ETH Zürich, D-INFK
Spring 2018

Prof. Ueli Maurer
Christian Badertscher
Fabio Banfi

Cryptography Foundations

Exercise 2

2.1 Block Ciphers in ECB and CBC Mode

Goal: *When should a symmetric encryption scheme be considered* secure*? We discuss how (not) to use block ciphers and introduce common modes of operation.*

Let $F\colon \{0,1\}^n \times \{0,1\}^\kappa \to \{0,1\}^n$ be a block cipher and $k \in \{0,1\}^\kappa$ a uniformly distributed key.

a) A straightforward technique to encrypt bit strings of length $\ell \cdot n$ for $\ell \geq 1$ is called *electronic codebook (ECB)* mode: Split $m \in \{0,1\}^{\ell n}$ into $m = m_1 | \dots | m_\ell$ with $m_1, \dots, m_\ell \in \{0,1\}^n$ and compute $c \coloneqq F(m_1, k) | \dots | F(m_\ell, k)$.

Should this encryption scheme be considered secure if we assume that an attacker does not know anything about the encrypted messages?

b) Assume only messages of length n need to be encrypted. Describe an attack scenario in which it is insecure to encrypt a message $m \in \{0,1\}^n$ as $c \coloneqq F(m, k)$.

c) A widely used alternative to ECB mode is the so-called *cipher-block chaining (CBC)* mode: To encrypt a message $m = m_1 | \dots | m_\ell$ with $m_1, \dots, m_\ell \in \{0,1\}^n$, choose $c_0 \in \{0,1\}^n$ uniformly at random, compute $c_i := F(m_i \oplus c_{i-1}, k)$ for $i = 1, \dots, \ell$, and let the ciphertext be $c := c_0 | \dots | c_\ell$. The value c_0 is called *initialization vector (IV)*.

How can a ciphertext be decrypted?

d) Another mode of operation is the so-called *counter (CTR)* mode: To encrypt a message $m = m_1 | \dots | m_\ell$ with $m_1, \dots, m_\ell \in \{0,1\}^n$ and $\ell \leq 2^{\lceil n/2 \rceil}$, choose $r \in \{0,1\}^{\lfloor n/2 \rfloor}$ uniformly at random, compute $c_i := m_i \oplus F(r | \langle i \rangle, k)$, for $i = 1, \dots, \ell$, where $\langle i \rangle$ denotes the representation of i as an $\lceil n/2 \rceil$-bit string, and let the ciphertext be $c := r | c_1 | \dots | c_\ell$. The value r is called *nonce* (short for number used once).

How can a ciphertext be decrypted? Why is the nonce needed?

2.2 Information Theoretically Secure Message Authentication

Goal: *Devise information-theoretically secure message authentication codes.*

We have seen in the lecture that a MAC for which the 1-message MAC-forgery game is hard can be used to construct a single-use authenticated channel from an insecure channel and a shared secret key. The goal of this task is to devise MACs for which even computationally unbounded adversaries can win this game only with small probability. For the whole task, we assume the keyspace $\mathcal{K} = \{0,1\}^n$ for an even n.

a) Let the message space be $\mathcal{M} = \{0,1\}$. Devise a MAC $f\colon \mathcal{M} \times \mathcal{K} \to \mathcal{T}$ and derive an upper bound on the winning probability of an adversary in the 1-message MAC-forgery game.

b) Modify your MAC from subtask **a)** for the message space $\mathcal{M} = \{0,1,2\}$ without increasing the maximal winning probability of the attacker.

c) Let the message space be $\mathcal{M} = \{0,1\}^{\frac{n}{2}}$. Devise a MAC such that the maximal winning probability of the attacker matches the one you derived in subtask **a)** and **b)**.

Hint: Consider the messages to be elements of $\mathrm{GF}(2^{\frac{n}{2}})$ and use the ideas from **a)** and **b)**.

2.3 MAC Construction

Goal*: We construct an authenticated channel from a shared key and an insecure channel.*

Consider the MAC function $f\colon \mathcal{M} \times \mathcal{K} \to \mathcal{T}$ from Task **2.2c)** where $\mathcal{K} = \{0,1\}^n$ and $\mathcal{M} = \{0,1\}^{\frac{n}{2}}$. We want to construct a single-message authenticated channel $\bullet\!\!\longrightarrow$ using a multi-message insecure channel $\longrightarrow\!\!\!\!\!\rightarrow$ (in particular parameterized by the maximum number q_E of injections at interface E) and a shared secret key $\bullet\!\!=\!\!\bullet$. Concretely, we present converters tag, vrf, and a simulator σ and prove that

$$\Delta^D(\mathsf{tag}^A\,\mathsf{vrf}^B[\bullet\!\!=\!\!\bullet, \longrightarrow\!\!\!\!\!\rightarrow], \sigma^E\bullet\!\!\longrightarrow) \leq q_E \cdot 2^{-\frac{n}{2}}. \tag{1}$$

The involved resources are defined as follows:

The shared secret key $\bullet\!\!=\!\!\bullet$
(for key space $\mathcal{K}$)

Variable $k \in \mathcal{K}$: Initially chosen uniformly at random from $\mathcal{K}$.

- **Interfaces A/B:** On input read, output k.
- **Interface E:** Inactive.

The insecure channel $\longrightarrow\!\!\!\!\!\rightarrow$
(for message space $\mathcal{M}'$ and maximum numbers of messages/injections $q_A, q_E \in \mathbb{N}$)

Multiset $\mathcal{B}$ on $\mathcal{M}'$: Initialized to $\emptyset$.

- **Interface A:** On input $x \in \mathcal{M}'$, set $\mathcal{B} := \mathcal{B} \uplus \{x\}$. Inactive after q_A inputs.
- **Interface B:** On input read, output $\mathcal{B}$.
- **Interface E:**
  - On input read, output $\mathcal{B}$.
  - On input (inj, x'), set $\mathcal{B} := \mathcal{B} \uplus \{x'\}$. Inactive on inputs $(\mathsf{inj}, \cdot)$ after q_E such inputs.

The authenticated channel $\bullet\!\!\longrightarrow$
(for message space $\mathcal{M}$)

Variable $x \in \mathcal{M} \cup \{\bot\}$: Initialized to $\bot$.

- **Interface A:** On the first input $x' \in \mathcal{M}$, set $x := x'$. Ignore all subsequent inputs at this interface.
- **Interface B:** On input read, output x.
- **Interface E:** On input read, output x.

Note that, for this task, the assumed insecure channel has messages space $\mathcal{M}' := \mathcal{M} \times \mathcal{T}$, and that it is sufficient to have $q_A = 1$.

a) Depict both the real system $\mathsf{tag}^A\,\mathsf{vrf}^B[\bullet\!\!=\!\!\bullet, \longrightarrow\!\!\!\!\!\rightarrow]$ and the ideal system $\sigma^E\bullet\!\!\longrightarrow$.

b) Describe the converters tag, vrf, and σ.

c) Using the results from **2.2c)**, prove that the inequality (1) holds.

Discussion of solutions:
5/6.3.2018 (Tasks 2.1 and 2.2)
12/13.3.2018 (Task 2.3)
The Monday and Tuesday sessions of each week cover the same material.