ETH Zürich, D-INFK
Spring 2019

Prof. Ueli Maurer
Fabio Banfi
Daniel Jost
Jiamin Zhu

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 $c := F(m_1, k) || \dots || F(m_\ell, k)$. Is this encryption scheme 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 $c := F(m, k)$.

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 $c := c_0 || \dots || c_\ell$. How can a ciphertext be decrypted?

2.2 Construction of a Secure Channel Using Symmetric Encryption

Goal: *We prove that a IND-CPA secure encryption scheme constructs a secure channel from an authentic one and a shared secret key.*

a) We first introduce yet another bit-guessing problem $[\![S_t^{\mathsf{rro}}; B]\!]$ capturing the CPA security notion, which will be easier to relate to the constructive view. It is defined as follows.

1. S_t^{rro} chooses a random secret key k according to the key distribution P_K.
2. S_t^{rro} obtains t messages. For *each* message m it makes the following case distinction:
   - If $B = 0$, it computes $c = E(m, k)$ for fresh and independent randomness, and returns c.
   - If $B = 1$, it chooses a uniformly random message $\widetilde{m}$ of length $|m|$, computes $\widetilde{c} = E(\widetilde{m}, k)$ for fresh and independent randomness, and returns $\widetilde{c}$.

We now want to show that the IND-CPA notion from the lecture notes implies this new notion. In Exercise 1.1 a) we have seen that IND-CPA security implies RRC-CPA security, therefore we only need to show that RRC-CPA security implies RRO-CPA security.

To this end, for each distinguisher D for $[\![S_t^{\mathsf{rro}}; B]\!]$, we construct a new one D' for $[\![S_{t-1}^{\mathsf{rrc}}; B]\!]$ that works as follows.

1. D' samples τ *uniformly* at random from $\{1, \dots, t\}$.
2. Then for the i-th query m of D, it submits the following message to $[\![S_{t-1}^{\mathsf{rrc}}; B]\!]$ (and returns the corresponding ciphertext back to D):
   - if $i < \tau$, then a uniformly random message $\widetilde{m}$ of length $|m|$ is submitted as a query;

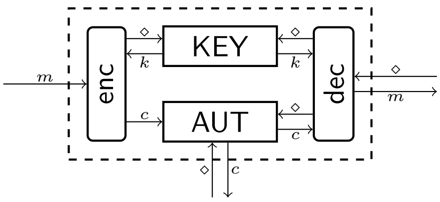
- if $i = \tau$, then m is submitted as challenge;
- if $i > \tau$, then m is submitted as a query,

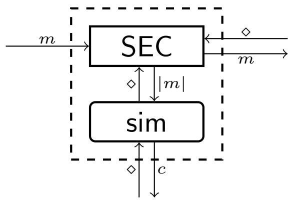
3. D' returns as guess Z' the same bit Z as D.

Prove that $\Lambda^D([\![S_t^{\mathsf{rro}}; B]\!]) = t \cdot \Lambda^{D'}([\![S_{t-1}^{\mathsf{rrc}}; B']\!])$.

Hint: Observe that by Lemma 2.3, showing $\Lambda^D([\![S_t^{\mathsf{rro}}; B]\!]) = t \cdot \Lambda^{D'}([\![S_{t-1}^{\mathsf{rrc}}; B']\!])$ is equivalent to showing $\Delta^D(S_t^{\mathsf{rro}\text{-}0}, S^{\mathsf{rro}\text{-}1}) = t \cdot \Delta^{D'}(S_{t-1}^{\mathsf{rrc}\text{-}0}, S_{t-1}^{\mathsf{rrc}\text{-}1})$, for appropriately defined $S_t^{\mathsf{rro}\text{-}b}$ and $S_{t-1}^{\mathsf{rrc}\text{-}b}$. Design a sequence of intermediate systems $H_1, H_2, \ldots, H_{t+1}$ between $S_t^{\mathsf{rro}\text{-}0}$ and $S_t^{\mathsf{rro}\text{-}1}$ (so-called hybrids), and apply Lemma 2.2.

b) We now want to prove the claim outlined in Section 3.3.5 of the lecture notes, that a protocol $(\mathsf{enc}, \mathsf{dec})$ using a symmetric encryption scheme (E, d) satisfying the IND-CPA notion suffices to construct a secure channel SEC from an authenticated channel AUT and a shared secret key KEY. Recall the real-world system $R := \mathsf{enc}^{\mathrm{A}}\,\mathsf{dec}^{\mathrm{B}}\,[\mathsf{KEY}, \mathsf{AUT}]$ and the ideal-world system $S := \mathsf{sim}^{\mathrm{E}}\,\mathsf{SEC}$, depicted below.





Describe an adequate simulator sim and prove that for any given distinguisher D for $\langle R \,|\, S \rangle$, there is a new distinguisher D' (which internally uses D) such that

$$\Delta^D(R, S) = \Lambda^{D'}([\![S_t^{\mathsf{rro}}; B]\!]),$$

where the key KEY, the authentic channel AUT, and the secure channel SEC are defined as follows (each of them accepting at most t inputs at each interface),

- KEY: Upon initialization, a key $k \in \mathcal{K}$ is chosen according to P_K. Then on input $\diamond$ from interface A (resp., B), k is output at interface A (resp., B).
- AUT: Upon initialization, a list $(x_1, \ldots, x_t) \in (\mathcal{C} \cup \{\perp\})^t$, for $t \in \mathbb{N}$ and a special symbol $\perp \notin \mathcal{C}$, is initialized to $(\perp, \ldots, \perp)$. Then:
  - On the i-th input $c \in \mathcal{C}$ at interface A, x_i is set to c.
  - On the i-th input $\diamond$ at interface B (resp., E), x_i is returned (at the same interface).
- SEC: Upon initialization, a list $(x_1, \ldots, x_t) \in (\mathcal{M} \cup \{\perp\})^t$, for $t \in \mathbb{N}$ and a special symbol $\perp \notin \mathcal{M}$, is initialized to $(\perp, \ldots, \perp)$. Then:
  - On the i-th input $m \in \mathcal{M}$ at interface A, x_i is set to m.
  - On the i-th input $\diamond$ at interface B (resp., E), x_i (resp., $|x_i|$) is returned (at the same interface).

and the converters enc, dec, which both keep an internal variable $k \in \mathcal{K} \cup \{\perp\}$ initially set to $\perp \notin \mathcal{K}$ and accept at most t inputs at each interface, as follows:

- enc: On input m at the outside interface, if $k = \perp$ output $\diamond$ at the inside interface connected to KEY, and set k to the returned value. Then set $c := E(m, k)$, and output c at the inside interface connected to AUT.
- dec: On input $\diamond$ at the outside interface, if $k = \perp$ output $\diamond$ at the inside interface connected to KEY, and set k to the returned value. Then output $\diamond$ at the inside interface connected to AUT, and after obtaining c, if $c \neq \perp$ set $m := E(c, k)$ (and $m := \perp$ otherwise), and output m at the outside interface.

2.3 Information Theoretically Secure Message Authentication

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

The goal of this task is to devise MACs for which even computationally unbounded adversaries can win the 1-message MAC-forgery 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)**.