Code: 17D08102

M.Tech II Semester Supplementary Examinations January/February 2019

NETWORK SECURITY & CRYPTOGRAPHY

(Common to CSE & CS)

(For students admitted in 2017 only)

Time: 3 hours Max. Marks: 60

Answer all the questions

*****

1 $C = (P \times K_1 + K_2) \bmod 26$; $P = ((C-K_2) \times K_1^{-1}) \bmod 26$ is the affine cipher to encrypt and decrypt with mod26 where K_1^{-1} is the multiplicative inverse of K_1 and $-K_2$ is the additive inverse of K_2. Use it to encrypt the message "Helo" to "ZEBW" with the key pair (7, 2) in mod26. A gain decrypt the message "ZEBW" with the key pair (7, 2) in mod26.

OR

2 Differentiate between block and stream ciphers. Explain the block cipher modes of operations? What are the attacks on block ciphers?

3 Explain the encryption, decryption and key generation in RSA with neat diagrams. Also write the pseudo code associated with them? Give the taxonomy of practical attacks on RSA.

OR

4 Give an overview of SHA-512 by explaining processing steps very clearly.

5 Distinguish between MDC (modification detection code) and MAC (message authentication code).

OR

6 What is digital signature and what process involved in it? Differentiate between conventional and digital signatures. How it provides the major security service directly? What are the possible attacks over it?

7 One of the major roles of public-key encryption has been to address the problem of key distribution, with two distinct aspects:
(i) The distribution of public keys.
(ii) The use of public-key encryption to distribute secret keys.
Explain clearly with neat diagram.

OR

8 The pretty good privacy (PGP) secure email program, is a remarkable phenomenon, has grown explosively and is now widely used. The actual operation of PGP consists of five services: authentication, confidentiality, compression, e-mail compatibility and segmentation. Explain each service very clearly with proper steps.

9 By implementing security at the IP level, an organization can ensure secure networking not only for applications that have security mechanisms but also for the many security-ignorant applications. Write about IP security: Uses, benefits and services. What is encapsulating security payload?

OR

10 What is a firewall and limitations? Explain in detail the three common types of firewalls: Packet filters, application-level gateways & circuit-level gateways?

*****