𝔽oundations of Cybersecurity
Exercise Sheet 7
Singapore University of Technology and Design
October 25, 2017

*Note*: Some notes.

- There can be multiple acceptable answers. Justify carefully your reasoning.
- Go to the point, avoid copying verbatim definitions from the slides or the book.
- Show the solutions of classwork (groups of max 3 persons) to an instructor before the end of the class.
- Submit your homework solutions (groups of max 2) to eDimension by the deadline below.

## Classwork due on Wednesday October 25, 10:00 PM

### Question 1

Hash `"Foundations of Cybersecurity"` using SHA-512.

### Question 2

Compute any official test vector of HMAC-SHA256 (see `https://tools.ietf.org/html/rfc4868#section-2.7.2.1`).

### Question 3

Let us define a hash function $H_n(.)$ that executes SHA-512 and outputs the $n$ bits. Find a collision of $H_8$, $H_{16}$, $H_{24}$, $H_{32}$, and $H_{40}$. Measure how long it takes to find a collision.

### Question 4

For $H_8$, $H_{16}$, $H_{24}$, $H_{32}$ and $H_{40}$ find a preimage of the corresponding hashes: `"\00"`, `"\00"*2`, `"\00"*3`, `"\00"*4`, and `"\00"*5`. Measure how long it takes to find a preimage.

**Homework** due on Wednesday November 01, 6:59 PM

## Question 1

Using the collision files from `https://shattered.io/` create a new SHA-1 collision.

## Question 2

Find two messages that produce the same tag for AES-based CBC-MAC. Show code that demonstrates that.

## Question 3

Let's assume that CBC-MAC is used as a MAC scheme. Suppose $c$ is one block long, $a$ and $b$ are strings that are a multiple of the block length, and $MAC_K(a\|c) = MAC_K(b\|c)$. Then $MAC_K(a\|d) = MAC_K(b\|d)$ for any block $d$. Explain why this claim is true.