10EC832 – Network Security

Assignment-II

Note: i) Write the assignment in a A4 size paper
iii) Mention your USN, name and section on the top right corner of first page
ii) Submit the assignment on or before 11.00 AM, Monday, 11/04/2016

1. Explain Autokey cipher with an example.
2. Briefly explain the need for product ciphers.
3. With the help of a neat figure, explain the working of a rotor machine.
4. Write a short note on Block Ciphers.
5. Explain Confusion and Diffusion of message key.
6. With neat figures, explain Fiestal cipher and DES.
7. Illustrate hill cipher encryption and decryption for the message “we are the champions”.

   Let $A = \begin{bmatrix} 2 & 1 \\ 3 & 4 \end{bmatrix}$ be the encryption matrix.

8. Decrypt the following message which was encrypted using the Hill Cipher.
   Cipher Text: IWGEJLFWRBUEUOWBHPZMLMXNXUBOEUAHG
   Key Matrix,

   $$A = \begin{bmatrix} 11 & 20 & 20 \\ 2 & 1 & 24 \\ 9 & 3 & 3 \end{bmatrix}$$

9. Following message is encrypted using Row-Transposition cipher. Recover the plaintext.
   Key: APPLE (14532)
   Ciphertext: TSUTPI ILRSTX SOANIX HAMROO ICNASN
10. What is an application-level gateway?
11. What is a circuit-level gateway?
12. What are the differences among the firewalls
13. What are the common characteristics of a bastion host?
14. Why is it useful to have host-based firewalls?
15. What is a DMZ network and what types of systems would you expect to find on such networks?
16. What is the difference between an internal and an external firewall?
17. List and briefly define three classes of intruders
18. What are three benefits that can be provided by an intrusion detection system?
19. What is the difference between statistical anomaly detection and rule-based intrusion detection?
20. What metrics are useful for profile-based intrusion detection?
21. What is the difference between rule-based anomaly detection and rule-based penetration identification?
22. What is a honeypot?
23. What is a salt in the context of UNIX password management?