Assignment 4

Deadline: First Day after Leave.

1. Define authentication system. Illustrate the need of mutual authentication over one-way authentication with an example.
2. Explain about working Mechanism of Kerberos. How it differs from Needam Schroder ?
3. What is Rabin Miller primality test? Find if 61 is prime or not.
4. Miller-Rabin test for primality is based on the fact that there are only two numbers in Zp that when squared give us 1. What are those two numbers?
5. What is meant by the strong collision resistance property of a hash function?
6. How Does Kerberos protocol ensure authentication and confidentiality in secure system? Explain.
7. How Hash functions differ from MAC? Given a message m, discuss what arithmetic and logical functions are used by MD4 to produce message digest of 128 bits.
8. What do you mean by digital signature? How digital signatures can be enforced using encryptions? Illustrate with an example.
9. There are two aspects to a secure communication link: authentication and confidentiality. How do you understand these two words? Does the Kerberos protocol give us both?
10. Differentiate between direct digital signature and arbitrated digital signature. How signing and verifying process is done in Digital Signature Standard.
11. How padding is done in SHA-1? How 160-bit of hash value is generated by taking an input message of variable size using SHA-1?
12. Define authentication system and its components. How hardware-based challenge response systems can be used as authentication approach.
13. How padding is done in MD5? What enhancements in MD4 are done to get better hash function MD5?
14. What do you mean by password aging? How online dictionary attacks differ from offline attacks?
15. What is the importance of Trap Door function in cryptography?
16. What are errors in Biometric? Explain.
17. How MAC differs from Hash? What is difference between authentication and authorization?
    Explain with examples.
18. What is meet in Middle Attack in Data Encryption Standard (DES)? Explain.