University Roll No.:

YMCA UNIVERSITY OF SCIENCE AND TECHNOLOGY, FARIDABAD

M. TECH (III SEM) EXAMINATION (UNDER CBS)

Security in Communication Networks (E-16C-707C)

Time: - Three Hours Maximum Marks:-60

Note:- (i) Question no.1 is compulsory from Section-A.
(ii) Attempt any four questions from Section-B.

SECTION-A (2x10 = 20 Marks)

Q.1.a) Which attacks are more harmful active or passive. Give reason also.

b) Differentiate between trust and cryptographic security mechanisms (2)

c) What is a captcha and why it is used. (2)

d) Which is more secured AES or DES? Give reason to support your answer. (2)

e) Why older cryptographic algorithm are not used for image encryption. (2)

f) How email security is different from other security mechanisms (2)

g) An instruction takes 0.1 micro second to execute on a processor. Calculate the brute force search time required by it to find the password of a word file having 4 character passwords (Given). Assume that the password can be a combination of 256 characters. (2)

h) Why MAC enabled internet access providers are not secured. (2)

i) Explain at which layer proxy firewall is used and the purpose of it. (2)

j) Explain why time complexity of both 2DES and 3DES is same. (2)

SECTION-B (4x10 = 40 Marks)

Q.2.a) Explain various network security requirements and how they can be achieved (5)

b) Explain network security model and of internetwork security. (5)

Q.3.) Explain AES algorithm and do explain its various steps with the help of algorithms (especially Key Generation) (10)

Q.4.) Differentiate between conventional and digital signature. How they are created. Also explain which network security requirements are achieved using it. (10)

Q.5.a) Differentiate between AH and ESP. Also explain the working of ESP protocol. (5)

b) What are the three criteria's of checking a hash function. A hash function is formed by adding all the characters given in the text. Does this hash function satisfy all the criteria. Give reasons. (5)

Q.6.a) How email security is different from other security mechanisms. Also explain email security in detail. (5)

b) Differentiate between SSL and TLS. Also explain TLS in detail (5)

Q.7.a) Calculate the value of key using diffie hellman algorithm for the following data p=11, q=17 (Random number shared between source and destination), x=57 (chosen by source), y=99 (chosen by destination). (5)

Q. b) Explain the advantages of SNMPv3 over SNMPv1 and v2. Also explain SNMPv3 in detail. (5)