Cryptography (SS2006) Prof. Michael Backes

Solutions for Exercise Sheet 3

Out: 17/05/2006 Saarland University

Problem 1: Negligible Functions

Let $c \in \mathbb{R}_0^+$ and let f and g two negligible functions, i.e.

$$\forall a \in \mathbb{N}\ \exists n_a \in \mathbb{N}\ \forall n \geq n_a : f(n) \leq \frac{1}{n^a},\ g(n) \leq \frac{1}{n^a}$$

(a) *Claim:* $h(n) := c \cdot f(n)$ is negligible

Proof. If $c = 0$ then $c \cdot f(n) \equiv 0$, and it is immediately clear that 0 is negligible as $\frac{1}{n^a} \geq 0$ for all $a, n \in \mathbb{N}$. If $c > 0$ we know that $\forall b : \exists n_b :\ f(n) \leq \frac{1}{n^b}$ by the definition of negligibility. So in particular for $b = a+1$ we know that $\exists n_{a+1}\ \forall n > n_{a+1} :\ f(n) \leq \frac{1}{n^{a+1}}$. Now we choose $n_a := \max\{n_{a+1}, \lceil c \rceil\}$, and we show that this can be used in the definition of negligibility, i.e.,

$$\forall n \geq n_a :\ \frac{1}{c \cdot n^a} \overset{(1)}{\geq} \frac{1}{n \cdot n^a} = \frac{1}{n^{a+1}} \overset{(2)}{\geq} f(n),$$

where (1) holds as by construction $n \geq n_a \geq c$ and (2) follows from the fact that $n_a \geq n_{a+1}$ and the construction of n_{a+1}. ∎

(b) *Claim:* $h(n) := f(n) + g(n)$ is negligible.

Proof. By assumption we know that f and g are negligible. Using (a) we know that for all $c \in \mathbb{R}_0^+$: $c \cdot f(n)$ is negligible. Consequently, we have

$$f \text{ is negligible} \Leftrightarrow \quad f \in \bigcap_{a \in \mathbb{N}} O(\frac{1}{n^a}). \quad (*)$$

Since for all $a \in \mathbb{N}$ we have

$$f, g \in O(\frac{1}{n^a}) \Rightarrow h \in O(\frac{1}{n^a}),$$

it follows

$$h \in \bigcap_{a \in \mathbb{N}} O(\frac{1}{n^a}),$$

hence h is negligible by equation (*). ∎

(c) *Claim:* $h(n) := f(n) \cdot g(n)$ is negligible. (There was a typo that caused some confusion.)

Proof. By assumption we know that f and g are negligible. As f is negligible we know in particular that it approaches 0 for $n \to \infty$, and consequently we find a c such that $c \geq f(n)$ for all $n \in \mathbb{N}$, and consequently $f(n) \cdot g(n) \leq c \cdot g(n)$. As the later is negligible by (a), h is also negligible. ∎

(d) *Claim:* $h(n) := 0.999^n$ is negligible.

Proof. It suffices to show

$$h \in \bigcap_{c\in\mathbb{N}} O(\frac{1}{n^c}) \text{ or, equivalently: } \forall c \in \mathbb{N} : h \in O(\frac{1}{n^c}).$$

For a fixed $c \in \mathbb{N}$, we examin the limes

$$\lim_{n\to\infty} \frac{0.999^n}{n^{-c}} = \lim_{n\to\infty} \frac{n^c}{\left(\frac{1000}{999}\right)^n} = 0,$$

as it is well-known that a^n for $a > 1$ grows exponentially and thus faster than any polynom, in particular, faster than n^c for any c. Thus h is negligible.

■

(e) *Claim:* $h(n) := 0$ is negligible.

Proof. This is obvious, as for all $a, n \in \mathbb{N}$: $0 \leq \frac{1}{n^a}$. ■

(f) *Claim:* $h(n) := 10^{-10^{42}}$ is *not* negligible.

