CS255: Cryptography and Computer Security **Winter 2003**

Final Exam

Instructions
− Answer **four** of the following five problems. Do not answer more than four.
− The exam is open book and open notes. A calculator is fine, but a laptop is not.
− You have two hours.

Problem 1. Questions from all over.

a. Recall that in a typical signature scheme one signs a long message M by first computing a message digest, $H(M)$, and then signing the resulting digest. (1) Describe the minimum security property that the hash function should satisfy. (2) Describe a potential attack if the hash function does not satisfy this property.

b. Consider the set of integers $\{0, 1, \ldots, p-1\}$. This set defines a group by defining the group operation as addition modulo p. This group has order p. Is the discrete-log problem hard in this group? If so, explain why. If not, how would you solve discrete-log in this group?

c. Let E be some block cipher such as DES. Consider an encryption mode using E that is completely deterministic (i.e. no randomness is involved during encryption). Explain why this encryption mode is insecure (e.g., by explaining why it cannot be semantically secure).

d. Briefly explain what goes wrong if the same RC4 secret key is used to encrypt two distinct messages M_1 and M_2. You may assume the adversary sees both ciphertexts.

Problem 2. Quotable signatures. Suppose Alice sends Bob a signed email. Our goal is to design a signature scheme that will enable Bob to deduce a signature on a subset of the message. This will enable Bob to quote a signed paragraph from the email where the signature can be verified using only the quoted paragraph. Suppose the email M is a sequence of words $m_1 m_2 \ldots m_n$. The signature works as follows: (1) Alice has a private key for a standard signature scheme such as RSA, (2) to sign the message M Alice views these n words as leaves of a binary tree, (3) she computes a Merkle hash tree from these leaves (i.e. all pairs of words are hashed, then all pairs of hashes are hashed, etc.) and obtains the root hash at the top of the tree, (4) she signs this root hash using the standard signature scheme to obtain a signature S. Alice then sends M along with this signature S to Bob.

a. In one sentence explain how, given (M, S) and Alice's public key, Bob verifies Alice's signature S on M.

b. Suppose Bob wants to quote a paragraph from the message, namely a consecutive set of words $m_i m_{i+1} \ldots m_j$. Show that Bob can generate a signature on this paragraph that will convince a third party that the paragraph is from Alice. This signature will contain S plus at most $2\lceil \log n \rceil$ additional hashes. Explain how Carol verifies the signature on this quoted paragraph. Briefly explain why Alice's signature cannot be forged on a quotable paragraph, assuming that a proper hash function is used to construct the hash tree.

c. Suppose Bob wants to quote a subset of t words that are not necessarily consecutive. Using the method from (b) what is the worst-case length of the resulting signature as a function of t and n? In other words, what is the maximum number of hashes that Bob must provide so that a third party is convinced that these words came from Alice.

Problem 3. Repeated squaring.

a. The number $p = 521$ is prime. Use Euler's theorem to decide whether 2 is a quadratic residue modulo this p. Show all intermediate steps in your calculation.

b. The number $N = 1517$ factors as $N = 37 * 41$. Is 2 a quadratic residue modulo this N? Show all intermediate steps in your calculation.

Problem 4. Suppose user A is broadcasting packets to n recipients $B_1, \ldots, B_n$. Privacy is not important but integrity is. In other words, each of $B_1, \ldots, B_n$ should be assured that the packets he is receiving were sent by A. The broadcaster A decides to use a MAC.

a. Suppose user A and $B_1, \ldots, B_n$ all share a secret key k. User A MAC's every packet she sends using k. Each user B_i can then verify the MAC. Using at most two sentences explain why this scheme is insecure, namely, show that user B_1 is not assured that packets he is receiving are from A.

b. Suppose user A has a set $S = \{k_1, \ldots, k_m\}$ of m secret keys. Each user B_i has some subset $S_i \subseteq S$ of the keys. When A transmits a packet she appends m MAC's to it by MACing the packet with each of her m keys. When user B_i receives a packet he accepts it as valid only if all MAC's corresponding to keys in S_i are valid. What property should the sets $S_1, \ldots, S_n$ satisfy so that the attack from part (a) does not apply? We are assuming all users $B_1, \ldots, B_n$ are sufficiently far apart so that they cannot collude.

c. Show that when $n = 6$ (i.e. six recipients) the broadcaster A need only append 4 MAC's to every packet to satisfy the condition of part (b). Describe the sets $S_1, \ldots, S_6 \subseteq \{k_1, \ldots, k_4\}$ you would use.

Problem 5. Batch RSA.

a. Let $N = pq$ such that neither 3 or 5 divide $\varphi(N)$. We are given p, q and $M_1, M_2 \in \mathbb{Z}_N$. Show how to compute both $S_1 = M_1^{1/3} \bmod N$ and $S_2 = M_2^{1/5} \bmod N$ by just computing the 15'th root of $T = (M_1)^5(M_2)^3 \bmod N$ and doing a bit of extra arithmetic. In other words, show that given $T^{1/15} \bmod N$, it is possible to compute both S_1 and S_2 using a constant number of arithmetic operations modulo N.

b. Describe an algorithm for computing a 15'th root in $\mathbb{Z}_N$ using a single exponentiation (for N as in part (a)).

c. Explain how you would use this trick to produce two RSA signatures at about the same cost as producing a single signature. Describe the resulting signature scheme: (1) the key generation algorithm, (2) the signing algorithm (for signing two distinct messages) and signature format, and (3) the verification algorithm.

Your construction shows that RSA signatures can be generated in pairs faster than generating the signatures one-by-one.