# Introduction to Cryptography - Exercise session 6

Prof. Sebastian Faust

November 28, 2018

In the first part of this exercise, we recall the new topics covered during the lecture: the block cipher AES and Message authentication codes (MACs). The second part of this sheet contains more interesting exercises.

---

PART 1

---

**Exercise 1 (MAC)**

(a) Give the definition of MAC.

(b) Explain with security experiments how would you define MAC.

(c) Define a new experiment $\mathsf{Mac\text{-}sforge}_{\mathcal{A},\Pi}(n)$, by modifying the above experiment such that adversary wins also if he outputs a new valid tag for a message queried earlier.

In the literature, the modified experiment $\mathsf{Mac\text{-}sforge}_{\mathcal{A},\Pi}(n)$ above is used in order to define a stronger version of the MAC, called *Strong MAC*. More precisely:

**Definition 1 (Strong MAC)** *A message authentication code* $\Pi = (\mathsf{Gen}, \mathsf{Mac}, \mathsf{Vrfy})$ *is strongly secure or a strong MAC, if for all probabilistic polynomial-time adversaries* $\mathcal{A}$*, there is a negligible function* $\mathsf{negl}$ *such that:*

$$\Pr[\mathsf{Mac\text{-}sforge}_{\mathcal{A},\Pi}(n) = 1] \leq \mathsf{negl}$$

**Exercise 2 (Canonical Verification)**

Let $(\mathsf{Gen}, \mathsf{Mac}, \mathsf{Vrfy})$ be a MAC scheme, where $\mathsf{Mac}$ is a deterministic algorithm. Explain how $\mathsf{Vrfy}$ works.

## PART 2

**Exercise 3 (Size of a tag)**

Say $\Pi = (\mathsf{Gen}, \mathsf{Mac}, \mathsf{Vrfy})$ is a secure MAC, and for $k \in \{0,1\}^n$ the tag-generation algorithm $\mathsf{Mac}_k$ always outputs tags of length $t(n)$. Prove that if $t(n) = \mathcal{O}(\log(n))$ then $\Pi$ cannot be a secure MAC.

**Exercise 4 (Canonical Verification $\implies$ Strong MAC)**

Let $\Pi = (\mathsf{Gen}, \mathsf{Mac}, \mathsf{Vrfy})$ be a secure MAC, where $\mathsf{Mac}$ is deterministic and $\mathsf{Vrfy}$ uses canonical verification. Prove that $\Pi$ is a strong MAC.

**Exercise 5 (Strong MAC)**

Let $F_k$ be a PRF and let $\Pi = (\mathsf{Gen}, \mathsf{Mac}, \mathsf{Vrfy})$ be a MAC defined as follows:

1. $\mathsf{Gen}(1^n)$: outputs a uniform key $k \in \{0,1\}^n$
2. $\mathsf{Mac}_k(m) := (F_k(m) \parallel F_k(m))$
3. $\mathsf{Vrfy}_k(m,t)$: outputs 1 if and only if $t = (F_k(m) \parallel F_k(m))$

(a) Prove that $\Pi$ is a secure MAC.

(b) Is $\Pi$ from part (a) strongly secure? Explain your answer.

(c) Prove or disprove: If $\Pi = (\mathsf{Gen}, \mathsf{Mac}, \mathsf{Vrfy})$ is a strongly secure MAC then $\mathsf{Mac}$ is a pseudorandom function.

**Exercise 6 (Constructions using a PRF)**

Let $F$ be a pseudorandom function. Show that each of the following message authentication codes is insecure, even if used to authenticate fixed-length messages. (In each case the shared key outputed by $\mathsf{Gen}$ is a random $k \in \{0,1\}^n$ and $< i >$ denotes an $n/2$-bit encoding of the integer $i$.

