Homework 2

Due date: Friday, Feb 17th 11:30 AM

Question 1 (20 points)

Let F be a pseudorandom permutation, and define a fixed-length encryption scheme (Enc, Dec) as follows: On input $m \in \{0,1\}^{n/2}$ and key $k \in \{0,1\}^n$, algorithm Enc chooses a uniform string $r \in \{0,1\}^{n/2}$ of length $n/2$ and computes $c := F_k(r||m)$.

Show how to decrypt, and prove that this scheme is CPA-secure for messages of length $n/2$.

Question 2 (20 points)

For any function $g : \{0,1\}^n \to \{0,1\}^n$, define $g^{\$}(.)$ to be a probabilistic oracle that, on input 1^n, choose uniform $r \in \{0,1\}^n$ and return (r, g(r)). A keyed function F is a *weak pseudorandom function* if for all PPT algorithm D, there exists a negligible function **negl** such that:

$$\left|\Pr[D^{F_k^{\$}(.)}(1^n) = 1] - \Pr[D^{f^{\$}(.)}(1^n) = 1]\right| \leq negl(n) \tag{1}$$

where $k \in \{0,1\}^n$ and $f \in Func_n$ and chosen uniformly.

1. Let F' be a pseudorandom function, and define

$$\mathrm{F_k(x)} \stackrel{\mathrm{def}}{=} \begin{cases} \mathrm{F'_k(x)} & \text{if x is even} \\ \mathrm{F'_k(x+1)} & \text{if x is odd} \end{cases} \tag{2}$$

   Prove that F is weakly pseudorandom.

2. Is CTR-mode encryption using a weak pseudorandom function necessary CPA-secure? Does it necessarily have indistinguishable encryptions in the presence of an eavesdropper? Prove your answers.

3. Prove that the following construction is CPA-secure if F is a weak pseudorandom function.

   Construction: Let F be a pseudorandom function. Define a private-key encryption scheme for messages of length n as follows:

   - Gen: on input 1^n, choose uniform $k \in \{0,1\}^n$ and output it.
   - Enc: on input a key $k \in \{0,1\}^n$ and a message $m \in \{0,1\}^n$, choose uniform $r \in \{0,1\}^n$ and output the ciphertext:

$$c := \langle r, F_k(r) \oplus m \rangle \tag{3}$$

- Dec: on input a $k \in \{0,1\}^n$ and a ciphertext $c = \langle r, s \rangle$, output the plaintext message

$$m := F_k(r) \oplus s \tag{4}$$

Question 3 (20 points)

Consider the following MAC for messages of length $\ell(n) = 2n - 2$ using a pseudorandom function F: On input a message $m_0 \parallel m_1$ (with $|m_0| = |m_1| = n - 1$) and key $k \in \{0,1\}^n$, algorithm Mac outputs $t = F_k(0||m_0)||F_k(1||m_1)$. Algorithm Vrfy is defined in the natural way. Is (Gen, MAC, Vrfy) secure? Prove your answer.

Question 4 (25 points)

In this question, we explore what happens when the basic CBC-MAC construction is used with messages of different lengths.

- Say the sender and receiver do not agree on the message length in advance (and so $\mathrm{Vrfy_k(m, t)} = 1 \text{iff } \mathrm{t} \stackrel{?}{=} \mathrm{Mac}_k(m)$, regardless of the length of m), but the sender is careful to only authenticate messages of length 2n. Show that an adversary can forge a valid tag on a message of length 4n.

- Say the receiver only accepts 3-block messages (so $\mathrm{Vrfy_k(m, t)} = 1$) only if m has length 3n and $\mathrm{t} = \mathrm{Mac}_k(m)$, but the sender authenticates messages of any length a multiple of n. Show that an adversary can forge a valid tag on a new message.

Question 5 (15 points)

Suppose that an organization has a large number of read only documents which are categorized in 300 different categories. All the documents in the same category i is encrypted using the same key that we denote by K_i (i.e. there are 300 keys, one for each document category). The encrypted documents are accessible to any employee in the organization, but the authorized employee to view can decrypt it. The organization allows each employee to view a range $[\ell, r]$ of document categories where $1 \leq \ell \leq r \leq 300$. In addition, we assume that the pair ℓ and r are different for each employee. Each key K_i is the XOR of two bit-strings F_i and B_i that are defined as follows:

- A forward hash chain: $F_i = H(F_{i-1})$ for $2 \leq i \leq 300$ where F_1 is chosen uniformly at random.

- A backward hash chain: $B_i = H(B_{i+1})$ for $1 \leq i \leq 299$ where B_{300} is chosen uniformly at random.

The organization gives only two values (let we call them α *and* β) to each employee who is allowed to view a range $[\ell, r]$ of document categories. Which of the following pairs could we provide to each employee?

- $(\alpha, \beta) = (K_\ell, K_r)$
- $(\alpha, \beta) = (F_\ell, B_r)$
- $(\alpha, \beta) = (B_\ell, F_r)$
- $(\alpha, \beta) = (F_\ell, K_r)$

Justify your answer. If the pair works then explain how each employee could use α *and* β to derive K_j if $\ell \leq j \leq r$ and why the employeee cannot derive K_j if $\ell \geq j$ or $r \leq j$. If there are multiple options work which option is most convenient. Explain your answer.