1. So2al 3n l vigenere cipher => given: plaintext & key required=>ciphertext
2. malicious software types with brief description
3. DES diagram
4. Phases of operation of virus or worm
5. Characteristics of hash functions.
6. Difference between SSL session and SSL connection
7. Difference between Monoalphabetic and Polyalphabetic
8. Difference between Encryption and Steganography
9. Difference between confusion and diffusion
10. Difference between block and stream
11. So2al 3n el SSL bs msh fakro kan fe zy table (t2riban kan usage bta3t Change Cipher spec protocol , alert protocol, handshake protocol, SSL Record Protocol)
12. Key distribution with (certificate authority **I think**) diagram

13. In an RSA system, the public key of a given user is e = 31, n = 3599.What is the private key of this user?

14. So2al 3l modes:
    An error occurred in the fifth block what happens in (.., ..) block cipher modes

15. Kan fi so2al nktb el kelma eli bt-refer liha l gomla (lw had faker ay haga mnhom yb2a yktbhom)
    - Two block cipher modes allow preprocessing of key
    - Property that ensures received data is the same as that sent by the sender
    - Document that validates public key
16. What are SSL record services (with diagram **I THINK)**
17. Mention 3 attacks prevented by message authentication
18. MCQ:
    - Which polynomial is reducible in GF(2)
    - RSA find ciphertext given e, p, q, plaintext
    - RSA given e,n what is d?
    - Deffie- hellman
    - Which block cipher mode is used for short data
    - Digital signature is used for: verifying sender identity, in court ,prevent denial ,all
    - Given a block diagram of public key cryptosystem, does it provide auth, conf, integrity, all
    - Which block cipher error will not propagate
    - DES round: key size=? input size=?
19. T/F:
- If A wants to encrypt msg such that only B can read it, it will use public key of A
- Some block cipher modes can be used to generate stream ciphers

20. definition of honeypot