Code No: 138DT **R16**

JAWAHARLAL NEHRU TECHNOLOGICAL UNIVERSITY HYDERABAD
B. Tech IV Year II Semester Examinations, July - 2021
NETWORK SECURITY AND CRYPTOGRAPHY
(Electronics and Communication Engineering)

Time: 3 hours **Max. Marks: 75**

Answer any Five Questions
All Questions Carry Equal Marks

1.a) Explain the types of attacks on data being transmitted over an insecure channel? Also describe the services on which these attacks are performed.

b) Alice has a long message to send. She is using mono alphabetic substitution cipher. She thinks that if she compresses the message it may protect the text from single letter frequency attack by Eve. Does the compression help? Should she compress the message before the encryption or after the encryption? Defend. [8+7]

2.a) How is steganography different from Cryptography? Will it result in better security combining the two? If so, how? If not, why?

b) Differentiate IDEA and DES algorithm. [7+8]

3.a) List the characteristics of modern block cipher algorithms.

b) With the linear congruential algorithm, a choice of parameters that provides a full period does not necessarily provide a good randomization. For example, consider the following two generators:
$Xn+1 = (6Xn) \bmod 13$
$Xn+1 = (7Xn) \bmod 13$
Write out the two sequences to show that both are full period. Which one appears more random to you? [8+7]

4.a) Why is $\gcd(n, n+1) = 1$ for two consecutive integers n and $n + 1$?

b) If n is composite and passes the Miller-Rabin test for the base a, then n is called a *strong pseudo prime to the base a*. Show that 2047 is a strong pseudo prime to the base 2.[7+8]

5.a) In a public-key system using RSA, you intercept the ciphertext $C = 10$ sent to a user whose public key is $e = 5$, $n = 35$. What is the plaintext M?

b) In what ways can a hash value be secured so as to provide message authentication?[8+7]

6.a) List two disputes that can arise in the context of message authentication. In what order should the signature function and the confidentiality function be applied to a message, and why?

b) What drawbacks of Kerberos version 4 are addressed in Kerberos Version 5? Explain how? [8+7]

7.a) Is Oakley protocol vulnerable to clogging attack? If so, how? If not, why?

b) Explain in detail an open encryption and security specification designed to protect credit card transactions on the internet? [7+8]

8.a) What are two default policies that can be taken in a packet filter if there is no match to any rule? Which is more conservative? Explain with example rule sets both the policies?

b) Explain in detail virus structure? Explain how a compression virus propagates? [7+8]

--ooOoo--