Proof. This is obvious, as for all $a \in \mathbb{N}$: $\frac{1}{n^a} \overset{n\to\infty}{\to} 0$, so there exists n_a such that for all $n \geq n_a$: $10^{-10^{42}} \geq \frac{1}{n^a}$. ■

Problem 2: Semantic Security and the One-time Pad

(a) The encryption scheme (E, D) over $(\mathcal{K}, \mathcal{M}, \mathcal{C})$ has perfect secrecy means by definition:

$$\begin{aligned} \forall m_0, m_1 \in \mathcal{M}\ \forall c \in \mathcal{C} \quad : \quad & Pr[c = c'; K' \leftarrow_{\mathcal{R}} K, c' \leftarrow \mathsf{E}(K', m_0)] \\ = \quad & Pr[c = c'; K' \leftarrow_{\mathcal{R}} K, c' \leftarrow \mathsf{E}(K', m_1)] \end{aligned}$$

This immediately implies that for $c \leftarrow \mathsf{E}(K, m_b)$, both experiments $b = 0$ and $b = 1$ look exactly the same to any adversary, so consequently $Pr[Exp^{\mathsf{CT-only}}(0) = 1] = Pr[Exp^{\mathsf{CT-only}}(1) = 1]$. From this it follows directly that

$$Adv^{\mathsf{CT-only}}[\mathsf{A}, \mathsf{OTP}] = \left| Pr[Exp^{\mathsf{CT-only}}(0) = 1] - Pr[Exp^{\mathsf{CT-only}}(1) = 1] \right| = 0.$$

(b) This follows directly from Problem 3, as the One-time Pad is deterministic.

Problem 3: Determinism and Semantic Security

We construct an adversary A that has an advantage of 1 as follows: A selects two arbitrary messages m_0, m_1 with $|m_0| = |m_1|$ and sends the first to the challenger, receiving $c_0 \leftarrow \mathsf{E}(K, m_0)$ as response. Then he sends m_0 and m_1 and receives $c' \leftarrow E(K, m_b)$ in response. If $c' = c_0$ then he outputs 0, otherwise 1.

As E is deterministic, a message encrypts always to the same ciphertext (for the same key). Consequently

$$\begin{aligned} Pr[Exp^{\mathsf{CPA}}(0) = 1] &= 0 \\ Pr[Exp^{\mathsf{CPA}}(1) = 1] &= 1 \end{aligned}$$

Thus

$$Adv^{\mathsf{CPA}}[\mathsf{A}, \mathsf{E}] = \left| Pr[Exp^{\mathsf{CPA}}(0) = 1] - Pr[Exp^{\mathsf{CPA}}(1) = 1] \right| = |0 - 1| = 1.$$

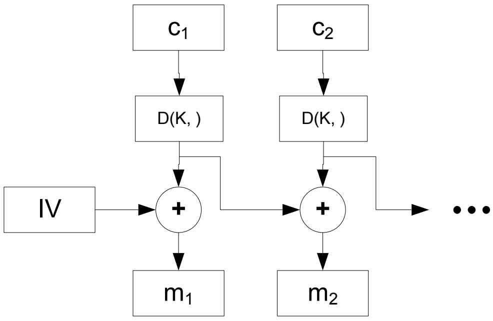


Figure 1: Decryption of CBC^*

Problem 4: Variants of Modes of Operation

(a) Decryption is given in Figure 1.

(b) We construct an adversary A as follows: It constructs two message $m_0 := 0^k \mid 1^k$ and $m_1 := 1^k \mid 0^k$, where k is the blocksize of the cipher, and sends both messages to the challenger (m_0, m_1). He receives one encryption $c = (c^{(1)}, c^{(2)}) \leftarrow \mathsf{E}^{\mathsf{CBC}^*}(K, m_b)$. If $c^{(1)} = c^{(2)}$ he outputs 1, otherwise 0. Note that we assume that E is deterministic, this is true for blockciphers.

Let us calculate $\mathsf{Pr}[Exp^{\mathsf{CT-only}}(1) = 1]$: If $b = 1$ then the challenger encrypted $m_1 = 1^k \mid 0^k$, so $c^{(1)} = \mathsf{E}(K, IV \oplus 1^k)$ and $c^{(2)} = \mathsf{E}(K, IV \oplus 1^k \oplus 0^k) = c^{(1)}$. In this case A outputs 1 by construction, thus we have $\mathsf{Pr}[Exp^{\mathsf{CT-only}}(1) = 1] = 1$.

