CST-603-C&N SECURITY

Full Marks: 80 Time : 3 Hours

Answer any Five Questions including Q No. 1 & 2

Figures in the right hand margin indicates marks

Q.1	Answer ALL the questions:	2X10
a)	Define attack? List the types of attack.	
b)	What do you mean by plaintext and cipher text?	
c)	List out some Transposition techniques.	
d)	List down some functions of firewall.	
e)	What is VPN?	
f)	What are the major threats to Data or Information?	
g)	What is the role of hash function in cryptography?	
h)	What do you know about Vernam Cipher?	
i)	How authentications vary from authorization?	
j)	Define Encryption and Decryption.	
Q.2	Answer any SIX questions:	
a)	Explain Digital Signature algorithm.	5X6
b)	Write the difference between block cipher and stream cipher.	
c)	Write the procedure of DES algorithm.	
d)	Write short notes on i) SHTTP ii) Secure Socket Layer	
e)	Describe the principle of security	
f)	List down difference between substitution and transposition techniques.	
g)	Briefly describe the certificate based techniques of authentication.	
Q.3	Describe Asymmetric key cryptography with RSA algorithm.	10
Q.4	What is the role of SET protocol in Internet Security? Describe in detail.	10
Q.5	Explain the layering architecture of TCP/IP.	10
Q.6	What do you mean by secret key cryptography and Public Key Cryptography? How they are different from one another?	10
Q.7	Write short notes on i) PKIX Model ii) Biometric Authentication	10

6TH SEM./CSE/IT/ 2022(S)

TH1 Cryptography and Network security

Full Marks: 80 Time- 3 Hrs

Answer any five Questions including Q No.1& 2
Figures in the right hand margin indicates marks

1. Answer **All** questions 2 x 10

   a. Differentiate between substitution technique and Transposition technique.
   b. Define Rail Fence technique.
   c. Where SSL layer is located in TCP/IP?
   d. Define seed.
   e. Write the problem associated with clear text password.
   f. Define IP address spoofing
   g. Define static web page and Dynamic web page.
   h. What are the problems with symmetric key cryptography?
   i. Define VPN.
   j. Define Brute-force attack.

2. Answer **Any Six** Questions 6 x 5

   a. Discuss about different types of attack.
   b. Difference between symmetric and asymmetric key cryptography.
   c. Discuss the mechanism used by a RA for checking the user's proof of possession of the private key.
   d. Discuss about screen host firewall, single-homed Bastion configuration.
   e. Discuss about PKIX Services.
   f. Discuss about Digital Envelop.
   g Discuss about Authentication token.

3 Briefly Discuss about key principle of network security. 10

4 Define digital certificate. Write the step to create digital certificate. 10

5 Define SSL and discuss how SSL works? 10

6 Discuss about DES and how it works. 10

7 Explain about IP Security. 10

6TH SEM./CS & E /I T / 2023(S)

TH- 1 Cryptography and Network security

Full Marks: 80 Time- 3 Hrs

Answer any five Questions including Q No.1& 2
Figures in the right hand margin indicates marks

1. Answer **All** questions 2 x 10
   a. Define Brute-force attack.
   b. What is masquerade?
   c. Compare Substitution and Transposition techniques.
   d. Convert the Given Text "ALL THE BEST" into cipher text using Rail fence Technique.
   e. What is Tiny Fragment attack?
   f. Define static and dynamic webpage.
   g. Define digital envelop.
   h. Define CRL.
   i. Write the name of participants in the SET system.
   j. Write the problem associated with clear text password.

2. Answer **Any Six** Questions 6 x 5
   a. Differentiate between symmetric key and asymmetric key cryptography.
   b. Explain briefly about SSL protocol.
   c. Discuss different types of attacks.
   d. Define authentication token and illustrate how Challenge/Response Tokens works.
   e. Write the mechanism to protect private keys.
   f. Define digital certificate and the different process to revoke a digital certificate
   g Explain the followings:
   (a) Caesar cipher (b) Polygram substitution cipher**.**

3 Write the RSA algorithm and explain it with example 10

4 Encrypt "SWARAJ IS MY BIRTH RIGHT" by play fair cipher using the keyword MONARCHY. 10

5 Briefly Discuss about key principle of network security 10

6 Explain in detail about architecture of IP Security 10

7 Write short notes on any two 10
   a) PKIX Services.
   b) VPN
   c) Biometric Authentication.
   d) Encryption and Decryption

6TH SEM./CS&E /IT/ 2024(S)

Th-1 Cryptography and Network Security

Full Marks: 80 **Time- 3 Hrs**

Answer any five Questions including Q No.1& 2
Figures in the right hand margin indicates marks

1. Answer **All** questions 2 x 10
   a. Distinguish between passive attack and active attack.
   b. Define Denial of service.
   c. What are the protocols used in IP security?
   d. Convert the Given Text "CRYPTOGRAPHY" into cipher text using Rail fence Technique.
   e. Name three configuration of firewall.
   f. Define active webpage.
   g. Define time stamping protocol.
   h. Define block cipher.
   i. Write the name of participants in the SET system.
   j. Define SEED.

2. Answer **Any Six** Questions 6 x 5
   a. Differentiate between symmetric key and asymmetric key cryptography.
   b. Convert the plain text "ACT" using hill cipher to cipher text using key matrix.
   6 24 1
   13 16 10
   20 17 15
   c. Write the RSA algorithm and explain it with a suitable example.
   d. Define authentication token and illustrate how Challenge/Response Tokens works.
   e. Discuss briefly about Digital Signature.
   f. Define firewall. How application Gateway and Packet filter works.
   g Why is SSL layer positioned between the application layer and transport layer? Explain the SSL handshake protocol.

3 Define digital certificate and write down the steps required to generate a digital certificate. 10

4 Briefly Discuss about key principles of network security. 10

5 Define Secure Electronic Transaction. Discuss the entire SET process briefly. 10

6 Briefly explain about the architecture of VPN. 10

7 Write short notes on any two. 10
   a) SSL
   b) Biometric Authentication
   c) IPSec
   d)Encryption and Decryption