SA,

This is the questions someone of credit hours told me(if any on can classify each to its chapter as I dont know):

1)Play Fair (encrypt keyword)

Chapter 2

2)Draw Round of DES

Page 77

3)Draw Public Key Distr. (Authority or certificate)

Page 293,294

4)Draw Authentication and Secrecy

Fig 9.4 ---Page 265

5)Modes of DES

Ely homa el 5 modes ECB , CBC, CFB,Cipher Output Feedback, Cipher Counter

6)*6 requirements of public key*

Page 266

1. It is computationally easy for a party B to generate a pair (public key PUb, private key PRb).
2. It is computationally easy for a sender A, knowing the public key and the message to be encrypted, M, to generate the corresponding ciphertext:
C = E(PUb, M)
3. It is computationally easy for the receiver B to decrypt the resulting ciphertext using the private key to recover the original message:
M = D(PRb, C) = D(PRb, E(PUb, M))
4. It is computationally infeasible for an opponent, knowing the public key, PUb, to determine the private key, PRb.
5. It is computationally infeasible for an opponent, knowing the public key, PUb, and a ciphertext, C, to recover the original message, M.
6. The two keys can be applied in either order
M= D[Pub,E(PRb,M)]= D[PRb,E(Pub,M)]

7)Attacks that ccan be handled with MAC

Masquerade: Insertion of messages into the network from a fraudulent source. This includes the creation of messages by an opponent that are purported to come from an authorized entity. Also included are fraudulent acknowledgments of message receipt or nonreceipt by someone other than the message recipient. ***Content modification:*** Changes to the contents of a message, including insertion, deletion, transposition, and modification. ***Sequence modification:*** Any modification to a sequence of messages between parties, including insertion, deletion, and reordering. ***Timing modification:*** Delay or replay of messages. In a

connection-oriented application, an entire session or sequence of messages could be a replay of some previous valid session, or individual messages in the sequence could be delayed or replayed. In a connectionless application, an individual message (e.g., datagram) could be delayed or replayed.

8)Why Stream Cipher is not recommended to use same key?

If two plaintexts are encrypted with the same key using a stream cipher, then cryptanalysis is often quite simple. If the two ciphertext streams are XORed together, the result is the XOR of the original plaintexts. If the plaintexts are text strings, credit card numbers, or other byte streams with known properties, then cryptanalysis may be successful.

9)3 ways to do MAC

Encryption ,Mac , Hash Functio

10)Avalanche effect?

The avalanche effect is a property of any encryption algorithm such that a small change in either the plaintext or the key produces a significant change in the ciphertext.

11)Deffie Hellman(given q and a get x(a) 7aga zy kda)

Page 314 -------- prob 10.2

12)Requirements of strong hash fn.

1. H can be applied to a block of data of any size.
2. H produces a fixed-length output.
3. H(x) is relatively easy to compute for any given x, making both hardware and software implementations practical.
4. For any given value h, it is computationally infeasible to find x such that H(x) = h. This is sometimes referred to in the literature as the one-way property.
5. For any given block x, it is computationally infeasible to find $y \neq x$ with H(y) = H(x).
6. It is computationally infeasible to find any pair (x, y) such that H(x) = H(y).

13)Smallest number multiplied by 7 to get (2 mod 5) 7aga kda bardo

I think x=1

14)Problem on firewall to allow some addresses (fill a table of rules)

Page 627

15)Difference between SSL session and SSL connection

Connection: A connection is a transport (in the OSI layering model definition) that provides a suitable type of service. For SSL, such connections are peer-to-peer relationships. The connections are transient. Every connection is associated with

one session.
Session: An SSL session is an association between a client and a server. Sessions are created by the Handshake Protocol. Sessions define a set of cryptographic security parameters, which can be shared among multiple connections. Sessions are used to avoid the expensive negotiation of new security parameters for each connection.

16)SSL participants (short statement on each) and the set

Cardholder: In the electronic environment, consumers and corporate purchasers interact with merchants from personal computers over the Internet. A cardholder is an authorized holder of a payment card (e.g., MasterCard, Visa) that has been issued by an issuer. ***Merchant***: A merchant is a person or organization that has goods or services to sell to the cardholder. Typically, these goods and services are offered via a Web site or by electronic mail. A merchant that accepts payment cards must have a relationship with an acquirer. ***Issuer:*** This is a financial institution, such as a bank, that provides the cardholder with the payment card. Typically, accounts are applied for and opened by mail or in person. Ultimately, it is the issuer that is responsible for the payment of the debt of the cardholder. Acquirer: This is a financial institution that establishes an account with a merchant and processes payment card authorizations and payments. Merchants will usually accept more than one credit card brand but do not want to deal with multiple bankcard associations or with multiple individual issuers. The acquirer provides authorization to the merchant that a given card account is active and that the proposed purchase does not exceed the credit limit. The acquirer also provides electronic transfer of payments to the merchant's account. Subsequently, the acquirer is reimbursed by the issuer over some sort of payment network for electronic funds transfer. ***Payment gateway:*** This is a function operated by the acquirer or a designated third party that processes merchant payment messages. The payment gateway interfaces between SET and the existing bankcard payment networks for authorization and payment functions. The merchant exchanges SET messages with the payment gateway over the Internet, while the payment gateway has some direct or network connection to the acquirer's financial processing system. ***Certification authority (CA):*** This is an entity that is trusted to issue X.509v3 public-key certificates for cardholders, merchants, and payment gateways. The success of SET will depend on the existence of a CA infrastructure available for this purpose. As was discussed in previous chapters, a hierarchy of CAs is used, so that participants need not be directly certified by a root authority.

hope this helps