Cryptography (SS2006) Prof. Michael Backes

Exercise Sheet 3

Out: May 9, 2006 Saarland University

Problem 1: Negligible Functions

Let $f(k), g(k) : \mathbb{N} \to \mathbb{R}_0^+$ be negligible functions and $c \in \mathbb{R}_0^+$. Prove that the following functions are negligible:

$$(a)\ c \cdot f(k), \qquad (b)\ f(k) + g(k), \qquad (c)\ (k) \cdot g(k).$$

Are the following functions negligible? Prove or disprove.

$$(d)\ 0.999^k, \qquad (e)\ 0, \qquad (f)\ 10^{(-10^{42})}.$$

Problem 2: Semantic Security and the One-time Pad

Let us explore the relationship of the One-time Pad (taking messages and keys from $\{0,1\}^k$) and both variants of semantic security.

a) Prove that for every (efficient) adversary A, we have $Adv^{\mathsf{CT-only}}[\mathsf{A}, \mathsf{OTP}] = 0$, i.e., the One-time Pad is semantically secure under ciphertext-only (CT-only) attack.

b) Prove that there exists an efficient adversary A such that $Adv^{\mathsf{CPA}}[\mathsf{A}, \mathsf{OTP}] = 1$, i.e., the One-time Pad is not semantically secure under chosen-plaintext attack (CPA).

Problem 3: Determinism and Semantic Security

Let (E, D) denote a cipher where E is deterministic. Prove that there exists an adversary A such that $Adv^{\mathsf{CPA}}[\mathsf{A}, \mathsf{E}] = 1$. Thus no deterministic cipher satisfies semantic security under CPA!

Problem 4: Variants of Modes of Operation

A major drawback of the CBC mode is that it is highly sequential. One could try to circumvent this problem using the modification CBC* shown in Figure 1. Assume that the initial value IV is randomly chosen again for every new encryption and that IV is sent together with the ciphertext.

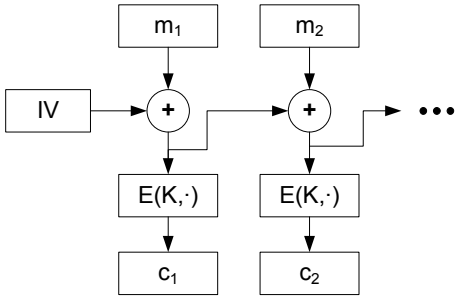

Figure 1: CBC* mode

(a) Show how decryption is done for the CBC* mode (showing by picture is fine).

(b) Show that CBC* is not even semantically secure under ciphertext-only (CT-only) attack. More precisely, show that an efficient adversary A exists such that $Adv^{\mathsf{CT-only}}[\mathsf{A}, \mathsf{CBC}^*] = 1$.

Problem 5*: PRF Candidates

Suppose that $\{F : \{0,1\}^k \times \{0,1\}^k \mapsto \{0,1\}^k\}_{k\in\mathbb{N}}$ is a family of pseudo-random functions, mapping k-bit inputs to k-bit outputs, where the index k denotes the length of the key (and the message). We would like to construct a new PRF family. Consider the following constructions, and for each of them show whether it yields a PRF family again or not. We write $x||y$ to denote concatenation of x and y and $\bar{x}$ to denote the bitwise negation of x.

Prove or disprove that the following construction yields a PRF:

(a) $F_1(K, x) := F(K, x) \oplus c$ for an arbitrary but fixed constant $c \in \{0,1\}^k$ which is known to the adversary.

Prove that the following constructions are not PRFs:

(b) $F_2(K, x) := F(K, x) \;||\; c$ for an arbitrary but fixed constant $c \in \{0,1\}^k$ which is known to the adversary.

(c) $F_3(K, x) := F(K, x) \;||\; F(K, 0^k)$.

(d) $F_4(K, x) := F(K, x) \;||\; F(K, \bar{x})$.
(**Hint:** What is $F_4(K, \bar{x})$?)

(e) $F_5(K, x) := F(K, x) \;||\; F(0^k, x)$.