Internet Tech. & Security-2014

onlineBU.com

Note: Attempt are questions from each unit.

Unit-I

1. (a) Differentiate between differential cryptanalysis and linear cryptanalysis.
(b) Explain how monolithic lipher is prove to statistical analysis attack? How is this problem elimimated in vigilance?

Or

2. Differentiate among the following:
(a) Plaintext and ciphertext,
(b) Symmetric and public Key cipher,
(c) Block Ciphers and stream ciphers,
(d) Substitution cipher and transportation ciphers

Unit-II

3. (a) What is the strength of RSA? If modules used in RSA has very small Prime Factors will the RSA has very small Prime Factors will the RSA implementation be secure? Justify your answer.
(b) What is the strength of ECC based encryption scheme? How to increase the security level.

Or

4. (a) What is clogging attack on Diffie-Hellman Key exchange? Suggest a suitable counter measure.
(b) In RSA if cipher text c = 10, e = 5, n = 35 determine M?

Unit-III

5. (a) Explain use of Hash function to provide source authentication
(i) Using public key encryption
(ii) Without using public key encryption
(b) What is the strength of MAC? Is MAC reversible function? If no, does it pose any limitation or is designed to be so.

Or

6. (a) Differentiate between Message Authentication code and Hash value which are encrypted?
(b) What are the characteristics of good hash function.

Unit-IV

7. (a) What are the service provided by IPSEE? Explain.
(b) In the context of bio metric user authentication, explain the term, enrollment, verification and identification.

Or

8. (a) List and briefly describe common techniques for selecting password, assigning password or to protect password file.
(b) Explain ker beros and x.509.

Unit-V

9. (a) What are different type of firewall explain in detail.
(b) Explain trusted system in detail.

Or

10. Write short note on:
(a) Viruses and worm, (b) Firewall configuration

onlineBU.com

onlineBU.com