AMERICAN UNIVERSITY
LIBRARY
OF BEIRUT

AMERICAN UNIVERSITY
LIBRARY
OF BEIRUT

Final Exam
CMPS 396C: Computer Security
Fall 2004

Instructions. You have 90 minutes to complete the exam. You are **not** allowed to consult your books or notes during the exam. Make your answers clear and concise. Illegible answers will be marked wrong.

1. (5 pts) Consider the following protocol that involves both RSA public-key operations and DES shared-key operations. Suppose A has an RSA private key prv(A) and an RSA public key pub(A). Suppose that B has an RSA private key prv(B) and an RSA public key pub(B). And suppose that each of the parties, A and B, knows the RSA public key of the other party. A wants to send to B some message M. A selects a random DES key K and sends B the following two messages:

- RSA-ENC(RSA-SIG(K, prv(A)), pub(B)) , and
- DES(M, K)

The notations are: RSA-ENC(X, Y) is RSA encryption of text X with public key Y; RSA-SIG(X, Y) is RSA signature of the text X with private key Y; and DES(X, Y) is DES encryption of the text X with key Y. Consider the following three statements about this protocol.

1. Only B (and A) can decipher the contents of the message M.
2. B is certain that the message M arrived from A.
3. B can prove to a third party that the message M arrived from A.

Which combination of statements (1), (2), and (3) above is correct?

2. (5 pts) Consider the following shared-key authentication protocol between A and B. We assume that A and B share a long-term secret key K. A starts the protocol by sending its name to B. Then, B responds by sending a random number R back to A. Then, A sends to B the value h(K,R), where h is an agreed hash function. Finally, B replies to A with the value h(K,R+1). This protocol is repeated every time A initiates a communication with B. Which of the following statements about this protocol is correct?

a. A cannot deduce that she is speaking with the real B, but B can deduce that he is speaking with the real A.

b. B cannot deduce that he is speaking with the real A, but A can deduce that she is speaking with the real B.

c. A can deduce that she is speaking with the real B and B can deduce that he is speaking with the real A.

d. B cannot deduce that he is speaking with the real A and A cannot deduce that she is speaking with the real B.

3. (3 pts) Why isn't 3DES (EDE) with K1 = K2 = K3 used?

4. (6 pts) Suppose that a message which is 1,024 bits long is hashed. The hash value is 128 bits. You are given the hash and would like to find the message that hashes to it.

a. About how many guesses will it take?

b. What if the message is 128 bits long?

c. About how many guesses will it take to find 2 messages that hash to the same value?

5. (6 pts)

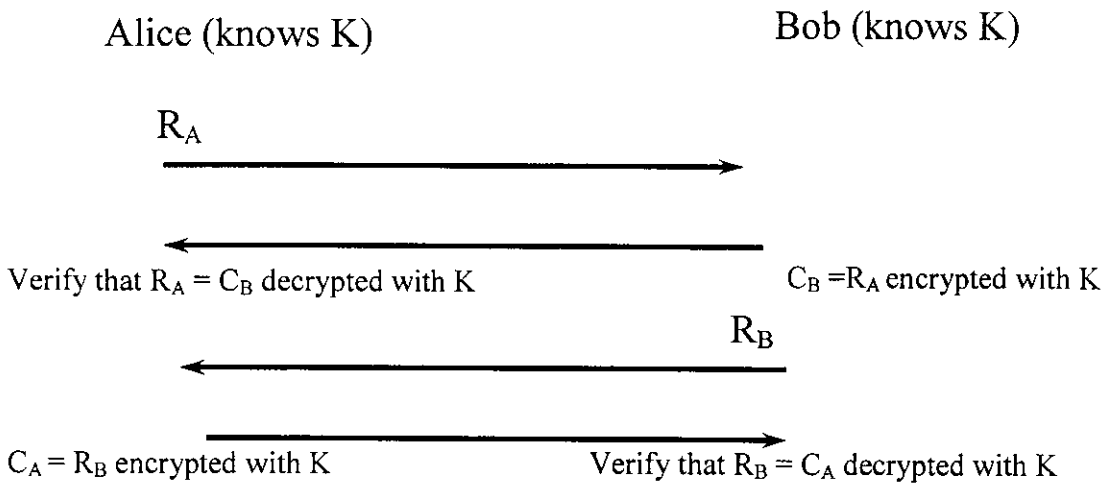
The security of encrypting using RSA is based on the difficulty of _____

The security of signing using RSA is based on the difficulty of _____

The security of exchanging keys using Diffie-Hellman is based on the difficulty of _____

6. (8 pts) Alice proposes the following way to confirm that Alice and Bob are both in possession of the same secret key. Bob creates a random bit string as long as the key, XORs it with the key, and sends the result to Alice. Alice XORs the incoming block with her key (which should be the same as Bob's key) and sends it back. Bob checks if it is equal to the original random string he selected. If so, then Bob has verified that Alice has the same secret key. In this scheme neither of the parties has ever transmitted the key in the clear. Is this scheme secure? Justify your answer.

7. (8 pts) Alice and Bob can authenticate each other using secret-key encryption as follows:



Assuming that Alice can open more than one connection to Bob, describe how she could authenticate herself to Bob without knowing K.

8. (10 pts) Give an argument on why the initial and final permutations in DES have no security value.

9. (13 points)
a) Describe why 2DES with same key is not much more secure than single DES.

b) Describe why 2DES with 2 keys is not much more secure than single DES. Assume that you have at least 2 known (PlainfText, Cipher) pairs.

10. (5 pts) Bob suspects that his private key d for using RSA has been compromised. Rather than generating a new n, he decides to generate a new d and e with the old n. Is this safe? Defend your answer.

11. (5 pts) What is the difference between a MAC and a plain hash? When would you use a MAC as opposed to a plain hash?

12. (5 pts) Alice wants to send a signed message to Bob using RSA. Alice's public and private keys are (e, n) and (d, n) respectively. Let M be the message and S the signature, then $S = M^d \bmod n$.
Since Bob knows M, n and S couldn't he just compute d?

13. (5 pts) Explain how non-repudiation could be guaranteed using a public-key scheme but not necessarily using a secret-key scheme. You can use an example.

14. (13 pts) Given Bob's RSA public key (e=7, n=187).
a) Knowing that (7*23 = 1 mod 160) find φ, p, q and d.
b) In a blinding attack, Alice wants Bob to sign message m' without knowing its content. She sends him m to sign instead of m'. Show how she can figure out the signature of m' without knowing d. Specifically, answer the following:

i) What should she send Bob to sign?
ii) What will Bob send her back?
iii) How would she extract the signature of m' from ii)

15. (3 pts) Alice wants to send Bob a very long message

$$M = M_1 + M_2 + \ldots + M_n$$

In order to authenticate the message, Alice uses the following method: Alice and Bob share a secret key K. Let H be a hash function. Let $N_j = H(M_{j+1})$ for $j=1..(n-1)$. Let $E_A(X)$ denote Alice's signature on the value 'X' (which Bob can verify).

Alice then sends Bob the message

$$N = E_K(N_0) + M_1 + N_1 + M_2 + \ldots + N_{n-1} + M_n .$$

When Bob receives this message, he checks Alice's signature on the first block. Is this method of message authentication secure? Justify your answer. (Assume H is safe).