

**Answer any four questions. Circle below the questions you want me to grade. Failure to do so will result in the first four being graded and the fifth ignored.**

1   2   3   4   5

1. (a) With ECB mode of DES, if there is an error in a block of the transmitted cipher-text, only the corresponding plaintext block is affected. Is this also true for the CBC mode? If there is an error in the first cipher-text block,  $C_1$ , how does this affect the reconstruction of plaintext blocks  $P_1$ ,  $P_2$ , etc.
- (b) Describe what is triple DES? Comment on its security relative to DES.

2. (a) In the RSA cryptosystem, you intercept the ciphertext  $C = 10$  sent to a user whose public key  $e = 17$  and the modulus  $m = 35$ . What is the plaintext?
- (b) Suppose Alice and Bob are using the Diffie-Hellman Key exchange protocol. They choose the public modulo  $n = 101$  and the generator  $g = 2$ . Suppose Alice and Bob secretly choose  $x = 8$  and  $y = 10$  respectively. What is the secret key they can compute?

3. (a) Given the RSA parameters in the previous problem, what would be the signature for a message, whose hash value is 3.
- (b) What is the birthday paradox and the related birthday attack? What consequences does the birthday paradox have on the security of cryptographic hash functions and message digests.

4. The *wide-mouth frog* protocol for authentication and session key exchange using a Key Distribution Center (KDC) works as follows:

- Alice sends to KDC -  $ID_A, K_A(B, K_S)$ . Where  $ID_A$  is her ID,  $K_A$  is the private key she shares with the KDC and  $K_S$  is the desired session key.
- KDC sends to Bob -  $K_B(ID_A, K_S)$  where  $K_B$  is the private key Bob shares with the KDC.

- (a) Why is  $ID_A$  sent in plaintext along with the encrypted session key?
- (b) Show how this protocol cannot withstand a replay attack.
- (c) What would be a simple way of fixing the protocol against the replay attack.

5. Consider the following protocol for user authentication. Alice and the host share a secret key  $K_A$  which is communicated securely once at the outset. After that, every time Alice wants to log on she uses the following protocol:
- Alice sends to the host her ID and a nonce  $R_1$ .
  - The host returns a nonce  $R_2$  and also the encrypted nonce  $R_1$  using the secret key that the host shares with Alice, that is  $E_{K_A}(R_1)$ .
  - Alice returns  $E_{K_A}(R_2)$
- (a) Is the above protocol susceptible to a replay attack? Explain your answer.
- (b) Show how the above protocol is susceptible to a *reflection attack* where Oscar starts multiple instances of the protocol claiming he is Alice. He then uses information obtained from one instance to complete the other. So for example, Oscar initiates a log in and goes through the first two steps above. He then initiates a second instance using  $R_2$  as the nonce. Explain in more detail how the reflection attack will succeed.
- (c) Suggest how the protocol can be modified to resist this attack.