Code No: **R42042** **R10** **Set No. 1**

IV B.Tech II Semester Regular Examinations, April/May - 2014

NETWORK SECURITY & CRYPTOGRAPHY

(Common to Electronics & Communication Engineering and Electronics and Computer Engineering)

Time : 3 hours **Max. Marks: 75**

Answer any Five Questions
All Questions carry equal marks
*****

1 a) What is buffer overflow? What is to be done after overflowing the buffer? List the defensive techniques against buffer overflows. [8]
b) What is a format string? How does a format string vulnerability look like? Describe the role of stack at format strings. [7]

2 How is key generated in Blowfish algorithm? Explain about the encryption function in Blowfish algorithm. Comment on the security of Blowfish. [15]

3 a) What is congruence? Describe the modular arithmetic operations using congruence with examples? [8]
b) What are discrete logarithms? Explain their use in public key cryptography? [7]

4 a) Give the structure of a public key cryptosystem. Demonstrate how sender authentication and confidentiality be achieved simultaneously with public key cryptography. What are the requirements of a public key cryptosystem? [9]
b) "RSA is vulnerable to chosen cipher text attack". Comment on it. [6]

5 a) What is the role of authentication in network security? Name the several methods used for authentication. [8]
b) What is a dictionary attack? Explain with an example. [7]

6 a) Kerberos is based on five symmetric keys. What are they? How are they used? [7]
b) Illustrate a two step process for obtaining a service in Kerberos. [8]

7 a) Describe the steps involved in the handshake protocol and the types of attacks that it may encounter. [8]
b) Explain the use of Diffie Hellman in SSL/TLS. [7]

8 a) Describe the limitations of firewall inspection. [8]
b) Describe the important practices required in maintaining the effectiveness of a firewall. [7]

Code No: **R42042** **R10** **Set No. 2**

IV B.Tech II Semester Regular Examinations, April/May - 2014

NETWORK SECURITY & CRYPTOGRAPHY

(Common to Electronics & Communication Engineering and Electronics and Computer Engineering)

Time : 3 hours **Max. Marks: 75**

Answer any Five Questions
All Questions carry equal marks
*****

1		Mention all the classical ciphers. Explain with an example.	[15]
2		Illustrate the process of encryption in AES.	[15]
3	a)	How do you find large prime numbers using Millers Rabin algorithm?	[8]
	b)	What is Euler's totient function? Explain its use.	[7]
4	a)	What are the characteristics of public key cryptography?	[7]
	b)	Let p=101, q=113 and e=3533. Find d? From this example describe the computational issues in RSA?	[8]
5	a)	What are the properties of hash functions? Explain their use in authentication.	[6]
	b)	Give the structure of HMAC. Describe its capabilities when it is based on SHA.	[9]
6	a)	What are the features of S/MIME? What services are offered by S/MIME?	[9]
	b)	Compare the features of S/MIME with PGP.	[6]
7	a)	Explain how IPSec is used in the Transport & Tunnel mode.	[8]
	b)	List all the crypto schemes available in TLS.	[7]
8	a)	What are the different types of malware and their means of propagation?	[10]
	b)	Give the structure of a Worm? Quote some examples for worm attacks.	[5]

Code No: **R42042** **R10** **Set No. 3**

IV B.Tech II Semester Regular Examinations, April/May - 2014

NETWORK SECURITY & CRYPTOGRAPHY

(Common to Electronics & Communication Engineering and Electronics and Computer Engineering)

Time : 3 hours **Max. Marks: 75**

Answer any Five Questions
All Questions carry equal marks
*****

1	a)	What is an SQL injection? Using this attack, what things can the attacker do?	[8]
	b)	What messages are exchanged in a typical session between a client & server? What types of attacks can be performed on this session?	[7]
2		Mention the key size, block size and mathematical operations used by CAST 128 algorithm. Describe CAST 128 encryption function.	[15]
3	a)	State Fermat's Little theorem. State the importance of this theorem in RSA cryptosystem.	[8]
	b)	Propose an algorithm to compute a^{120} mod n, where a is a 100 digit number and n is a 200 digit number.	[7]
4	a)	Give an outline of the mathematical operations employed in Diffie Hellman key exchange.	[8]
	b)	How can a secure communication between two unknown parties be done using public key cryptography?	[7]
5	a)	What are the properties of Message Authentication Codes? Explain their use for authentication.	[8]
	b)	Explain how password based authentication works?	[7]
6		Describe the entire encryption and decryption process in PGP.	[15]
7	a)	When the client side uses a password for authentication, describe how the SSL/TLS protect this password?	[8]
	b)	Compare the differences and similarities that exist between the SSL and TLS.	[7]
8	a)	What is the functionality of an Intrusion detection system?	[6]
	b)	Explain the anamoly based intrusion detection methods in detail.	[9]

Code No: **R42042** **R10** **Set No. 4**

IV B.Tech II Semester Regular Examinations, April/May - 2014

NETWORK SECURITY & CRYPTOGRAPHY

(Common to Electronics & Communication Engineering and Electronics and Computer Engineering)

Time : 3 hours **Max. Marks: 75**

Answer any Five Questions
All Questions carry equal marks
*****

1 a) What is meant by phishing? How these attacks are performed and transmitted? [8]
b) Explain the properties Confusion & Diffusion. What is the importance of these properties in cryptographic algorithms? [7]

2 a) Mention the Block Cipher modes of operations. Describe the use of DES in CBC mode. [8]
b) What is linear and differential cryptanalysis done? [7]

3 a) Define a primitive root. Show that if g is a primitive root of m, then the powers 1, g, g^2, …. $g^{\phi(m)-1}$ represent each integer relatively prime to m uniquely modulo m. In particular, if m>2, then $g^{\phi(m)/2}$= 1 modulo m. [7]
b) Give the algorithm for extended Euclid's algorithm. Show the steps in computing gcd(576, 486). [8]

4 a) An elliptic curve over GF(p) is defined as y^2=mod p=x^3+ax+b mod p in which a=b=1 and p=23. Find the solutions of this equation. Plot the curve. [8]
b) Compare RSA with Diffie Hellman key exchange algorithm. [7]

5 a) Write the steps for computing Key and signature verification process in Digital Signature Standard. [8]
b) Describe any two authentication protocols in detail. [7]

6 a) Describe the detailed information contained within a X.509 certificate. [10]
b) How is trust managed in X.509 certificates? [5]

7 a) Describe the use of HMAC in SSL/TLS. [7]
b) How is Authentication header used in transport and tunnel mode in IPv4 and IPv6? [8]

8 a) At what positions the firewalls may be located. Explain. [5]
b) What are the various features and operations of stateless packet filtering? Describe how a stateless packet filter blocks an incoming TCP connection. What are the weakness of stateless packet filtering? [10]