Code No: RR410504 **Set No.1**

IV B.Tech. I Semester Regular Examinations, November -2005
NETWORK SECURITY AND CRYPTOGRAPHY
(Computer Science & Engineering)

Time: 3 hours **Max Marks: 80**

Answer any FIVE Questions
All Questions carry equal marks

⋆ ⋆ ⋆ ⋆ ⋆

1. (a) What is Steganography? [6]
   (b) Explain various modes of operations of block ciphers [10]
2. Demonstrate that Blow Fish decryption is inverse of Blowfish encryption. [16]
3. (a) What are Principal elements of a public - key crypto systems? [8]
   (b) What are the roles of the public and private key? [8]
4. Given 2 as a primitive root of 29, construct a table of indices, and use it to solve the following congruences:
   (a) $17x^2 \equiv 10 \bmod 29$
   (b) $x^2 - 4x - 16 \equiv 0 \bmod 29$
   (c) $x^7 \equiv 17 \bmod 29$ [5+5+6]
5. (a) What is the difference between weak and strong collision resistance?
   (b) What is the role of a compression function in a hash function? [6+10]
6. Explain X.509 Authentication services [16]
7. (a) What services are provided by the SSL Record Protocol?
   (b) What steps are involved in the SSL Record Protocol transmission? [6+10]
8. (a) List and briefly define three classes of intruders.
   (b) What are two common techniques used to protect a password file? [8+8]

⋆ ⋆ ⋆ ⋆ ⋆

Code No: RR410504 **Set No.2**

IV B.Tech. I Semester Regular Examinations, November -2005
NETWORK SECURITY AND CRYPTOGRAPHY
(Computer Science & Engineering)

Time: 3 hours **Max Marks: 80**

Answer any FIVE Questions
All Questions carry equal marks

⋆ ⋆ ⋆ ⋆ ⋆

1. (a) What is Steganography? [6]
   (b) Explain various modes of operations of block ciphers [10]
2. (a) List the characteristics of advanced block ciphers. [8]
   (b) What are the differences between RC5 and RC2? [8]
3. Consider the following scheme
   (a) Pick an odd number E
   (b) Pick two prime numbers, P and Q, where (P-1)(Q-1)-1 is evenly distributed by E
   (c) Multiply P and Q to get N
   (d) Calculate $D = \frac{(P-1)(Q-1)(E-1)+1}{E}$
   Is this scheme is equivalent to RSA ? Show why or why not [16]
4. (a) Explain Chinese Remainder Theorem.
   (b) Find all primitive roots of 7. [8+8]
5. (a) List requirements for a Hash Function.
   (b) How the hash function value is generated in Simple Hash functions? [6+10]
6. (a) List limitations of SMTP/822 scheme?
   (b) What are the MIME specifications? [8+8]
7. (a) What is replay attack?
   (b) Why does ESP include a padding field? [6+10]
8. (a) what information used by a typical packet-filtering router?
   (b) What are some weaknesses of a packet-filtering router?
   (c) What is the difference between a packet-filtering router and a stateful inspection firewall? [8+4+4]

⋆ ⋆ ⋆ ⋆ ⋆

Code No: RR410504 **Set No.3**

IV B.Tech. I Semester Regular Examinations, November -2005
NETWORK SECURITY AND CRYPTOGRAPHY
(Computer Science & Engineering)

Time: 3 hours **Max Marks: 80**

Answer any FIVE Questions
All Questions carry equal marks

⋆ ⋆ ⋆ ⋆ ⋆

1. This problem provides a numerical example of encryption using a one-round version of DES. We start with the same bit pattern for the key and plain text, namely,
In hexadecimal notation 0 1 2 3 4 5 6 7 8 9 A B C D E F

Inbinary notation:	0000	0001	0010	0011	0100	0101	0110	0111
	1000	1001	1010	1011	1100	1101	1110	1111

   (a) Derive K_1, the first - round subkey.
   (b) Derive L_0, R_0
   (c) Expand R_0 to get $E[R_0]$
   (d) Calculate A=$E[R_0] \oplus K_1$.
   (e) Group the 48-bit result of (d) into sets of 6 bits and evaluate the corresponding S-box substitutions.
   (f) Cancatenate the results of (e) to get a 32-bit result,B.
   (g) Apply the permutation to get P(B).
   (h) Calculate R1=P(B) $\oplus$ L_0
   (i) write down the cipher text. [16]

2. Demonstrate that Blow Fish decryption is inverse of Blowfish encryption. [16]

3. (a) Explain RSA Algorithm? [8]
   (b) In a RSA system, the public key of a given user is e=31,n=3599.What is the private key of this user? [8]

4. (a) what is a prime Number?
   (b) What is a relative prime number?
   (c) What is Euler's totient?
   (d) What is the meaning of the expression a divides b? [4+4+6+2]

5. (a) What is a message authentication code?
   (b) When a combination of symmetric encryption and an error control code is used for message authentication, in what order must the two functions be performed?
   (c) Explain Data Authentication Algorithm. [4+4+8]

6. (a) What is the purpose of the X.509 standard?
   (b) What is a chain of certificates?
   (c) How is an X.509 certificate revoked? [4+4+8]

7. Write a short note on
   (a) Electronic mail Services
   (b) Firewalls [8+8]

8. (a) what information used by a typical packet-filtering router?
   (b) What are some weaknesses of a packet-filtering router?
   (c) What is the difference between a packet-filtering router and a stateful inspection firewall? [8+4+4]

⋆ ⋆ ⋆ ⋆ ⋆

Code No: RR410504 **Set No.4**

IV B.Tech. I Semester Regular Examinations, November -2005
NETWORK SECURITY AND CRYPTOGRAPHY
(Computer Science & Engineering)

Time: 3 hours **Max Marks: 80**

Answer any FIVE Questions
All Questions carry equal marks

⋆ ⋆ ⋆ ⋆ ⋆

1. This problem provides a numerical example of encryption using a one-round version of DES. We start with the same bit pattern for the key and plain text, namely,
In hexadecimal notation 0 1 2 3 4 5 6 7 8 9 A B C D E F

Inbinary notation:	0000	0001	0010	0011	0100	0101	0110	0111
	1000	1001	1010	1011	1100	1101	1110	1111

   (a) Derive K_1, the first - round subkey.
   (b) Derive L_0, R_0
   (c) Expand R_0 to get $E[R_0]$
   (d) Calculate A=$E[R_0] \oplus K_1$.
   (e) Group the 48-bit result of (d) into sets of 6 bits and evaluate the corresponding S-box substitutions.
   (f) Cancatenate the results of (e) to get a 32-bit result,B.
   (g) Apply the permutation to get P(B).
   (h) Calculate R1=P(B) $\oplus$ L_0
   (i) write down the cipher text. [16]

2. (a) List the characteristics of advanced block ciphers. [8]
   (b) What are the differences between RC5 and RC2? [8]

3. List four general categories of schemes for distribution of public keys. [16]

4. (a) Define a Groups, a Rings and a Fields?
   (b) Construct Additive table and Multiplicative table for GF(7)? [6+10]

5. (a) What is the difference between weak and strong collision resistance?
   (b) What is the role of a compression function in a hash function? [6+10]

6. (a) Discuss cryptographic algorithms used in S/MIME
   (b) List limitations of SMTP/822 scheme? [8+8]

7. Write a short note on
   (a) Electronic mail Services
   (b) Firewalls [8+8]

8. Write notes on
   (a) Trapdoors
   (b) Logic bomb
   (c) Trojan horses [5+5+6]

⋆ ⋆ ⋆ ⋆ ⋆