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

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. In class we showed that the one-time pad is malleable. Explain what that means.

b. For each of the following statements, say whether they are true or false and briefly explain why:

1. RSA signature generation is faster than RSA signature verification.
2. RSA decryption is faster than RSA encryption.

c. SSHv2 uses the following mechanism for combining symmetric encryption and MAC:

$$C = E_{k_1}(M) \| MAC_{k_2}(M) \tag{1}$$

Show that there exist a semantically secure encryption system (against a passive adversary) and an existentially unforgeable MAC for which the construction above is not semantically secure. Use a semantically secure encryption system $\overline{E}$ and a MAC that is existentially unforgeable, $\overline{MAC}$, as building blocks.
Hint: try changing $\overline{MAC}$ in a way that retains the security of the MAC, but would break semantic security of the construction in (1).

d. Why are RSA public keys so much longer than keys in a symmetric key system, for the same security? (e.g. 1024-bit RSA modulus vs. 128-bit AES keys).

Problem 2. (double encryption) Suppose Alice has a secret key $k_1 \in \{0,1\}^n$ and Bob has secret key $k_2 \in \{0,1\}^n$. They wish to encrypt a message M so that both their keys are needed for decryption. They are considering using a block cipher E using one of the following methods:

1. $C \leftarrow E_{k_1}[E_{k_2}[M]]$
2. $C \leftarrow E_{k_1 \oplus k_2}[M]$
3. $C \leftarrow (E_{k_1}[r], E_{k_2}[r \oplus M])$ where r is a fresh random string of the same length as M

For whichever method they use, the attacker will be given one message/ciphertext pair (M, C) and his goal is to decrypt some other ciphertext C'. We refer to (M, C, C') as the challenge to the attacker. You may assume the message M is long enough so that the pair (M, C) uniquely defines the keys (k_1, k_2) in methods (1) and (3). Note that exhaustive search for k_1, k_2 takes time 2^{2n}.

a. For all three methods the challenge (M, C, C') can be broken in approximately time 2^n (ignoring log factors). Explain how you would break the challenge for each method. Which method is the easiest to break?

b. Suppose the key length n is sufficiently large so that the attacks of part (a) are infeasible. Which of the three methods is the most efficient to use?

Problem 3. (authenticated Diffie-Hellman) We consider a natural protocol for Authenticated Diffie-Hellman Key Exchange. The goal is to provide mutual authentication with key exchange. We assume each party has a private signing key for some signature scheme and a certificate on the corresponding public key. The protocol proceeds as follows:

$$\begin{tikzcd}[column sep=huge]
 & \arrow[r, "g^x"] & & \\
A & & \arrow[l, "{g^y,\ B,\ CERT_B,\ SIG_B(g^x, g^y)}"'] & B \\
 & \arrow[r, "{A,\ CERT_A,\ SIG_A(g^x, g^y)}"] & &
\end{tikzcd}$$

The result is a shared secret $K_{AB} = g^{xy}$ from which the parties derive a session-key to encrypt and MAC all traffic between A and B.

a. Briefly explain the purpose of the signatures in the protocol above. What standard attack do they defend against?

b. Show that an active person-in-the middle, Eve, can interfere with the protocol so that at the end we have the following:

- A thinks that she is communicating securely with B (as required), but
- B thinks he is communicating securely with Eve.

In other words, B is fooled into thinking that the encrypted messages he is receiving (from A) are coming from Eve. Note that Eve cannot eavesdrop on the resulting encrypted channel. Briefly explain why your person-in-the-middle attack results in the confusion described above.

Hint: Eve does not modify the first two messages, but replaces the third message with something new. It relays all other messages unmodified. You may assume Eve also has a certificate, $CERT_E$, on her public signature verification key.

c. Briefly describe a hypothetical example of how Eve can use this attack to steal money from A. For example, suppose A makes money by giving expert advice in a private chat room run by B.

d. Propose a way to fix the protocol to defend against this attack. Explain why your fix prevents the attack from part (a).

Problem 4. (proxy cryptography) Let p be a prime. Suppose user Alice has two ElGamal private keys x_1 and x_2 and two corresponding ElGamal public keys $(g, y_1 = g^{x_1}) \in \mathbb{Z}_p^2$ and $(g, y_2 = g^{x_2}) \in \mathbb{Z}_p^2$. The first private key is stored on Alice's office machine while the second is on Alice's home machine. A mail gateway receives encrypted messages for Alice encrypted under one of the two public keys. If the incoming mail is encrypted under the first public key while Alice is at home, the gateway needs to "translate" the ciphertext to the second public key. If the incoming mail is encrypted under the second public key while Alice is at her office, the gateway needs to "translate" the ciphertext to the first public key. To enable the gateway to do so, Alice gives the gateway a secret derived from her two private keys.

a. Describe a trivial mechanism that enables the gateway to translate ciphertexts between the two public keys (this is not a trick question).

b. Now, suppose Alice does not want the gateway to be able to decrypt her incoming email. Show that Alice can give the gateway a secret derived from her two private keys that enables the gateway to translate ciphertexts between her two public keys without ever being able to decrypt the incoming email itself. Explain what is the secret given to the gateway and explain how the gateway uses the secret to translate ciphertexts in either direction between the two public keys. You may assume Alice's two private keys x_1 and x_2 are relatively prime to $p-1$ so that both x_1, x_2 are invertible modulo $p-1$.
Hint: the secret is just one value in $\{1, \ldots, p-1\}$ derived from x_1 and x_2. You only need to ensure that after translation the resulting ciphertext can be decrypted using the appropriate private key.
Recall that an ElGamal encryption of a message $m \in \{0,1\}^\ell$ under a public key $(g, y) \in \mathbb{Z}_p^2$ is $(g^r, m \oplus H(y^r))$. Here r is random in $\{1, \ldots, p-1\}$ and H is a hash function $H : \mathbb{Z}_p \to \{0,1\}^\ell$.

c. Briefly explain why the secret given to the gateway in part (b) reveals no information about the contents of incoming emails.

Problem 5. (incremental hashing) Let p be a prime and let $g \in \mathbb{Z}_p^*$ be an element of prime order q. We let G denote the group generated by g and we let I denote the set of integers $\{1, \ldots, q\}$. Fix n values $g_1, \ldots, g_n \in G$ and define the hash function $H : I^n \to G$ by

$$H(x_1, \ldots, x_n) = g_1^{x_1} g_2^{x_2} \cdots g_n^{x_n}$$

a. Show that H is collision resistant assuming discrete-log in G is intractable. That is, show that an attacker capable of finding a collision for H for a *random* $g_1, \ldots, g_n \in G$ can be used to compute discrete-log in G.
Hint: given a pair $g, h \in G$ your goal is to find an $\alpha \in \mathbb{Z}$ such that $g^\alpha = h$. Choose $g_1, \ldots, g_n \in G$ so that a collision on the resulting H will reveal α.

b. Let M be a message in I^n. Suppose user Alice already computed the hash of M, namely $H(m)$. Now, Alice changes only one coordinate of M to obtain a new message M'. Show that Alice can quickly compute $H(M')$ from $H(M)$ in time that is independent of the length of M.
You have just shown that after making a small change to a message there is no need to rehash the entire message. Collision resistant hash functions of this type are said to support *incremental hashing*.