Cryptography

Problem set 4

Problem 1 Let F be a pseudorandom function $F : \{0,1\}^n \times \{0,1\}^n \to \{0,1\}^n$. Let G_i : be the result of applying i round Feistel network for a .

1. show that for all $i \geq 1$, $G_{F,i} : \{0,1\}^{2n} \to \{0,1\}^{2n}$ is a permutation.
2. show that $G_{F,1}$ is not PRF/PRP.
3. show that $G_{F,2}$ is not PRF/PRP.
4. show that $G_{F,3}$ is not PRP.

Problem 2 Let F be a pseudorandom function. The fixed-length MAC for messages of length n is defined as follows:

Gen: on input 1^n, choose $k \leftarrow \{0,1\}^n$ uniformly at random,

Mac: on input a key $k \in \{0,1\}^n$ and a message $m \in \{0,1\}^n$, output the tag $t := F_k(m)$.

Vrfy: on input a key $k \in \{0,1\}^n$, a message $m \in \{0,1\}^n$, and a tag $t \in \{0,1\}^n$, output 1 if and only if $t = F_k(m)$.

Show that the above construction is a fixed-length MAC for messages of length n and that is existentially unforgeable under an adaptive chosen-message attack.

Problem 3 (CBC-MAC) Let F be a pseudorandom function. The basic, fixed-legnth CBC-MAC construction is as follows:

Gen: on input 1^n, choose $k \leftarrow \{0,1\}^n$ uniformly at random,

Mac: on input a key $k \in \{0,1\}^n$ and a message m of length $l \cdot n$ do the following:

1. Parse m as $m = m_1, \ldots, m_l$ where each m_i is of length n and set $t_0 = 0^n$.
2. For $i = 1$ to l, set $t_i = F_k(t_{i-1} \oplus m_i)$.

Output t_l as the tag.

Vrfy: on input a key $k \in \{0,1\}^n$, a message $m \in \{0,1\}^{ln}$, and a tag $t \in \{0,1\}^n$, output 1 if and only if $t = \mathsf{Mac}_k(m)$.

Show that the above construction is a fixed-length MAC for messages of length n and that is existentially unforgeable under an adaptive chosen-message attack.

Problem 4 Show that the above construction is not secure if messages can be of arbitrary lenght.

Problem 5 Let Mac' be the following modification of basic CBC-MAC: instead of selecting $t_0 = 0^n$, t_0 is selected uniformly at random, *i.e.,* for message $m = m_1, \ldots, m_l$, a tag is computed as:

- $t_0 \leftarrow \{0,1\}^n$ is selected uniformly at random,
- the tag is $\langle t_0, t_l \rangle$.

Show that Mac' is forgeable, even if the length of messages is fixed.

Problem 6 Say $\Pi = \langle \mathsf{Gen}, \mathsf{Mac}, \mathsf{Vrfy} \rangle$ is a secure MAC and for $k \in \{0,1\}^n$ the tag-generation algorithm Mac_k always outputs tags of length $t(n)$. Prove that t must be super-logarithmic or, equivalently, that if $t(n) = \mathcal{O}(\log n)$ then Π cannot be a secure MAC.

Hint: consider the probability of randomly guessing a valid tag.

Problem 7 Let F be a pseudorandom function. Show that the following MAC for messages of length $2n$ is secure/insecure.

The shared key is a random $k \in \{0,1\}^n$. To authenticate a message $m_1||m_2$ with $|m_1| = |m_2| = n$, compute the tag $\langle F_k(m_1), F_k(F_k(m_2))\rangle$.

Problem 8 Let F be a pseudorandom function. Show that each of the following message authentication codes is insecure.

1. To authenticate a message $m = m_1||\cdots||m_l$, where $m_i \in \{0,1\}^n$, compute $t \leftarrow F_k(m_1) \oplus \ldots \oplus F_k(m_l)$.
2. To authenticate a message $m = m_1||\cdots||m_l$, where $m_i \in \{0,1\}^n$, choose $r \leftarrow \{0,1\}^n$ at random, compute $t \leftarrow F_k(r) \oplus F_k(m_1) \oplus \ldots \oplus F_k(m_l)$ and send $\langle r, t\rangle$.
3. To authenticate a message $m = m_1||\cdots||m_l$, where $m_i \in \{0,1\}^{n/2}$, choose $r \leftarrow \{0,1\}^n$ at random, compute $t \leftarrow F_k(r) \oplus F_k(<1>||m_1) \oplus \ldots \oplus F_k(<l>||m_l)$ where $<i>$ is an $n/2$-bit encoding of the integer i and send $\langle r, t\rangle$.

Problem 9 Let $\pi = \langle \mathsf{Gen}(), \mathsf{Enc}(), \mathsf{Dec}()\rangle$ be a CPA-secure encryption scheme and $\gamma = \langle \mathsf{Gen}_{MAC}(), \mathsf{Mac}(), \mathsf{Vrf}$ be an existentially unforgeable MAC scheme. Let π' be the following encryption scheme:

- $\mathsf{Gen}(')1^n$:
  - $k_{enc} \leftarrow \mathsf{Gen}(1^n)$
  - $k_{mac} \leftarrow \mathsf{Gen}_{MAC}(1^n)$
  - $k = \langle k_{enc}, k_{mac}\rangle$

Consider the following cases:

(a) $\mathsf{Enc}_k(m) = \langle c, t\rangle$ where $c = \mathsf{Enc}_{k_{enc}}(m)$; $t = \mathsf{Mac}_{k_{mac}}(m)$

(b) $\mathsf{Enc}_k(m) = \langle c\rangle$ where $t = \mathsf{Mac}_{k_{mac}}(m)$ and then $c = \mathsf{Enc}_{k_{enc}}(m||t)$;

(c) $\mathsf{Enc}_k(m) = \langle c, t\rangle$ where $c = \mathsf{Enc}_{k_{enc}}(m)$; $t = \mathsf{Mac}_{k_{mac}}(c)$;

For each of them tell it the resulting scheme is CCA-secure?