Problem Set 1
Course **Secure Channels**
(Summer Term 2016)

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

Due Date: 19 April 2016, 1:30 PM, via email to `eik.list(at)uni-weimar.de`.

*Note: For all tasks, explain your solutions in brief in your own words. You can work in groups of at most **three students**. Only one write-up per group is required. The use of LaTeX is recommended; a LaTeX template file can be found on the website of the problem session.*

Note: *For all tasks, we assume* $E : \{0,1\}^k \times \{0,1\}^n \to \{0,1\}^n$ *is a secure block cipher, with a secret random key* $K \in \{0,1\}^k$ *chosen by the oracle.*

Task 1 – CBC-MAC (3 Credits)

Consider the following variant of CBC-MAC (see Slide 12) for fixed-length messages where the initialization value $C_0 \xleftarrow{\$} \{0,1\}^n$ is chosen uniformly at random and the authentication tag T for a message $M = (M_1, \ldots, M_m)$ is computed as follows:

$$\begin{aligned} &C_0 \xleftarrow{\$} \{0,1\}^n, \\ &C_i \leftarrow E_K(M_i \oplus C_{i-1}), \text{ for } 1 \le i \le m, \\ &T \leftarrow C_m. \end{aligned}$$

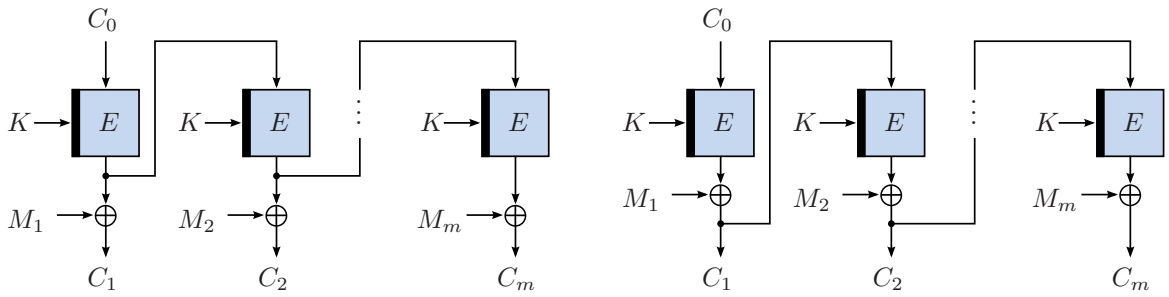
The MAC returns (C_0, T). Assume, the adversary $\mathcal{A}$ has obtained a valid pair (C_0, T) for a message M. Show *or* disprove that, with this information, $\mathcal{A}$ can efficiently find a valid pair (C_0', T') for a second message $M' \neq M$.

Task 2 – CBC-MAC (3 Credits)

Let CBC-MAC for arbitrary-length messages $M = (M_1, \ldots, M_m)$, be defined as described on Slide 12. So, $C_0 = 0^n$ for all messages. Show *or* disprove that one can efficiently find two messages $M \neq M'$ with $|M| \neq |M'|$ and $T = \text{CBC-MAC}_K(M) = \text{CBC-MAC}_K(M') = T'$.

Task 3 – Blockwise-Adaptive RoR-CPA Attacks (2 Credits)

Let Random-IV CBC be defined as on Slide 7, where the initial value $C_0 \xleftarrow{\$} \{0,1\}^n$ is chosen uniformly at random for each message. $\mathcal{A}$ is a blockwise-adaptive adversary against CBC, this means, $\mathcal{A}$ can see C_i before it has to choose M_{i+1}. Show how $\mathcal{A}$ can mount an efficient attack in the **Real-or-Random-Chosen-Plaintext** (RoR-CPA) model.



The OFB (left) and CFB (right) modes of operation.

Task 4 – Attacks on Further Modes (6 Credits)
In the following, we consider attacks on the OFB and CFB modes. Choose one of them: OFB *or* CFB. For each of the scenarios below, *either* argue comprehensibly why the mode is secure in the scenario (e.g. with a proof sketch as shown in the lecture) *or* show an efficient attack.

a) C_0 must be a nonce that is unique for each encrypted message and is chosen by the **Real-or-Random-CPA** adversary $\mathcal{A}$.

b) $C_0 \xleftarrow{\$} \{0,1\}^n$ is chosen uniformly at random by the oracle for each encrypted message. $\mathcal{A}$ is a **Real-or-Random-CPA** adversary.

c) $C_0 \xleftarrow{\$} \{0,1\}^n$ is chosen uniformly at random by the oracle for each encrypted message. $\mathcal{A}$ is a **Real-or-Random-CCA** adversary.

Task 5 – Generic Composition (4 Credits)
Assume, Alice combines the Counter mode with CBC-MAC in an authenticated encryption scheme. Given a message $M = (M_1, \ldots, M_m)$, her scheme first encrypts M in Random-IV CTR to $C = (C_0, C_1, \ldots, C_m)$ with a random initial value $C_0 \xleftarrow{\$} \{0,1\}^n$ (see Slide 52). Thereupon, an authentication tag $T = \text{CBC-MAC}_K(M)$ is computed from the same M using CBC-MAC. Finally, the scheme outputs $(C_0, C_1, \ldots, C_m, T)$ as authenticated ciphertext.
Say, Alice uses E_K with the same key for all block-cipher calls in Random-IV CTR and CBC-MAC. Show *either* why this scheme provides authenticity *or* show how you can efficiently find an authentic ciphertext for a message M', $M \neq M'$, without knowledge about K.