Printed Pages : 4 MCA – 404(2)

(Following Paper ID and Roll No. to be filled in your Answer Book)

PAPER ID : 1476 Roll No.

MCA

(SEM. IV) EXAMINATION, 2006-07

CRYPTOGRAPHY & NETWORKS SECURITY

Time : 3 Hours] *[Total Marks : 100*

Note : *Attempt **all** questions.*

1. Attempt any **four** out of the following :

(a) What is denial of service attack? **5**

(b) What is Trojan Horse? What is the principle behind it? **5**

(c) What is repudiation? How can it be prevented in real life? **5**

(d) Let C be a block cipher of block size n : **5**

(i) How many different block values are possible?

(ii) How many different permutations of blocks are possible?

(iii) If C is not an arbitrary permutation, but has key length k, how many trials will be required to break c through exhaustive key search.

(e) While DES keys are 64 bites long, but its effective key length is only 56 bits, why? **5**

(f) What is the most security – critical component of DES round function. Give a brief description of this component. **5**

2. Attempt any **four** parts of the following:

(a) What is the idea behind meet in the middle attack? How it can be avoided in 3 DES? **5**

(b) What is the difference between block cipher and stream cipher? What are the different modes of block cipher operation? Explain any one of them. **5**

(c) Draw a diagram of cyclic encryption being used to generate pseudo-random Numbers. **5**

(d) Consider the diffic-Hellman scheme with a common-prime $q = 11$ and primitive root $\alpha = 2$. **5**

(i) Show that 2 is indeed a generator

(ii) If the user A has public key $Y_A = 9$ what is A's private key?

(iii) If the user B has public key $Y_B = 3$ what is the secret key k in between A and B.

(e) Explain Blowfish in detail. **5**

(f) Discuss the vulnerabilitus of DES **5**

3. Attempt any **two** out of the following:

(a) Assume you have a secret that you encrypt and publically post the cipher text. You use a 56 bit keying variable and then split the keying variable into two equal – size non-overlapping. Segments of 28 bits each. You give one of these segments to Trustee A and give the other to Trustee B. If one of these trustees tries to break the cipher, how many keying variables would the trustee have to key an advantage in order to be successful? **10**

(b) Write extended Euclid algorithm and find the value of the following: **10**

(i) $47^{1395} \bmod (48)$

(ii) $4^{3207} \bmod (1024)$

(iii) $2^{57} \bmod (123)$

(c) Write RSA algorithm if N = 187 and the encryption key E=17, find out the corresponding private key. **10**

4. Attempt any **two** out of the following:

(a) Alice is using a toy version of the DSS signature scheme with a prime modulus P = 47 and generator g = 2 of order q = 23. By accident, slice generates signatures for two different messages with the same per-message random number K. The hash codes of two signed messages are 2 and 3 and signatures are (4, 21) and (4,19) respectively, compute slice private key. **10**

(b) How the messages are generated and transmitted in pretty good privacy (PGP) protocol? Explain with clear diagrams. **10**

(c) Describe the properties of a cryptographic hashing function. Clearly describe how a cryptographic hashing function can be implemented using a block cipher. **10**

5 Attempt any **two** parts out of the following :

(a) Describe the man-in-the middle threat in secure shell and investigate which authentication options it offers. **10**

(b) List the characteristics of a good firewall implementation ? How is a circuit gateway different from an application gateway ? **10**

(c) Describe the role of Ticket granting server (TGS) in kerberos authentication protocol. **10**