Next we calculate $\mathsf{Pr}[Exp^{\mathsf{CT-only}}(0) = 1]$: If $b = 0$ then the challenger encrypted $m_0 := 0^k \mid 1^k$, where $c^{(1)} = \mathsf{E}(K, IV \oplus 0^k)$ and $c^{(2)} = \mathsf{E}(K, IV \oplus 0^k \oplus 1^k) = c^{(1)}$. Note that the terms $IV \oplus 0^k$ and $IV \oplus 0^k \oplus 1^k$ are different, thus, as $\mathsf{E}(K, \cdot)$ is a permutation, also $c^{(1)}$ and $c^{(2)}$ are different. Consequently A outputs 0 by construction, thus we have $\mathsf{Pr}[Exp^{\mathsf{CT-only}}(0) = 1] = 0$.

Finally we see that

$$Adv^{\mathsf{CT-only}}[\mathsf{A}, \mathsf{CBC}^*] = \left|\mathsf{Pr}[Exp^{\mathsf{CT-only}}(0) = 1] - \mathsf{Pr}[Exp^{\mathsf{CT-only}}(1) = 1]\right| = |0 - 1| = 1.$$

Problem 5: PRF Candidates

(a) F_1 is a PRF, thus we have to show that for any A:

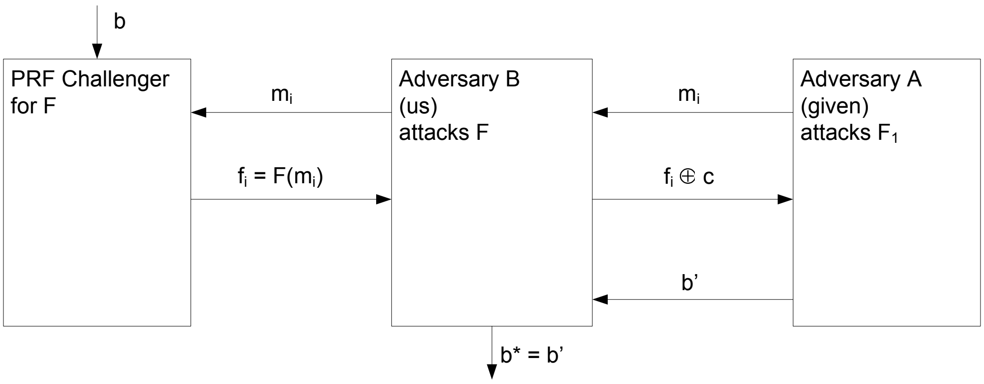
$$Adv^{\mathsf{PRF}}[\mathsf{A}, F_1] = |Pr[Exp^{\mathsf{PRF}}(0) = 1] - Pr[Exp^{\mathsf{PRF}}(1) = 1]|$$

is negligible.

Proof. Given an adversary A against the PRF F_1, we construct an adversary B, who attacks the PRF F. Our aim is to show, that

$$Adv^{PRF}[A, F_1] \leq Adv^{PRF}[B, F]$$

holds, i.e., the advantage of the adversary A attacking F_1 is smaller than the advantage of the adversary B attacking F. Then we conclude, since $Adv^{\mathsf{PRF}}\mathsf{B}, F]$ is negligible, that $Adv^{\mathsf{PRF}}[\mathsf{A}, F_1]$ has to be negligible, too, and thus we have finished the proof.



Construction of the adversary B

The adversary B gets a message m_i from the adversary A and returns $f_i \oplus c$ to the adversary A, where he gets f_i by sending m_i to the challenger.

- If $b = 0$ then the challenger returns $f_i = F(K, m_i)$, thus $\mathsf{A}'s$ input is exactly the same as if he played against a PRF challenger for F_1.
- If $b = 1$ then the challenger evaluates a random function, thus the values f_i are random values. Again, A's view is correctly simulated, as xoring a constant to a uniformly distributed value yields a uniformly distribute value again.

