CS255: Cryptography and Computer Security **Winter 2004**

Assignment #4

Due: Friday, March 12th. No late days allowed.

Problem 1. Certificate Revocation Trees (CRT's). Suppose Visa wants to use CRT's to help scale its creditcard validation process carried out at Point of Sale terminals. When a merchant wants to validate a creditcard number it communicates with a local Visa Validation Server (VVS). There are many VVS's all over the world. The VVS responds to the merchant with a message saying whether the given creditcard number is valid or invalid. Visa wants to use CRT's for this purpose. These CRT's are issued daily to all VVS's around the world from visa headquarters.

a. Consider an architecture where the only protection is that communication between a local VVS and a merchant is protected using SSL. What is the benefit of CRT's over this simple SSL based solution?

b. Suppose creditcard numbers are 4 digits long and the current list of revoked creditcards contains: $1234, 2435, 3651, 5621, 7243$.

- Explain how the VVS proves that 2435 is a revoked creditcard number.
- Explain how the VVS proves that 6542 is not revoked.

Describe exactly what values are sent from the VVS to the merchant (use H to denote the hash function).

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 collision resistant 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.