- What is the one-time pad cryptosystem? What is it used for?
- What is the main drawback of the one-time pad?
- You can encrypt 2^20 values in 1 second:
    - If the key is 40 bits long:
        - How long does it take to break it using brute force attack?
        - Mention a scenario where it's practical, another one where it's not practical.
    - If the key is 80 bits long:
        - How long does it take to break it?
        - Mention a scenario where it's practical, another one where it's not practical.
- Draw one round of DES.
- Explain Rail fence cipher, encrypt a plaintext using key (...)
- Mention modes of operation of DES (cbc, cfb,ctr,ecb,ofb)
- Draw OFB diagram.
- Write Needham equations. What is an obvious attack against it? How to counter it?
- HMAC: design objectives, what is the overhead over just using a hash function, diagram
- Draw HMAC block diagram and write all equations on it.
- SSL protocol stack Diagram.
- SSL Record Protocol operations and their security service.
- Write RSA equations and prove them, then given p, q calculate private and public keys.
- Write Diffie-Hellman's algorithm .
- Deffie-Helman suffers from man-in-the-middle attack, explain.
- Diffie-Hellman given q=71 and alpha= 7 , Xa=5 Xb=12 calculate Ya and Yb
- Types of malicious software, their description, and whether or not they need a host.
- Certificate requirements.
- Contents of certificate.
- Types of intruders and their descriptions.
- What is an Audit record? Why is it used?
- What is a Honeypot? How is it used?
- Playfair question (key = monarchy).
- How can two parties share a session key without having public keys (diagram).
- Mention the two techniques for detecting intruders and their description.
- Difference between SSL session and SSL connection
- Find (polynomial) mod (polynomial) in GF(2)
- MCQ:
    - Which of the following is reducible in GF(2):
        - X^3 + X^2 + 1
        - X^3 + 1
        - All of the above
        - **None of the above**
    - Gcd of 4321 and 1234 is??
    - RSA: if n=3599 and e=31 then d=?? **(factorize n: 59*61)**
    - RSA find ciphertext given e, p, q, plaintext
    - Deffie- hellman

  - Which block cipher mode is used for short data **ECB**
  - Digital signature is used for: verifying sender identity, in court ,prevent denial ,**all**
  - DES round: key size=? input size=?
  - Number of S-boxes
- T/F:
  - If A wants to encrypt msg such that only B can read it, it will encrypt it using public key of A? **(false: public key of B)**
  - Some block cipher modes can be used to generate stream ciphers?
  - Since hashing generates a text that is not readable it can provide confidentiality?
  - MAC can be used to provide both confidentiality and integrity?
- Write the term to which this definition refers:
  - Two block cipher modes allow the block cipher encryption function to be called before the data is available? **OFB & CTR**
  - Security requirement that ensures no one can read the data except the intende receiver? **Confidentiality**
  - Security requirement that ensures received data is the same as that sent by the sender **Integrity**
  - Document that validates public key?**Certificate**