CS255: Cryptography and Computer Security **Winter 2016**

Final Exam

Instructions:

- **Answer all six questions.**
- The exam is open book and open notes. Laptops are allowed with the network card turned off. Connecting to a network during the exam is a serious violation of the honor code.
- Students are bound by the Stanford honor code.
- You have two hours.

Problem 1. Questions from all over.

a. What is the difficulty with CRLs that is solved by the OCSP protocol?

b. Consider the following cipher (E, D) defined over $(\mathcal{K}, \mathcal{M}, \mathcal{C})$ where $\mathcal{C} = \mathcal{M} = \{0,1\}^\ell$ and $\mathcal{K}$ is the set of all $\ell!$ permutations of the set $\{0, \ldots, \ell - 1\}$. For a key $k \in \mathcal{K}$ and message $m \in \mathcal{M}$ define $E(k, m)$ to be the result of permuting the bits of m using the permutation k, namely

$$E(k, m) := m[k(0)]...m[k(\ell - 1)]$$

Show that this cipher is not semantically secure by showing an adversary that achieves advantage 1.

c. Let $\mathbb{G}$ be a group of prime order q with generator $g \in \mathbb{G}$. Let h be a random element in $\mathbb{G}$. In homework 3 you showed that the hash function $H(x, y) := g^x h^y$, from $\mathbb{Z}_q \times \mathbb{Z}_q$ to $\mathbb{G}$, is collision resistant, assuming the discrete-log problem in $\mathbb{G}$ is difficult. Show that H has a trapdoor: someone who knows the discrete-log of h base g can easily find collisions for H.

d. Let (E, D) be a semantically secure cipher. Suppose the plaintext message is compressed (using lossless compression) before encrypting it with E. Briefly explain why this compress-then-encrypt method can break semantic security. Make sure to describe a semantic security attacker.

Problem 2. Let $\pi : \mathcal{X} \to \mathcal{X}$ be a fixed public permutation (i.e., a one-to-one function) where $\mathcal{X} := \{0,1\}^n$. When we say that π is public we mean that anyone can compute $\pi(x)$ and $\pi^{-1}(x)$ for a given x in $\mathcal{X}$.
The Even-Mansour cipher (E, D) derived from π is defined as $E\big((k_0, k_1),\ m\big) := \pi(m \oplus k_0) \oplus k_1$.

a. Explain how $D\big((k_0, k_1),\ c\big)$ works.

b. Show that $E_1(k_1, m) := \pi(m) \oplus k_1$, with the corresponding D_1, is not a secure PRP.

c. Show that $E_2(k_0, m) := \pi(m \oplus k_0)$, with the corresponding D_2, is not a secure PRP.

Problem 3. Let us show that the Davies-Meyer construction may not be collision resistant when instantiated with a real-world block cipher. Let (E, D) be a block cipher defined over $(\mathcal{K}, \mathcal{X})$ where $\mathcal{K} = \mathcal{X} = \{0,1\}^n$. For $y \in \mathcal{X}$ let $\bar{y}$ denote the bit-wise complement of y.

a. Suppose that $E(\bar{k}, \bar{x}) = \overline{E(k,x)}$ for all keys $k \in \mathcal{K}$ and all $x \in \mathcal{X}$. The DES block cipher has precisely this property. Show that the Davies-Meyer construction, $h(k,x) := E(k,x) \oplus x$, is not collision resistant when instantiated with algorithm E.

b. Suppose (E, D) is an Even-Mansour cipher, $E(k,x) := \pi(x \oplus k) \oplus k$. Show that the Davies-Meyer construction instantiated with algorithm E is not collision resistant. As in the previous question, $\pi : \mathcal{X} \to \mathcal{X}$ is a fixed public permutation.

Problem 4. Double encryption. Let (E, D) be a cipher and define the cipher (E_2, D_2) as $E_2(k,m) = E\big(k, E(k,m)\big)$. One would expect that if encrypting a message once with E is secure then encrypting it twice as in E_2 should be no less secure.

a. Show that there is a (one-time) semantically secure cipher (E, D) such that (E_2, D_2) is not semantically secure.

b. Prove that for all CPA secure ciphers (E, D), the cipher (E_2, D_2) is also CPA secure. That is, show that for every CPA adversary $\mathcal{A}$ attacking (E_2, D_2) there is a CPA adversary $\mathcal{B}$ attacking (E, D) with about the same advantage and running time.

Problem 5. Let (Gen, S, V) be a secure signature scheme (existentially unforgeable under a chosen message attack) with message space $\{0,1\}^*$. Generate two signing/verification key pairs $(\mathrm{pk}_0, \mathrm{sk}_0) \leftarrow Gen$ and $(\mathrm{pk}_1, \mathrm{sk}_1) \leftarrow Gen$. Which of the following are secure signature schemes? Show an attack or explain why the scheme is secure, that is, explain why an attack on the scheme leads to an attack on (Gen, S, V).

