1. Consider the following attacker $D(1^n)$ given access to an oracle $g$: query $g$ to obtain $y_0 := g(0^n)$ and $y_1 := g(1^n)$. If $y_0 \oplus y_1 = G(0^n) \oplus G(1^n)$ then output 1; else output 0.

By inspection, we have $\Pr[D^{f_k}(1^n) = 1] = 1$, because for any key $k$ it holds that $G(0^n) \oplus G(1^n) = G(0^n) \oplus G(1^n) \oplus k = G(0^n) \oplus G(1^n)$.

On the other hand, if $g$ is a random function then $y_0, y_1$ are uniform and independent $n$-bit strings. So the probability that their XOR is any particular string (in this case, the fixed string $G(0^n) \oplus G(1^n)$) is $2^{-n}$. I.e., $\Pr[D^{f}(1^n) = 1] = 2^{-n}$. Since $1 - 2^{-n}$ is not negligible and $D$ is efficient, this shows that $F$ is not a pseudorandom function.

2. Consider the following attacker $A$:

- Request encryption of the message $0^n$; receive in return a ciphertext $\langle IV, c \rangle$.
- Let $m_0 = (IV + 1) \oplus IV$. Output $(m_0, m_1 = 0^n)$.
- Receive the challenge ciphertext $\langle IV + 1, c' \rangle$. If $c = c$ then output 0; else output 1.

Let $k$ be the key (unknown to $A$) used by encryption. From step 1, $A$ learns that $F_k(IV) = c$. Now, if $m_0$ is encrypted, then the ciphertext will be

$$\langle IV + 1, F_k((IV + 1) \oplus m_0) \rangle = \langle IV + 1, F_k(IV) \rangle = \langle IV + 1, c \rangle,$$

and so $A$ outputs 0. On the other hand, if $m_1$ is encrypted then $A$ always outputs 1. It follows that $\Pr[\text{PrivK}_{A,1}^{\text{cpa}}(n) = 1] = 1$, and so this scheme is not CPA-secure.

3. (a) Let $m_1, m_2 \in \{0,1\}^n$ be distinct. Then, the tag on the message $m_1$, $m_2$ is identical to the tag on $m_2, m_1$. Thus, an adversary $A$ can ask for the tag $t$ on $m_1, m_2$ and output the message $m_2, m_1$ together with $t$.

(b) Let $m_1, m'_1, m_2, m'_2 \in \{0,1\}^{n/2}$ with $m_1 \neq m'_1$ and $m_2 \neq m'_2$. The attacker obtains tag $t_1$ on the message $m_1, m_2$; tag $t_2$ on the message $m_1, m'_2$; and tag $t_3$ on the message $m'_1, m_2$. Then $t_1 \oplus t_2 \oplus t_3$ is a valid tag on $m'_1, m'_2$.

(c) Let $m_1 \in \{0,1\}^{n/2}$ be arbitrary. The attacker can set $r := \langle 1 \rangle \parallel m_1$ and output the forgery $\langle r, 0^n \rangle$ on the message $m_1$.

4. (a) Consider the following attack: Obtain tag $t_1, t_2$ on the message $m_1, m_2$, where $t_1 = F_k(m_1)$ and $t_2 = F_k(t_1 \oplus m_2)$. Next, output the message $t_1 \oplus m_2, t_2$ and the tag $t_2, t_1$. This is a valid forgery (unless $t_1 \oplus m_2 = m_1$ and $t_2 \oplus m_1 = m_2$, which occurs with only negligible probability), since $t_2 = F_k(t_1 \oplus m_2)$ and

$$t_1 = F_k(t_2 \oplus t_2 \oplus m_1) = F_k(m_1).$$

(b) Consider the following attack: obtain tag $(t_0, t)$ on the one-block message $m$. Then output $(m, t)$ as a valid tag for the message $t_0$. 

---

Homework 4—Solutions