ETH Zürich, D-INFK
Spring 2019

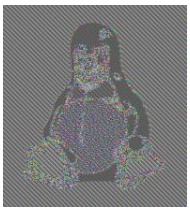
Prof. Ueli Maurer
Fabio Banfi
Daniel Jost
Jiamin Zhu

Cryptography Foundations

Solution Exercise 2

2.1 Block Ciphers in ECB and CBC Mode

a) If a block cipher is used in ECB mode, the encryption of two equal n-bit blocks (aligned at n-bit boundaries) of the plaintext will yield the same n-bit blocks in the ciphertext. This can be hazardous for security in applications: If the plaintext encodes a bitmap with a schematic image, then most of the n-bit blocks will either be 0^n or 1^n, so the ciphertext will mostly consist of the corresponding blocks $F(0^n, k)$ and $F(1^n, k)$. In fact, if the resulting ciphertext is drawn as a bitmap, then the schematic structure will still be visible, as shown in the example below.



`http://en.wikipedia.org/wiki/Block_cipher_modes_of_operation`.

b) The problem here is that the same message is always encrypted to the same ciphertext. Hence, message repetitions can be detected. To see that this is a problem, consider the following scenario as an example: Assume a trader encrypts either "buy" or "sell" and an attacker observes the resulting ciphertexts. If the attacker can find out whether something was bought or sold at some point, she can learn all future messages by simply comparing the ciphertext to the one that was sent before the known transaction.

c) Let F_k^{-1} be the inverse function of $F(\cdot, k)$, which exists since $F(\cdot, k)$ is a permutation. To decrypt the i-th block of a ciphertext $c = c_0 || \dots || c_\ell$, compute

$$F_k^{-1}(c_i) \oplus c_{i-1} = F_k^{-1}(F(m_i \oplus c_{i-1}, k)) \oplus c_{i-1} = m_i \oplus c_{i-1} \oplus c_{i-1} = m_i.$$

2.2 Construction of a Secure Channel Using Symmetric Encryption

a) In the following, let $S_t^{\mathsf{rro}\text{-}b}$ be the same as S_t^{rro}, but where the bit B is fixed to the value b, and analogously for $S_{t-1}^{\mathsf{rrc}\text{-}b}$. Therefore, by Lemma 2.3, note that showing

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

is equivalent to showing

$$\Delta^D(S_t^{\mathsf{rro}\text{-}0}, S_t^{\mathsf{rro}\text{-}1}) = t \cdot \Delta^{D'}(S_{t-1}^{\mathsf{rrc}\text{-}0}, S_{t-1}^{\mathsf{rrc}\text{-}1}).$$

Let also introduce the hybrid systems H_τ, for $\tau \in \{1, \dots, t+1\}$, defined as follows.

1. H_τ chooses a random secret key k according to the key distribution P_K.
2. H_τ obtains t messages. For the i-th message m it makes the following case distinction:
   - If $i < \tau$, 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 $\widetilde{c}$.
   - If $i \geq \tau$, it computes $c = E(m, k)$ for fresh and independent randomness, and returns c.

Observe the following:

