Fundamentals of Cryptography: Problem Set 6

Due Wednesday Oct 30, 3PM

Collaboration is permitted (and encouraged); however, you must write up your own solutions and acknowledge your collaborators.

Problem 0 Read Section 4, 5 of "Introduction to Modern Cryptography (2nd ed)" by Katz & Lindell **or** Section 6, 7.1–7.3, 8.1–8.5, 8.9, 9.1–9.4 of "A Graduate Course in Applied Cryptography" by Boneh & Shoup.

You are also recommended to read the rest of Section 9 of "A Graduate Course in Applied Cryptography", which includes quite a few examples of real world attacks.

Problem 1 (2pt) Let MAC be the authentication algorithm of a secure MAC scheme, and let MAC be deterministic. Consider a randomized algorithm

$$\mathsf{MAC}'(k, m) = (r, \mathsf{MAC}(k, r), \mathsf{MAC}(k, m \oplus r)).$$

Formally, $\mathsf{MAC}'(k, m)$ samples a random string r that is as long as m, and outputs $(r, \mathsf{MAC}(k, r), \mathsf{MAC}(k, m \oplus r))$. Choose the strongest correct statement, and briefly explain your answer.

A. MAC' must be the authentication algorithm of a strongly secure MAC scheme.

B. MAC' must be the authentication algorithm of a secure MAC scheme.

C. MAC' is poly-time computable.

Problem 2 (4pt) Function $E : \{0,1\}^* \to \{0,1\}^*$ is a *prefix-free encoding* if

- E can be computed by a polynomial-time algorithm;
- There exists an efficient decoding algorithm D, such that for any $x \in \{0,1\}^*$, we have $D(E(x)) = x$;
- For any distinct $x, x' \in \{0,1\}^*$, $E(x)$ is not a prefix of $E(x')$.

(More generally, we may define the encoding as $E : \mathcal{X}^* \to \mathcal{Y}^*$, where $\mathcal{X}, \mathcal{Y}$ are the source alphabet and target alphabet.)

Part A. Show that $E(x) = 0^{|x|}1x$ is a prefix-free encoding.

Part B. Construct a prefix-free encoding such that $|E(x)| = |x| + O(\log |x|)$.

Part C. Is there a prefix-free encoding such that $|E(x)| = |x| + o(\log |x|)$? Prove your answer.

Part D. For a given integer λ, construct a prefix-free encoding such that for any x whose length is less than $2^\lambda - 1$, we have $|E(x)| \le |x| + 2\lambda$ and $|E(x)|$ is a multiple of λ.

Problem 3 (6pt) A keyed function $F : \{0,1\}^\lambda \times \{0,1\}^* \to \{0,1\}^\lambda$ is a *prefix-free PRF* if for any PPT distinguisher $\mathcal{D}$, the distinguisher cannot distinguish the following real world and ideal world with non-negligible advantage, under an additional restriction that the distinguisher $\mathcal{D}$ cannot make two queries x_i, x_j such that x_i is a prefix of x_j.

Real world:

$\mathcal{D}$ is given 1^λ as input.

The challenger samples a random key $k \leftarrow \{0,1\}^\lambda$.

For $i \leq \text{poly}(\lambda)$:
$\mathcal{D}$ sends the challenger an input x_i;
the challenger replies $F(k, x_i)$.

Ideal world:

$\mathcal{D}$ is given 1^λ as input.

The challenger samples a random function $f : \{0,1\}^* \to \{0,1\}^\lambda$.

For $i \leq \text{poly}(\lambda)$:
$\mathcal{D}$ sends the challenger an input x_i;
the challenger replies $f(x_i)$.

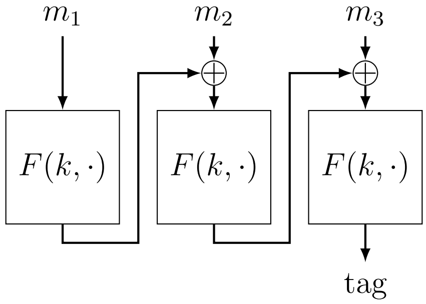

Figure 1: Basic CBC-MAC

Part A. Let $F : \{0,1\}^\lambda \times \{0,1\}^\lambda \to \{0,1\}^\lambda$ be a secure PRF. Prove that the basic CBC-MAC (illustrated in Figure 1)

$$F_{\text{CBC}}(k, (m_1, m_2, \ldots, m_\ell)) := \begin{cases} F(k, m_\ell \oplus F_{\text{CBC}}(k, (m_1, m_2, \ldots, m_{\ell-1}))), & \text{if } \ell > 1 \\ F(k, m_1), & \text{if } \ell = 1 \end{cases}$$
$$= F(k, m_\ell \oplus F(k, m_{\ell-1} \oplus \ldots F(k, m_2 \oplus F(k, m_1)) \ldots)).$$

is a prefix-free PRF. Since F_{CBC} is only defined on inputs whose length is a positive multiple of λ, we assume the distinguisher only queries such messages.

