1. What is the difference between block and stream cipher?
Block : Processes in fixed blocks of data (64 bit etc). Each block is independently encrypted.
Steam : Processes bit by bit or byte by byte. Encrypts by unit of data.
2. What is the difference between diffusion and confusion?
Diffusion : spreading influence of plaintext throughout the ciphertext, asin 1 bit change in plaintext results in multiple changes in ciphertext.
Confusion : Creating a highly non-linear, complex relationship / algorithm between the plaintext and ciphertext.
3. What are the parameters that define a simple Feistel cipher?
Block Size (n), Rounds (r,Key Schedule, rounding funct (f).
?-Subkey Gen and Data division
4. Why is DES considered less secure nowadays?
Uses a small key size and is vulnerable due to modern computing power.
-Exhaustive search attack (brute force).
5. Why is the AES algorithm considered better than the DES?
Supports longer key lengths (128,192,256 bits). No practical vulnerabilities. Efficient. Standardized.
6. Explain the avalanche effect in a crypto system.
A small change in input data results in a dramatic change in output. Creates unpredictable transformations. (aka high diffusion, moderate confusion)
7. What makes breaking the RSA algorithm so difficult by brute force?
Computational complexity of factoring large numbers. However, quantum computers can theoretically solve them nearly instantly, so we are researching a transition to vector-based encryption algorithms.
8. What is the fundamental difference between Hash values generated using digital signatures and ciphertext generated using encryption techniques like RSA and DES?
Hashing is one-way. Used for verification. Encryption is two-way, as the plaintext can be recovered with the same key and decrypting. Salting is adding characters to the plaintext, or along the obfuscation process. :p
9. How do Certification Authorities address limitations we find in Digital Signatures?
keys are bound to the identity of the cert holder. There is a hierarchy of trust, leading to root CA server. Has strict standards, with lots of timestamping.
10. Explain the difference between Stateless and Stateful packet filtering.
Both firewall/network security.
Stateless : Looks at individual packets, decides based on header info. Unaware of connection state. Faster.
Stateful : Considers connection state. Decisions based on communication context. More resource-intensive.
11. What is the difference between Firewalls and Intrusion Detection Systems?
Firewall : Barrier between trusted internal network and untrusted external networks. Controls and filters traffic based on rules.
IDS : monitors network activity for signs of malicious behavior. Does not block or allow traffic, just detects and alerts.

12. What is a Demilitarized Zone in a network?

A designated 'area' that acts asa buffer between an internal network and external network. Functions to segregate services and resources which need to be accessible from internal and external networks.

13. Explain each step in a single round of DES algorithm.

Initial Permutation : 64 bit block is rearranged according to the predefined permutation table.
Subkey Gen : 56-bit key is divided into 2 28-bit halves. Each half is circular left shifted, and combined to generate a 56-bit round subkey. Only used in current round.
Feistel function : 32-bit right-half of data block from first permutation is Fiestel function'd. [Expanded to 48 bits, XORed with round subkey, divided to 6-bit blocks, and substituted with 8 S-boxes. S-boxes are then permuted for 32-bit output.]
XOR left half w/ 32 bit right-half after Feistel.
Swap : Right and left halves are swapped, for next round.

14. Using the S-Box given below, explain what the output would be if the input is (ABC8E2193ACD) Given that in a sequence of 6 bits, the middle 4 bits represent column number and extreme two bits represent row number

= 1010 10,11 1100,1000 11,10 0010,0001 10,11 0011,1010 11,00 1101
=10=[2]0101=[5] = 6,5,12,1,1,11,9,13
=65C11B9D Output

15. Perform encryption and decryption using the RSA algorithm for the following terms. Show the steps for the process.

a. p = 3; q = 11; e = 7; m = 5

1. Key Gen n = pq = 33, (p-1)*(q-1)=20, 7 is coprime, d=3 (3*7 mod 20 = 1 mod 20) public key = (33,7) private = 3
2. Encrypt c = m^e mod n (5^7 mod 33) = 14 (ciphertext)
3. Decrypt m = c^d mod n = 14^3 mod 33 = 5

b. p = 5; q = 11; e = 3; m = 9

1. Key Gen n = pq = 55, (p-1)*(q-1)=40, 3 is coprime, d=27 (27*3 mod 40 = 1 mod 40) public key = (55,3) private = 27
2. Encrypt c = m^e mod n (9^3 mod 55) = 4 (ciphertext)
3. Decrypt m = c^d mod n = 4^27 mod 55 = 9