Thus we can compute the advantage of the adversary B attacking F as follows.

$$\begin{aligned} Adv^{\mathsf{PRF}}[\mathsf{A}, F_1] &= |Pr[Exp_{\mathsf{A}}^{\mathsf{PRF}}(0) = 1] - Pr[Exp_{\mathsf{A}}^{\mathsf{PRF}}(1) = 1]| \\ &= |Pr[Exp_{\mathsf{B}}^{\mathsf{PRF}}(0) = 1] - Pr[Exp_{\mathsf{B}}^{\mathsf{PRF}}(1) = 1]| \\ &= Adv^{\mathsf{PRF}}[\mathsf{B}, F] \end{aligned}$$

As we said before, this finishes the proof.

■

(b) The adversary A chooses an arbitrary message $m \in \{0,1\}^k$ and sends it to the challenger, getting back a value $f \in \{0,1\}^{2k}$. Write $f = f' \mid\mid c'$ with $f', c' \in \{0,1\}^k$ and test if $c = c'$. If yes it outputs $b^* = 0$, otherwise it outputs $b^* = 1$.

One easily sees that $Pr[Exp^{\mathsf{PRF}}(0) = 0] = 1$ and $Pr[Exp^{\mathsf{PRF}}(1) = 0] = \frac{1}{2^k}$, thus the advantage is

$$Adv^{\mathsf{PRF}}[\mathsf{A}, F_2] = 1 - \frac{1}{2^k}.$$

Hence the advantage of this adversary A is not negligible and F_2 is no PRF.

(c) The adversary A sends two randomly chosen messages $m_1 \neq m_2 \leftarrow_{\mathcal{R}} \{0,1\}^k$ to the challenger and gets back f_1, f_2. If the last k bits of the f_1, f_2 are identical then it outputs 0, otherwise 1.

Obviously, $Pr[Exp^{\mathsf{PRF}}(0) = 0] = 1$. If $b = 1$, i.e., the function is chosen randomly, then f_1, f_2 are random, thus the probability that the last K bits are equal is 2^{-k}. Thus $Pr[Exp^{\mathsf{PRF}}(1) = 0] = 2^{-k}$, and therefore

$$\begin{aligned} Adv^{\mathsf{PRF}}[\mathsf{A}, F_3] &= |Pr[Exp^{\mathsf{PRF}}(1) = 0] - Pr[Exp^{\mathsf{PRF}}(0) = 0]| \\ &= 1 - 2^k \end{aligned}$$

(d) The adversary chooses an arbitrary message $m_0 \in \{0,1\}^k$ and sends first m_0, then $m_1 = \overline{m_0}$ to the challenger, receiving f_0, f_1. Write these as $f_i = c_i \mid\mid c'_i$. If $c_0 = c'_1$ and $c'_0 = c_1$ then it outputs 0, otherwise 1.

It follows that

$$Pr[Exp^{\mathsf{PRF}}(0) = 0] = 1 \text{ and } Pr[Exp^{\mathsf{PRF}}(1) = 0] = 2^{-2k}.$$

Thus $Adv^{\mathsf{PRF}}[\mathsf{A}, F_4] = 1 - 2^{-2k}$ is not negligible, thus F_4 is no PRF.

(e) The adversary A sends a randomly chosen message $m \in \{0,1\}^k$ to the challenger receiving $f = c \,||\, c' \in \{0,1\}^{2k}$. If $c' = \mathsf{F}(0^k, m)$ it outputs 0, otherwise it outputs 1. Note that the function F is known to the adversary, thus if he knows the key he can evaluate it in his own.

It follows that

$$Pr[Exp^{\mathsf{PRF}}(0) = 0] = 1 \text{ and } Pr[Exp^{\mathsf{PRF}}(1) = 0] = 2^{-k}.$$

Thus $Adv^{\mathsf{PRF}}[\mathsf{A}, F_5] = 1 - 2^{-k}$ is not negligible, thus F_5 is no PRF.