

# Solutions

## 794Q Homework 1

Winter 2009

1. Let  $\vec{m}_0 := (m, m)$  and  $\vec{m}_1 := (m, m')$ , where  $m \neq m'$ .

Then  $\vec{c}_0 := (c, c)$  and  $\vec{c}_1 := (c, c')$ , where  $c = E_k(m)$  and  $c' = E_k(m')$ .

Given a challenge text  $\vec{c}$ , the adversary can tell whether it is the encryption of  $\vec{m}_0$  or  $\vec{m}_1$  by checking whether the two halves of  $\vec{c}$  are equal or not.

2. For every adversary  $A$  and every two messages  $m_0, m_1 \in \{0, 1\}$  with  $m_0 \neq m_1$ .

$$\begin{aligned} & \Pr[A(m_0, m_1, E_k(m_0)) = 1 : k \leftarrow_u K] \\ &= \sum_{k \in K} \Pr[k] \cdot \Pr[A(m_0, m_1, E_k(m_0)) = 1] \\ &= \Pr[0] \cdot \Pr[A(m_0, m_1, E_0(m_0)) = 1] + \Pr[1] \cdot \Pr[A(m_0, m_1, E_1(m_0)) = 1] \\ &= \frac{1}{2} \cdot \Pr[A(m_0, m_1, m_0 \oplus 0) = 1] + \frac{1}{2} \cdot \Pr[A(m_0, m_1, m_0 \oplus 1) = 1] \\ &= \frac{1}{2} \cdot \Pr[A(m_0, m_1, 0) = 1] + \frac{1}{2} \cdot \Pr[A(m_0, m_1, 1) = 1] \end{aligned}$$

The last equality holds because these two sets are equal:  $\{m_0 \oplus 0, m_0 \oplus 1\} = \{0, 1\}$ .

Similarly,

$$\begin{aligned} & \Pr[A(m_0, m_1, E_k(m_1)) = 1 : k \leftarrow_u K] \\ &= \frac{1}{2} \cdot \Pr[A(m_0, m_1, 0) = 1] + \frac{1}{2} \cdot \Pr[A(m_0, m_1, 1) = 1] \end{aligned}$$

So,  $\Pr[A(m_0, m_1, E_k(m_0)) = 1 : k \leftarrow_u K] = \Pr[A(m_0, m_1, E_k(m_1)) = 1 : k \leftarrow_u K]$ ,

and by definition the scheme is absolutely ciphertext-indistinguishable.

3.  $A_n = \{0,1\}^n$  and  $B_n = \{s \in \{0,1\}^n : s > 2^{100}\} \cup \{1^n\}$ . Let  $C_n = A_n - B_n$ . Thus,  $A_n = B_n \cup C_n$ .  
 Note: for sufficiently large  $n$  (say  $n > 100$ ),  $|A_n| = 2^n$ ,  $|B_n| = 2^n - 2^{100} - 1$ ,  $|C_n| = 2^{100} + 1$ .  
 Let  $D$  be any polynomial-time distinguisher. For  $n > 100$ ,

$$\begin{aligned}
 P_1(n) &= \Pr[D(s) = 1 : s \leftarrow_u A_n] \\
 &= \sum_{s \in A_n} \Pr[s] \cdot \Pr[D(s) = 1] \\
 &= \sum_{s \in A_n} \frac{1}{|A_n|} \cdot \Pr[D(s) = 1] \\
 &= \frac{1}{|A_n|} \cdot \left( \sum_{s \in B_n} \Pr[D(s) = 1] + \sum_{s \in C_n} \Pr[D(s) = 1] \right)
 \end{aligned}$$

$$\begin{aligned}
 P_2(n) &= \Pr[D(s) = 1 : s \leftarrow_u B_n] \\
 &= \sum_{s \in B_n} \Pr[s] \cdot \Pr[D(s) = 1] \\
 &= \sum_{s \in B_n} \frac{1}{|B_n|} \cdot \Pr[D(s) = 1]
 \end{aligned}$$

$$\begin{aligned}
 |P_1(n) - P_2(n)| &= \left| \left( \frac{1}{|A_n|} - \frac{1}{|B_n|} \right) \cdot \sum_{s \in B_n} \Pr[D(s) = 1] + \frac{1}{|A_n|} \cdot \sum_{s \in C_n} \Pr[D(s) = 1] \right| \\
 &\leq \left| \left( \frac{1}{|A_n|} - \frac{1}{|B_n|} \right) \cdot \sum_{s \in B_n} 1 + \frac{1}{|A_n|} \cdot \sum_{s \in C_n} 1 \right| \\
 &= \left| \left( \frac{1}{|A_n|} - \frac{1}{|B_n|} \right) \cdot |B_n| + \frac{1}{|A_n|} \cdot |C_n| \right| \\
 &\leq \left( 1 - \frac{|B_n|}{|A_n|} \right) + \frac{|C_n|}{|A_n|} \\
 &= \left( 1 - \frac{2^n - 2^{100} - 1}{2^n} \right) + \frac{2^{100} + 1}{2^n} \\
 &= \frac{2(2^{100} + 1)}{2^n}, \text{ which is negligible.}
 \end{aligned}$$

4.  $A_n = \{0,1\}^n$  and  $B_n = 0 \parallel \{0,1\}^{n-1}$ .

Let distinguisher  $D$  work as follows:

$$D(s) := \begin{cases} 0 & \text{if the first bit of } s \text{ is } 0 \\ 1 & \text{otherwise} \end{cases}$$

$D$  is obviously polynomial-time.

$$\Pr[D(s) = 1 : s \leftarrow_u A_n] = \frac{1}{2}.$$

$$\Pr[D(s) = 1 : s \leftarrow_u B_n] = 0.$$

$$|\Pr[D(s) = 1 : s \leftarrow_u A_n] - \Pr[D(s) = 1 : s \leftarrow_u B_n]| = \frac{1}{2}, \text{ not negligible.}$$

5.  $T[0] = 0$  and  $T[i] = (1 - i) \bmod 256$  for  $1 \leq i \leq 255$ .