[Total No. of Questions - 8] [Total No. of Printed Pages - 4] (2125)

15410

M. Tech 3rd Semester Examination

Information Security (NS)

EC-305

Time : 3 Hours **Max. Marks : 100**

The candidates shall limit their answers precisely within the answer-book (40 pages) issued to them and no supplementary/continuation sheet will be issued.

Note : Each Question carry equal marks (20 each). Attempt any five questions.

1. (a) Define the three security Goals. List and define security services and security mechanisms. (10)

   (b) Describe linear and differential cryptanalysis for DES cipher. (10)

2. (a) Draw the data flow diagram (tracking how the bits move) in an example three-round Feistel Substitution-Permutation Network (SPN). Be sure to label all the constituent parts and briefly explain what they do. (10)

   (b) Shift Cipher is based on modular arithmetic. Define the modular arithmetic and specify the properties satisfied by modular arithmetic. Explain these properties in terms of group, ring and fields also. Decrypt the following message.

   aol zpal jvbsk il altwvyhypsf buhchpshisl vy avv ibzf. ayf hnhpu pu h mid tvtluaz. (10)

[P.T.O.]

3. (a) Consider the elliptic curve :

   E: $y^2 = x^3 + 4x + 4 \pmod 5$

   Find the points on the curve. Given two points (1,2) and (4,3) compute the third point. Describe discrete logarithm problem for elliptic curve. (10)

   (b) Why is collision resistance a requirement for cryptographic hash functions? Explain with an attack scenario. (10)

4. (a) What is Message Authentication Code? Describe how you would design a way to compute a MAC using the block cipher. (10)

   (b) Consider Diffie-Hellman with p=7 and g=5. Assume Alice picket 2 as her random number while Bob picked 3 as his random number. What is the value of the shared secret between Alice and Bob following the Diffie-Hellman message exchange? (10)

5. (a) Describe Secure Hash Algorithm. Explain how SHA-1 is more secure than MD4 and MD5. (10)

   (b) Describe Kerberos authentication scheme. How do you ensure that your system is using Kerberos on your Web Server? (10)

6. (a) Consider the following C code:

```
/* Escapes all newlines in the input string, replacing them
with "\n". */

/* Requires: p != NULL; p is a valid '\0'-terminated
string */

void escape(char *p)

    {
```

```
while (*p ! = '\0')
switch (*p)
{
    case '\n':   memcpy(p+2, p+1,
strlen(p));
                 *p++ = 11-; *p+ + - 'n';
                 break;
    default:     p++;
}
}
```

You may assume that escape()'s argument is always non-null and points to a '\0'-terminated string.

Explain the security problem with this code and also suggest measures to overcome the same. (10)

(b) How can ICMP packets be misused by a hacker to gain access to internal network resources? What weaknesses of ICMP packets enable such attacks? (10)

7. (a) Phil Zimmermann chose IDEA, three-key triple DES (also know as triple DEA), and CAST-128 as conventional encryption algorithms for PGP. Give reasons why DES, Blowfish, and RC5 encryption algorithms are suitable or unsuitable for PGP. (10)

(b) Suppose you are working for a firm that wants to participate in an online tendering process of ONGC. What would be the prerequisites (from information security point of view) to be fulfilled by your company? Summarize how you will achieve them. (10)

[P.T.O.]

8. (a) Consider the following protocol of communication between Alice A, Bob B and a server S who mediates between them. The protocol employs two types of encryption

(i) **Standard encryption:** Using Encryption function E, Alice and Bob knows to produce E(m) for a given m, but only server knows how to decrypt such a message m. This encryption can be implemented using RSA.

(ii) **Vernam Encryption:** using two keys k1 and k2, V(kl, V(k1, k2)) = k2. It means that if k1 is known, then V(k1, k2) can be decrypted to obtain k2. The communication protocol establishes session key by exchanging following messages:

Message 1: $A \rightarrow S$: $A.S.B.E(k_a)$

Message 2: $S \rightarrow B$: $S.B.A$

Message 3: $B \rightarrow S$: $B.S.A.E(k_b)$

Message 4: $S \rightarrow A$: $S.A.B.V(k_a, k_b)$

Explain whether the given protocol is secure or not. If not give the intruder model and suggest the ways to mitigate the attack. (10)

(b) What is the difference between mail server and domain name server? What are the security issues in DNS? (10)