

The first four questions are mandatory. Question 5 is for extra credit. Note, no partial credit will be given for Question 5 and we recommend that you attempt it only after you are done with the first four. Also, the maximum grade for the exam is 100, irrespective of whether you get extra credit or not.

1. (25 pts)

(a) Recall that each iteration of DES is defined as follows:

$$L_i = R_{i-1}$$

$$R_i = L_{i-1} \oplus f(R_{i-1}, K_i)$$

Now suppose the function  $f()$  mapped every input to zero. Then what kind of output will this modified DES compute?

(b) Describe what is triple DES (two key and three key)? Comment on its security relative to DES. That is, how difficult is it to crack triple DES with a brute force attack?

2. (25 pts)

- (a) Alice has selected the public key ( $n = 33$ ;  $e = 13$ ). Bob wants to encrypt the plaintext message 6 and send it to Alice. What is the corresponding ciphertext?
- (b) What is Alice's private key  $d$ ?
- (c) Explain how you could use your answers to part a and b together to check your answers to those problems. (You don't have to actually do the computations; just explain what you'd do if you had enough time).
- (d) Explain why Alice's public key is a poor choice (for real-world encryption, not for an exam question) and what she needs to do differently to get a more secure key.

3. (25 pts)

- (a) State the 5 most important properties of cryptographic hash functions.
- (b) Message digests are reasonably fast, but here's a much faster function to compute. Take your message, divide it into 256-bit chunks (with appropriate padding)  $M_1, M_2, \dots, M_n$ . Then, XOR all chunks with odd indices together to compute  $B_1 = M_1 \oplus M_3 \oplus M_5 \oplus \dots$ , and all chunks with even indices together to compute  $B_2 = M_2 \oplus M_4 \oplus M_6 \oplus \dots$ . Now,  $B_1$  and  $B_2$  are both 256 bit long. Use these two blocks as an input for MD5. Is this a good collision-resistant hash function? Explain why or why not?

4. (25 pts)

- (a) Suppose Alice and Bob are using the Diffie-Hellman Key exchange protocol. They choose the public modulo  $n = 11$  and the generator  $g = 2$ . Suppose Alice and Bob secretly choose  $x = 5$  and  $y = 3$  respectively. What is the secret key they can compute? Give the value modulo 11.
- (b) Show how the Diffie-Hellman key agreement protocol is vulnerable to the man-in-the-middle attack.

5. (25 pts) **This is for extra credit and no partial credit will be given for it. Please attempt it only after you have finished the first four questions.**

The *Denning-Sacco* key exchange protocol uses a trusted third party *Trent*, who keeps a database of all the participants public keys. Also, all participants have a trusted copy of Trent's public key.

- (a) Alice sends a message to Trent with her identity and Bob's identity:  
 $A, B$ .
- (b) Trent sends Alice Bob's public key  $K_B$ , signed with Trent's private key. Trent also send Alice her own public key,  $K_A$  signed with his private key.  
 $S_T\{B, K_B\}, S_T\{A, K_A\}$ .
- (c) Alice sends Bob a random session key and a time-stamp, signed in her private key and encrypted in Bob's public key, along with signed public keys.  
 $E_B\{S_A\{K, T_A\}\}, S_T\{B, K_B\}, S_T\{A, K_A\}$ .
- (d) Bob decrypts Alice's message with his private key and then verifies Alice's signature with her public key. He checks to make sure that the time stamp is still valid.

At this point both Alice and Bob have the session key  $K$  and can communicate securely.

The problem with the above protocol is that Bob, after completing the protocol with Alice can immediately turn around and pretend to be Alice. This is done as follows:

- (a) Bob sends a message to Trent with his identity and Carol's identity:  
 $B, C$ .
- (b) Trent sends Bob Carol's public key  $K_C$ , signed with Trent's private key. Trent also sends Bob his own public key,  $K_B$  signed with his private key.  
 $S_T\{C, K_C\}, S_T\{B, K_B\}$ .
- (c) Bob sends Carol ....

Complete the above attack. Suggest how it can be fixed by adding additional information in the third step.