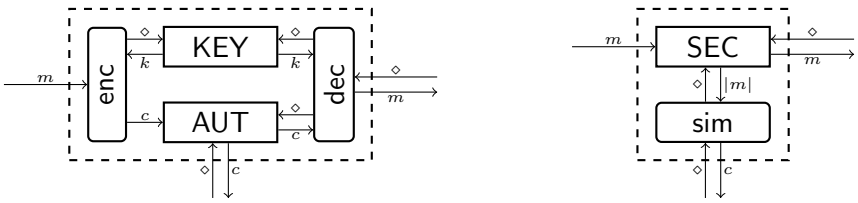
- The system emulated towards D by D' when interacting with $S_{t-1}^{\mathsf{rrc\text{-}0}}$ and conditioned on $T = \tau$ is the same as the system H_τ, therefore
$$\Pr^{D' S_{t-1}^{\mathsf{rrc\text{-}0}}}[Z' = z \,|\, T = \tau] = \Pr^{D H_\tau}[Z = z].$$
- The system emulated towards D by D' when interacting with $S_{t-1}^{\mathsf{rrc\text{-}1}}$ and conditioned on $T = \tau$ is the same as the system $H_{\tau+1}$, therefore
$$\Pr^{D' S_{t-1}^{\mathsf{rrc\text{-}1}}}[Z' = z \,|\, T = \tau] = \Pr^{D H_{\tau+1}}[Z = z].$$
- Systems H_1 and $S_t^{\mathsf{rro\text{-}0}}$ are equivalent as well as systems H_{t+1} and $S_t^{\mathsf{rro\text{-}1}}$.

Therefore we have

$$\begin{aligned}
\Delta^{D'}(S_{t-1}^{\mathsf{rrc\text{-}0}}, S_{t-1}^{\mathsf{rrc\text{-}1}}) &= \Pr^{D' S_{t-1}^{\mathsf{rrc\text{-}1}}}[Z' = 1] - \Pr^{D' S_{t-1}^{\mathsf{rrc\text{-}0}}}[Z' = 1] \\
&= \frac{1}{t} \sum_{\tau=1}^{t} \big(\Pr^{D' S_{t-1}^{\mathsf{rrc\text{-}1}}}[Z' = 1 \,|\, T = \tau] - \Pr^{D' S_{t-1}^{\mathsf{rrc\text{-}0}}}[Z' = 1 \,|\, T = \tau] \big) \\
&= \frac{1}{t} \sum_{\tau=1}^{t} \big(\Pr^{D H_{\tau+1}}[Z = 1] - \Pr^{D H_\tau}[Z = 1] \big) \\
&= \frac{1}{t} \sum_{\tau=1}^{t} \Delta^{D}(H_\tau, H_{\tau+1}) \\
&\overset{(1)}{=} \frac{1}{t} \cdot \Delta^{D}(H_1, H_{t+1}) \\
&= \frac{1}{t} \cdot \Delta^{D}(S_t^{\mathsf{rro\text{-}0}}, S_t^{\mathsf{rro\text{-}1}}),
\end{aligned}$$

where in (1) we used Lemma 2.2.

b) Again, note that by Lemma 2.3 we have $\Lambda^{D'}([\![S_t^{\mathsf{rro}}; B]\!]) = \Delta^{D'}(S_t^{\mathsf{rro\text{-}0}}, S_t^{\mathsf{rro\text{-}1}})$, and thus we need to show $\Delta^{D}(R, S) = \Delta^{D'}(S_t^{\mathsf{rro\text{-}0}}, S_t^{\mathsf{rro\text{-}1}})$, that is, we want to construct a distinguisher D' for distinguishing between $S_t^{\mathsf{rro\text{-}0}}$ and $S_t^{\mathsf{rro\text{-}1}}$ which internally runs the distinguisher D so that the view of the latter is the same as if it was distinguishing between the real world $R := \mathsf{enc}^{\mathrm{A}}\, \mathsf{dec}^{\mathrm{B}}\, [\mathsf{KEY}, \mathsf{AUT}]$ and the ideal world $S := \mathsf{sim}^{\mathrm{E}}\, \mathsf{SEC}$, depicted below.



The simulator works by initially choosing a random secret key k according to the key distribution P_K and then forwarding any input $\diamond$ at the outside interface to the inside interface, and after (immediately) obtaining an integer ℓ from the latter, choosing a uniformly random message $\widetilde{m}$ of length ℓ, computing the encryption of $\widetilde{m}$, i.e., $\widetilde{c} = E(\widetilde{m}, k)$ for fresh and independent randomness, and outputting $\widetilde{c}$ at the outside interface.