Part B. Let E be the prefix-free encoding in Problem 2 Part D. Show that $\mathsf{MAC}(k, x) := F_{\text{CBC}}(k, E(x))$ (together with uniform key generation and canonical verification) is a strongly secure MAC.

Problem 4 (5pt, Exercise 4.25 from KL) Let $F : \{0,1\}^\lambda \times \{0,1\}^\lambda \to \{0,1\}^\lambda$ be a strong PRP, and define the following encryption scheme (for fixed-length messages): On input a message $m \in \{0,1\}^{\lambda/2}$ and a key $k \in \{0,1\}^\lambda$, algorithm Enc samples an uniform $r \in \{0,1\}^{\lambda/2}$ and computes ciphertext $c := F_k(m \| r)$. Prove that this scheme is CCA2-secure[1], but is not an authenticated encryption scheme.

[1] CCA2 is the stronger CCA security.

Problem 5 (6pt, Exercise 8.20 from BS) The security analysis of HMAC assumes that the underlying compressing function is a *dual PRF*. Function $\hat{F} : \{0,1\}^n \times \{0,1\}^n \to \{0,1\}^n$ is a dual PRF if

- $\hat{F}$ is a PRF, and
- $\hat{F}'(k, x) := \hat{F}(x, k)$ is also a PRF.

Let $F : \{0,1\}^n \times \{0,1\}^n \to \{0,1\}^n$ be a PRF. We wish to build a dual PRF $\hat{F}$. This $\hat{F}$ can be used as a building block for HMAC.

Part A Show that, the most natural construction $\hat{F}(x, y) := F(x, y) \oplus F(y, x)$ is insecure: there exists a secure PRF F such that $\hat{F}$ is not a PRF.

Part B Let $g : \{0,1\}^n \to \{0,1\}^{2n}$ be a PRG. Let g_0, g_1 denote the first n-bit and the last n-bit of g, that is, $g(x) = g_0(x) \| g_1(x)$. Define $\hat{F}$ as

$$\hat{F}(x, y) = F(g_0(x), g_1(y)) \oplus F(g_0(y), g_1(x)).$$

Prove that $\hat{F}$ is a dual PRF if we additionally assume g_1 is collision resistant.

Remark: By definition, g_1 is not a CRHF because it is not compressing. Assuming the existence of OWP, it is not hard to construct a PRG g such that g_1 is a OWP (thus collision resistant).

Problem 6 (6pt, Exercise 7.15 from BS) Composing universal hash functions We say that a keyed hash function H defined over $(\mathcal{K}, \mathcal{M}, \mathcal{T})$ is an ε-bounded universal hash function, or ε-UHF, if for any distinct $m_0, m_1 \in \mathcal{M}$

$$\Pr_{k \leftarrow \mathcal{K}}[H(k, m_0) = H(k, m_1)] \leq \varepsilon.$$

Similarly, we say H is an ε-bounded difference unpredictable function, or ε-DUF, if for any distinct $m_0, m_1 \in \mathcal{M}$ and any $\delta \in \mathcal{T}$

$$\Pr_{k \leftarrow \mathcal{K}}[H(k, m_0) - H(k, m_1) = \delta] \leq \varepsilon.$$

(Here we assume $\mathcal{T}$ has algebraic structure.) We use these definitions to analyse the security of a composed universal hash function.

Let H_1 be a keyed hash function defined over $(\mathcal{K}_1, \mathcal{X}, \mathcal{Y})$. Let H_2 be a keyed hash function defined over $(\mathcal{K}_2, \mathcal{Y}, \mathcal{Z})$. Let H be the keyed hash function defined over $(\mathcal{K}_1 \times \mathcal{K}_2, \mathcal{X}, \mathcal{Z})$ as

$$H((k_1, k_2), x) := H_2(k_2, H_1(k_1, x))$$

Part A Show that if H_1 is an ε_1-UHF and H_2 is an ε_2-UHF, then H is an $(\varepsilon_1 + \varepsilon_2)$-UHF.

Part B Show that if H_1 is an ε_1-UHF and H_2 is an ε_2-DUF, then H is an $(\varepsilon_1 + \varepsilon_2)$-DUF.