Information Security Question bank

* 1.Explain types of Attacks?
* 2.Explain model for network security?
* 3.Explain playfair cipher with one example?
* 4.What are the principles of security?.
* 5.Give an example to explain the concept of transposition ciphers in detail
* 6.Explain security mechanisms?
* 7.What are the principles of security?.
* 8Consider the following: Plaintext: “PROTOCOL” Secret key: “NETWORK” What is the corresponding cipher text using play fair cipher method?
* 9Explain any two block cipher modes of operation
* 10Explain RSA algorithm with suitable examples.
* 11Give the Differences between AES algorithm and DES algorithm?
* 12Explain the AES algorithm
* 13Compare block ciphers with stream cipher
* 14Explain ECB?
* 15Explain Block Cipher design principles.
* 16What are the principles of public key cryptosystems
* 17Explain Authentication requirements?
* 18Explain hash functions?
* 19List three approaches to Message Authentication.
* 20Explain HMAC?
* 21Explain Timing modification, Traffic analysis, Masquerade?
* 22Explain Message Authentication code?
* 23Explain Secure hash algorithm?
* 24Explain Digital signature?