a. Sign double: $S_1\big(\mathrm{sk}_0,\ m\big) := S(\mathrm{sk}_0,\ m\|m)$. Verify: $V_1\big(\mathrm{pk}_0,\ m,\ \sigma\big) := V(\mathrm{pk}_0,\ m\|m,\ \sigma)$

b. Accept one valid: $S_2\big((\mathrm{sk}_0, \mathrm{sk}_1),\ m\big) := \big(S(\mathrm{sk}_0, m),\ S(\mathrm{sk}_1, m)\big)$. Verify:

$$V_2\big((\mathrm{pk}_0, \mathrm{pk}_1),\ m,\ (\sigma_0, \sigma_1)\big) = \text{`accept'} \iff \big[V(\mathrm{pk}_0, m, \sigma_0) = \text{`accept'} \quad \text{or} \quad V(\mathrm{pk}_1, m, \sigma_1) = \text{`accept'}\big]$$

c. Sign halves: $S_3\big((\mathrm{sk}_0, \mathrm{sk}_1),\ (m_\mathrm{L}, m_\mathrm{R})\big) := \big(S(\mathrm{sk}_0, m_\mathrm{L}),\ S(\mathrm{sk}_1, m_\mathrm{R})\big)$

$$V_3\big((\mathrm{pk}_0, \mathrm{pk}_1),\ (m_\mathrm{L}, m_\mathrm{R}),\ (\sigma_0, \sigma_1)\big) = \text{`accept'} \iff V(\mathrm{pk}_0, m_\mathrm{L},\ \sigma_0) = V(\mathrm{pk}_1, m_\mathrm{R},\ \sigma_1) = \text{`accept'}$$

d. Sign with randomness: for $m \in \{0,1\}^n$ do

$S_4\big(\mathrm{sk}_0,\ m\big) := \big[\text{choose random } r \leftarrow \{0,1\}^n,\ \text{ output } \big(r,\ S(\mathrm{sk}_0,\ m \oplus r),\ S(\mathrm{sk}_0,\ r)\big)\ \big]$.

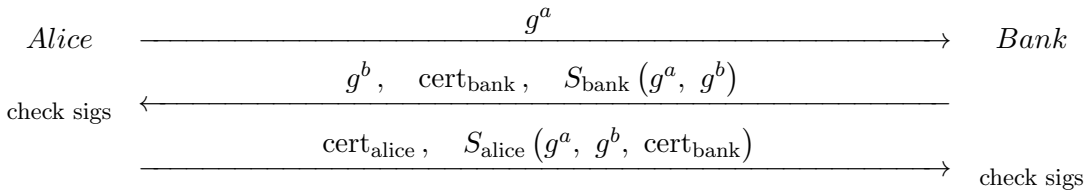
$V_4\big(\mathrm{pk}_0,\ m,\ (r, \sigma_0, \sigma_1)\big) = \text{`accept'} \iff V(\mathrm{pk}_0,\ m \oplus r,\ \sigma_0) = V(\mathrm{pk}_0,\ r,\ \sigma_1) = \text{`accept'}$

e. Sign with appendage:

$$S_5\big(\mathrm{sk}_1,\ m\big) := S(\mathrm{sk}_1,\ m\|1010) \quad ; \quad V_5\big(\mathrm{pk}_1,\ m,\ \sigma\big) := V(\mathrm{pk}_1, m\|1010,\ \sigma)$$

Problem 6. Authenticated key exchange (AKE). In lecture we saw a one-sided AKE with forward-secrecy and a two-sided AKE without forward-secrecy. Let's try to construct the best of both worlds: a two-sided AKE with forward-secrecy.

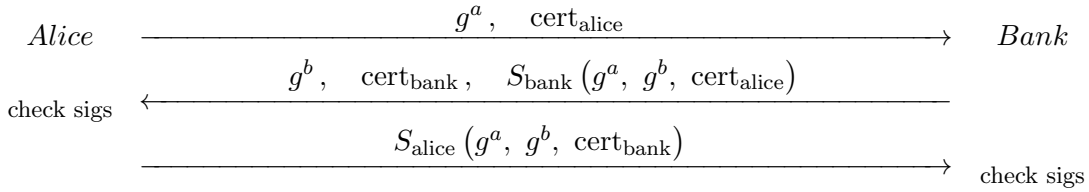
Consider the following two-sided AKE with forward-secrecy between Alice and Bank: They each have a certificate for a signing key and we denote by $S_{\text{alice}}(\text{data})$ and $S_{\text{bank}}(\text{data})$ their respective signatures on 'data'. They fix a group $\mathbb{G}$ of order q and generator $g \in \mathbb{G}$. Alice chooses a random a and Bank chooses a random b, both in $\mathbb{Z}_q$. They exchange the following messages:



Both sides compute the shared secret $k \leftarrow g^{ab} \in \mathbb{G}$ and each side deletes its secret a or b. If all the certificates and signatures verify correctly then Alice thinks she is speaking with Bank and Bank thinks it is speaking with Alice. The protocol provides forward-secrecy because a compromise of the server or the client does not compromise past sessions.

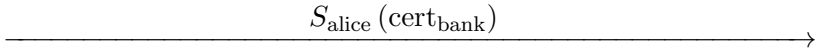
a. Since the Diffie-Hellman messages in this protocol are signed by the participants, one might expect that the protocol is secure against a man-in-the-middle attack. Unfortunately that is incorrect: show that the protocol is vulnerable to an identity misbinding attack.
Hint: The attacker can cause the protocol to complete successfully with Alice thinking she is speaking to Bank, but Bank thinks it is speaking to the attacker.

b. The protocol above can be repaired by sending $\text{cert}_{\text{alice}}$ in the first flow and having the Bank sign $\text{cert}_{\text{alice}}$ in the second flow as follows:



Both sides compute the shared secret $k \leftarrow g^{ab} \in \mathbb{G}$ and each side deletes its secret a or b. If all the certificates and signatures verify correctly then Alice thinks she is speaking with Bank and Bank thinks it is speaking with Alice. This prevents the attack above and is a secure two-sided AKE with forward-secrecy.

Suppose the third flow in this protocol is replaced with the following message:



Show that it is now possible to mount a key exposure attack: the attacker can establish a session with Bank where the attacker knows the session-key, but Bank thinks it is talking to Alice.