Let $V \in \{S_t^{\mathsf{rro\text{-}0}}, S_t^{\mathsf{rro\text{-}1}}\}$ be the system that D' is interacting with. D' needs to use the oracles provided by V in order to simulate R or S accordingly. To this end, D' internally keeps two lists $(x_1, \ldots, x_t) \in (\mathcal{M} \cup \{\bot\})^t$ and $(y_1, \ldots, y_t) \in (\mathcal{C} \cup \{\bot\})^t$, both initialized to $(\bot, \ldots, \bot)$. Then D' exports interfaces A, B, and E towards D and works as follows:

- On the i-th input $m \in \mathcal{M}$ at interface A, set $x_i := m$, obtain c by querying m to V, and set $y_i := c$.
- On the i-th input $\diamond$ at interface B, return x_i (at the same interface).
- On the i-th input $\diamond$ at interface E, return y_i (at the same interface).

Observe that if $V = S_t^{\mathsf{rro\text{-}0}}$, then D' perfectly emulates the real world R towards D, whereas if $V = S_t^{\mathsf{rro\text{-}1}}$, then D' perfectly emulates the ideal world S towards D. Therefore,

$$\begin{aligned}\Delta^{D'}(S_t^{\mathsf{rro\text{-}0}}, S_t^{\mathsf{rro\text{-}1}}) &= \Pr^{D' S_t^{\mathsf{rro\text{-}1}}}[Z' = 1] - \Pr^{D' S_t^{\mathsf{rro\text{-}0}}}[Z' = 1] \\ &= \Pr^{DS}[Z = 1] - \Pr^{DR}[Z = 1] \\ &= \Delta^{D}(R, S).\end{aligned}$$

2.3 Information Theoretically Secure Message Authentication

In the 1-message MAC-forgery game for f, the adversary can obtain the tags for up to one message of her choice. Hence, there are two ways to win the game: One option for the adversary is to ask for the tag for a message m and then submit a message $m' \neq m$ together with a valid tag for m' (this is called a *substitution attack*). The other option is directly submit a message m together with a valid tag for this message (this is called *impersonation attack*).

Let the key K be uniformly distributed over $\mathcal{K}$. This induces for each message $m \in \mathcal{M}$ a random variable $f(m, K)$, which corresponds to the tag for m. The MACs we provide in all subtasks will have the following two properties:

1. For each message $m \in \mathcal{M}$, the tag $f(m, K)$ is uniformly distributed. This guarantees that the success probability of an impersonation attack is bounded by $1/|\mathcal{T}|$.
2. For two different messages $m, m' \in \mathcal{M}$, the tags $f(m, K)$ and $f(m', K)$ are independent. This ensures that asking for a valid tag for the message m does not help the adversary to guess the tag for m'. Together with the property above, we thus have that the success probability of a substitution attack is also bounded by $1/|\mathcal{T}|$.

If both properties hold, the winning probability of any adversary in the 1-message MAC-forgery game is hence bounded by $1/|\mathcal{T}|$.

a) Consider the MAC $f\colon \{0,1\} \times \{0,1\}^n \to \{0,1\}^{\frac{n}{2}}$ given by

$$f\big(m, (k_1, \ldots, k_n)\big) = \begin{cases} (k_1, \ldots, k_{\frac{n}{2}}), & m = 0 \\ (k_{\frac{n}{2}+1}, \ldots, k_n), & m = 1. \end{cases}$$

Since the key is uniformly distributed, we obviously have that the tags for both possible messages are uniform, too. Furthermore, the tags for the messages 0 and 1 are independent since the bits in the key are independent. Therefore, the winning probability of any adversary is upper bounded by $1/|\mathcal{T}| = 2^{-\frac{n}{2}}$.

