Name: **Roll no:**

Quiz 2

Cryptography & Network Security I
CS 406: Spring 2018

April 21, 2018

[**Total: 100 pts | 3 hours**]

1. **Perfect Secrecy.** [10 pts]

   Let $\mathcal{M}$ be the message-space, $\mathcal{K}$ the key-space and $\mathcal{C}$ the ciphertext-space of a perfectly secure one-time SKE scheme (with deterministic decryption). For $c \in \mathcal{C}$, let $M(c) \subseteq \mathcal{M}$ be the set of messages that the ciphertext c can be decrypted to, based on all possible keys. That is, $M(c) = \{m \in \mathcal{M} \mid \exists K \in \mathcal{K} \text{ s.t. } \mathsf{Dec}_K(c) = m\}$.

   In each of the following, fill in the blank **and justify your answer**.

   (a) For every $c \in \mathcal{C}$ which the encryption operation can result in, $M(c) =$ ____________________.

   (b) For every $c \in \mathcal{C}$, $|M(c)|$ ______ $|\mathcal{K}|$ (choose from $=$, $\leq$ and $\geq$).

   (c) From the above, derive a comparison between $|\mathcal{K}|$ and $|\mathcal{M}|$. ______________________________.

2. **Proof of Security: Domain Extension of a MAC** [20 pts]

This problem requires you to prove the security of domain extension of MACs using a Weak CRHF, as discussed in class.[1]

Specifically, suppose M is a secure MAC on k bit messages, with keys drawn uniformly from a key-space $\mathcal{K}$, and $\mathcal{H}$ is a weak CRHF with functions that map arbitrarily long messages to k bit digests. Show that M^* defined as follows, with keys drawn uniformly from $\mathcal{K} \times \mathcal{H}$, is a secure MAC for arbitrarily long messages.

$$\mathsf{M}^*_{K,h}(m) = \mathsf{M}_K(h(m)).$$

[1] Recall the security definition for a weak CRHF $\mathcal{H}$. For any PPT adversary A, $\Pr_{h \leftarrow \mathcal{H}}[A^h() \rightarrow (x, y) \wedge h(x) = h(y)]$ should be negligible. Note that A is given only oracle access to h.

3. **Finding Collisions** [25 pts]

   (a) Given a CRHF $\mathcal{H}$ that compresses $2k$ bit strings to k bit strings, we attempt to define a new CRHF $\mathcal{H}'$ that compresses $3k+1$ bit strings to k bit strings, as follows. For each function h in $\mathcal{H}$, we define a function h' as follows (where x, y, z are k bits each, and b is a single bit):

$$h'(b||x||y||z) = \begin{cases} h(x||h(y||z)) & \text{if } b = 0 \\ h(h(x||y)||z) & \text{if } b = 1 \end{cases}$$

   Show that $\mathcal{H}'$ is not collision resistant.

(b) Recall that NMAC (on which HMAC is based) has the form of M* from Problem 2, where the weak CRHF $\mathcal{H}$ is designed using a "compression function" $f : \{0,1\}^{2k} \to \{0,1\}^k$. $\mathcal{H}$ consists of functions h_K defined using k-bit keys K, that can be applied to messages consisting of an integral number of k-bit blocks, as follows:

$$h_K(m_1, \ldots, m_n) = f(f(f(\ldots f(f(K||m_1)||m_2)|| \ldots ||m_{n-1})||m_n)||\langle n \rangle),$$

where $\langle n \rangle$ denotes an encoding of n as a k-bit string. Suppose we change this construction as follows:

$$h_K(m_1, \ldots, m_n) = f(f(f(\ldots f(f(m_1||m_2)||m_3)|| \ldots ||m_n)||\langle n \rangle)||K).$$

Show that $\mathcal{H}$ redefined as above will not be a weak CRHF given a PPT adversary that knows a collision for f.

Name: **Roll no:**

4. **Extended Euclidean Algorithm** [25 pts]

   (a) Suppose $n = pq$, where p, q are distinct primes. Give an isomorphism between $\mathbb{Z}_n$ and $\mathbb{Z}_p \times \mathbb{Z}_q$, and show that it can be efficiently computed in both directions given p, q.[2]

   You may use the fact that given p, q, two integers a, b such that $ap + bq = 1$ can be found efficiently, using the Extended Euclidean algorithm.

[2] Recall that an isomorphism $\phi : \mathbb{Z}_n \to \mathbb{Z}_p \times \mathbb{Z}_q$ is a bijection such that $\phi(x + y) = \phi(x) + \phi(y)$ and $\phi(xy) = \phi(x) \cdot \phi(y)$. The operations in $\mathbb{Z}_p \times \mathbb{Z}_q$ are defined coordinate-wise, using operations in $\mathbb{Z}_p$ and $\mathbb{Z}_q$ respectively.

(b) Describe an efficient algorithm which, when given distinct primes p, q, and an integer $e \in \mathbb{Z}^*_{\varphi(n)}$, where $n = pq$ and φ denotes the Euler totient function, finds $e^{-1} \in \mathbb{Z}^*_{\varphi(n)}$. You should explicitly specify all uses of the Extended Euclidean algorithm in your algorithm.

5. **Establishing a MAC key** [10 pts]

   Suppose Alice and Bob have generated signing/verification key pairs (SK_A, VK_A) and (SK_B, VK_B) for a digital signature scheme, and have already shared their verification keys with each other. Give a *2-message protocol* for them to establish a MAC key for future communication over an adversarial network. You may use a CPA secure PKE scheme in addition to the above digital signature. (No definition or proof of security is needed.)

6. **Multiple Choice and fill in the blanks.** [10 pts]

(a) The main difference between CPA and CCA security for PKE is that, in the latter, the adversary is given access to

____.

(b) Match the following schemes to their purpose, by writing one or more of the choices from the right hand column against the entries in the left hand column.

i. Merkle tree ____________________

ii. Cipher-Block Chaining ____________________

iii. Counter mode ____________________

iv. 2-Universal Hash Function ____________________

(a) Randomness extraction

(b) Domain extension for Weak PRF

(c) Domain extension for SKE

(d) Domain extension for CRHF

(e) Statistically secure one-time MAC

(c) Which of the following problems does DNS-over-TLS address:

□ Anyone can read a DNS query.

□ Anyone can respond to a DNS query with a wrong IP address.

□ A corrupt name server could respond with a wrong IP address.

□ A corrupt name server could pretend that a domain name is absent.

□ None of the above.

Scratch space