1. Problem Session
Secure Channels
(Winter Term 2014/2015)

Bauhaus-Universität Weimar, Chair of Media Security
Prof. Dr. Stefan Lucks, Jakob Wenzel
URL: `http://www.uni-weimar.de/de/medien/professuren/mediensicherheit/teaching/`

Date: 21.10.2014 (1:30 pm) **Room:** SR013, B11

Information

- You can work in groups of at most **three students**. Only one write-up per group is required.
- I highly recommend to compose your solutions in LaTeX.
- A LaTeX template can be found on the homepage of the problem session.
- The explanations given below should just help solving the problem session. They will get formally defined later in the course.

Goal of this Problem Set: *In this problem set, you should learn how to look at a given cryptographic construction from different view points (attack scenarios). Further, you should understand which part fulfills which purpose.*

Chosen-Plaintext Attack (CPA): In the CPA scenario, an adversary $\mathcal{A}$ can ask an encryption oracle for the encryption of arbitrary messages $M_1, \ldots, M_q$, receiving the corresponding ciphertexts $C_1, \ldots, C_q$. It is only bounded by the number of queries q and by the restriction that it is not allowed to ask for the encryption of the same message twice.

Blockwise Adaptive Adversary: A blockwise adaptive adversary $\mathcal{A}$ encrypting a message $M = (m_1, \ldots, m_\ell)$ gets knowledge about the i-th ciphertext block c_i before it has to choose the $(i+1)$-th message block m_{i+1}.

Task 1 (4 Credits) CBC Encryption
Let CBC be defined as on Slide 7 of the lecture and let E_K be a secure block cipher. Thus, a message $M = (m_1, \ldots, m_\ell)$ is encrypted as follows, where $m_i, c_i \in \{0,1\}^n$ with $1 \leq i \leq \ell$:

$$\begin{aligned} c_0 &\xleftarrow{\$} \{0,1\}^n \\ c_i &\leftarrow E_K(m_i \oplus c_{i-1}) \\ \text{return } C &\leftarrow (c_0, \ldots, c_\ell), \end{aligned}$$

where $c_0 \xleftarrow{\$} \{0,1\}^n$ denotes that the value c_0 is chosen uniformly at random from the set $\{0,1\}^n$. Show that the CBC encryption algorithm is vulnerable against an **adaptive chosen-plaintext adversary** by presenting an attack in the **Real-or-Random-CPA Scenario** (see Slide 38).

Task 2 (2 Credits) Weak-CBC Encryption
Let Weak-CBC be a variant of the CBC encryption scheme, where the initialization vector c_0 is a constant value. A message $M = (m_1, \ldots, m_\ell)$ is encrypted as shown in Task 1 (except that c_0 is fixed and known). Show that Weak-CBC is vulnerable against a **non-adaptive chosen-plaintext adversary** by presenting an attack in the **Real-or-Random-CPA Scenario**.

Task 3 (4 Credits) Weak-CBC-MAC
Let Weak-CBC-MAC be a slightly changed variant of the CBC-MAC (see Slide 12), where the initialization vector c_0 is chosen uniformly at random from the set $\{0,1\}^n$. Again, let E_K be a secure block cipher. Thus, the authentication tag T for a message $M = (m_1, \ldots, m_\ell)$ is computed as follows, where $m_i, c_i \in \{0,1\}^n$ with $1 \leq i \leq \ell$:

$$
\begin{aligned}
c_0 &\xleftarrow{\$} \{0,1\}^n \\
c_i &\leftarrow E_K(m_i \oplus c_{i-1}) \\
T &\leftarrow c_\ell \\
\text{return } &(c_0, T).
\end{aligned}
$$

Assume that Eve asks for the tag T of a chosen message $M = (m_1, m_2, m_3)$ and receives the tuple (c_0, T). Show that Eve can easily find a message $M' \neq M$ which results in the same authentication tag T. Note that Eve can choose the value c_0.

Task 4 (3 Credits) CBC-MAC with Arbitrarily Large Messages
Let CBC-MAC be as defined on Slide 12. Show that it is easy to find two messages $M \neq M'$ with $|M| \neq |M'|$ and $T = T'$, where $T = \text{CBC-MAC}(M)$ and $T' = \text{CBC-MAC}(M')$.