Printed Pages : 4

* 2 1 4 4 0 6 *

CA406

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

PAPER ID : 214406

Roll No. □□□□□□□□□□

M.C.A.

(SEM. IV) THEORY EXAMINATION, 2014-15

NETWORK SECURITY & CRYPTOGRAPHY

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

Note:(1) Attempt ALL questions.

(2) All questions carry equal marks.

(3) Notation/Symbols/Abbreviations used have usual meaning.

(4) Make suitable assumption, wherever required.

1 Attempt any four parts of the following: 5×4=20

(a) Draw the block diagram showing the structure of Fiestal cipher. Write down the main features of the Fiestal structure.

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

(c) Describe the ECB and CFB modes of operation of a block cipher.

(d) What are the advantages of polyalphabetic substitution ciphers over monoalphabetic substitution ciphers ? Describe encryption and decryption process of any polyalphabetic substitution cipher.

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

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

2 Attempt any four parts of the following: 5×4=20

(a) Determine the multiplicative inverse of 1234 mod 4321.

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

(c) Describe the encryption and decryption process of a block cipher in Output Feedback (OFB) mode.

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

(e) Answer following in context of DES cipher:

(i) What is the block size ?

(ii) What is the purpose of S-boxes and how many S-Boxes are there ?

(iii) What is the size of round keys ?

(iv) Is it possible that key schedule generated by one key is reverse of the key schedule generated by some other key ? Justify your answer.

(v) What is the importance of Initial permutation

www.aktuonline.com

(f) Let C be a block cipher of block size n:

(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 (through exhaustive key search.)

3 Attempt any two parts of the following: 10×2=20

(a) Describe the Digital Signature Algorithm (DSA) of Digital Signature Standard.

(b) 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?

(c) Write extended Euclid algorithm and find the value of the following :

(i) 47^{1395} mod(48)

(ii) 4^{3207} mod(1024)

(iii) 2^{57} mod(123)

www.aktuonline.com

4 Attempt any two parts of the following: 10×2=20

(a) How the messages are generated and transmitted in pretty good privacy (PGP) protocol?

Explain with clear diagrams.

(b) Write short notes on any one of the following :

(i) Kerberos

(ii) Firewalls.

(c) (i) What is dual signature in context of Secure Electronic Transaction (SET). Describe the sequence of events that are required for a SET transaction.

(ii) What are different modes in which IPSec services can be used ? Discuss.

5 Write short notes on any two of the following : 10×2=20

(a) Playfair Cipher

(b) Kerberos

(c) Vigenere Cipher.