b) We define the MAC function as follows:

$$f\big(m,(k_1,\dots k_n)\big) = \begin{cases} (k_1,\dots,k_{\frac{n}{2}}), & m=0 \\ (k_{\frac{n}{2}+1},\dots,k_n), & m=1 \\ (k_1\oplus k_{\frac{n}{2}+1},\dots,k_{\frac{n}{2}}\oplus k_n), & m=2. \end{cases}$$

As in subtask a), $f(0,K)$ and $f(1,K)$ are uniformly distributed and independent. By Exercise 1.2 we also have that $f(2,K)$ is uniformly distributed. Using Proposition 3.1 from the lecture notes, we can further deduce that $f(0,K)$ and $f(2,K)$ are independent: We have $f(2,K) = f(0,K)\oplus(k_{\frac{n}{2}+1},\dots,k_n)$. Since $(k_{\frac{n}{2}+1},\dots,k_n)$ is uniformly distributed and independent from $(k_1,\dots,k_{\frac{n}{2}}) = f(0,K)$, we have that $f(0,K)$ and $f(2,K)$ are independent. Similarly, we obtain that $f(1,K)$ and $f(2,K)$ are independent. Hence, the winning probability of any adversary is again upper bounded by $2^{-\frac{n}{2}}$.

c) The idea from the previous subtask can be generalized to the message space $\{0,1\}^{\frac{n}{2}}$ in the following way. Let $\varphi : \{0,1\}^{\frac{n}{2}} \to \mathbb{F}$ be a bijection from the bitstrings of length $\frac{n}{2}$ to the field elements $\mathbb{F} := \mathrm{GF}(2^{\frac{n}{2}})$ of $2^{\frac{n}{2}}$ elements. In fact, as you might remember from your discrete mathematics course, the standard example of $\mathrm{GF}(2^{\frac{n}{2}})$ consists of the polynomials of degree at most $\frac{n}{2}-1$ over $\mathbb{Z}_2$. Thus we have the canonical bijection

$$\varphi\colon (b_1,\dots,b_{\frac{n}{2}}) \mapsto b_1 X^{\frac{n}{2}-1} + \dots + b_{\frac{n}{2}-1}X + b_{\frac{n}{2}}.$$

With the help of φ we can identify the message space with the set $\mathbb{F}$. The key space is identified with the set $\mathbb{F}^2$ via the bijection

$$\varphi\times\varphi\colon (k_1,\dots,k_n) \mapsto \big(\varphi(k_1,\dots,k_{\frac{n}{2}}),\varphi(k_{\frac{n}{2}+1},\dots,k_n)\big).$$

Now let the MAC $f\colon \mathbb{F}\times\mathbb{F}^2 \to \mathbb{F}$ be given by

$$f\big(m,(k_1,k_2)\big) = k_1 m + k_2.$$

Since the second half K_2 of the key $K = K_1||K_2$ is uniformly distributed, it follows from Exercise 1.2 that, for each message $m \in \mathbb{F}$, the tag $f(m,K)$ is uniformly distributed. Moreover, we have for $m, m' \in \mathcal{M}$, $m \neq m'$,

$$\begin{aligned} \Pr[f(m,K)=t \ \wedge \ f(m',K)=t'] &= \Pr[K_1 m + K_2 = t \ \wedge \ K_1 m' + K_2 = t'] \\ &= \Pr\left[\begin{pmatrix} m & 1 \\ m' & 1 \end{pmatrix}\cdot\begin{pmatrix} K_1 \\ K_2 \end{pmatrix} = \begin{pmatrix} t \\ t' \end{pmatrix}\right] \\ &= 2^{-n} \\ &= \Pr[f(m,K)=t]\cdot\Pr[f(m',K)=t'], \end{aligned}$$

where we have used in the third step that there is exactly one pair (k_1,k_2) for which the equation holds, which follows from the fact that the determinant of the matrix is $m'-m \neq 0$. Hence, $f(m,K)$ and $f(m',K)$ are independent, and we again obtain that the winning probability of any adversary is upper bounded by $2^{-\frac{n}{2}}$.