(a) To authenticate a message $m = m_1, \ldots, m_l$, where $m_i \in \{0,1\}^n$, compute

$$t := F_k(m_1) \oplus \cdots \oplus F_k(m_l)$$

(b) To authenticate a message $m = m_1, \ldots, m_l$, where $m_i \in \{0,1\}^{n/2}$, compute

$$t := F_k(< 1 > || m_1) \oplus \cdots \oplus F_k(< l > || m_l)$$

(c) To authenticate a message $m = m_1, \ldots, m_l$, where $m_i \in \{0,1\}^{n/2}$, choose a random $r \leftarrow \{0,1\}$ and compute

$$t := (r, F_k(r) \oplus F_k(< 1 > || m_1) \oplus \cdots \oplus F_k(< l > || m_l)).$$

**Exercise 7 (AES)**

Let the plaintext be $M = \{000102030405060708090A0B0C0D0E0F\}$ and the key be $K = \{01010101010101010101010101010101\}$

(a) Show the original contents of State and the Key, displayed as a $4 \times 4$ matrix.

(b) Show the value of State after initial AddRoudKey (Hint: the key $K_0$ is equal to the original AES key).

(c) Show the value of State after SubBytes. You can find the substitution table at the end of this exercise sheet.

(d) Show the value of State after ShiftRows.

(e) Explain how to compute the State after MixColumns (as a voluntary homework exercise, you can try to explicitly compute the State).

| | 0 | 1 | 2 | 3 | 4 | 5 | 6 | 7 | 8 | 9 | a | b | c | d | e | f |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| 00 | 63 | 7c | 77 | 7b | f2 | 6b | 6f | c5 | 30 | 01 | 67 | 2b | fe | d7 | ab | 76 |
| 10 | ca | 82 | c9 | 7d | fa | 59 | 47 | f0 | ad | d4 | a2 | af | 9c | a4 | 72 | c0 |
| 20 | b7 | fd | 93 | 26 | 36 | 3f | f7 | cc | 34 | a5 | e5 | f1 | 71 | d8 | 31 | 15 |
| 30 | 04 | c7 | 23 | c3 | 18 | 96 | 05 | 9a | 07 | 12 | 80 | e2 | eb | 27 | b2 | 75 |
| 40 | 09 | 83 | 2c | 1a | 1b | 6e | 5a | a0 | 52 | 3b | d6 | b3 | 29 | e3 | 2f | 84 |
| 50 | 53 | d1 | 00 | ed | 20 | fc | b1 | 5b | 6a | cb | be | 39 | 4a | 4c | 58 | cf |
| 60 | d0 | ef | aa | fb | 43 | 4d | 33 | 85 | 45 | f9 | 02 | 7f | 50 | 3c | 9f | a8 |
| 70 | 51 | a3 | 40 | 8f | 92 | 9d | 38 | f5 | bc | b6 | da | 21 | 10 | ff | f3 | d2 |
| 80 | cd | 0c | 13 | ec | 5f | 97 | 44 | 17 | c4 | a7 | 7e | 3d | 64 | 5d | 19 | 73 |
| 90 | 60 | 81 | 4f | dc | 22 | 2a | 90 | 88 | 46 | ee | b8 | 14 | de | 5e | 0b | db |
| a0 | e0 | 32 | 3a | 0a | 49 | 06 | 24 | 5c | c2 | d3 | ac | 62 | 91 | 95 | e4 | 79 |
| b0 | e7 | c8 | 37 | 6d | 8d | d5 | 4e | a9 | 6c | 56 | f4 | ea | 65 | 7a | ae | 08 |
| c0 | ba | 78 | 25 | 2e | 1c | a6 | b4 | c6 | e8 | dd | 74 | 1f | 4b | bd | 8b | 8a |
| d0 | 70 | 3e | b5 | 66 | 48 | 03 | f6 | 0e | 61 | 35 | 57 | b9 | 86 | c1 | 1d | 9e |
| e0 | e1 | f8 | 98 | 11 | 69 | d9 | 8e | 94 | 9b | 1e | 87 | e9 | ce | 55 | 28 | df |
| f0 | 8c | a1 | 89 | 0d | bf | e6 | 42 | 68 | 41 | 99 | 2d | 0f | b0 | 54 | bb | 16 |