SUTD 51.505: 𝔽oundations of Cybersecurity (2018)

Exercise Sheet 8
November 2, 2018

- List your names (max 3 members for each group) on the answer sheet, **if you have actually worked on the exercises.**
- Answer questions in the same order as in the exercise sheet.
- Type in 12pt font, with 1.5 line spacing.
- There can be multiple acceptable answers. Justify carefully your reasoning.
- Go to the point, avoid copying verbatim definitions from the slides or the book.
- Submit your classwork and homework solutions (in pdf file) to eDimension by the deadlines below. Each group only needs one submission.
- Grading: total 100 points for each classwork and homework, each exercise has equal points in the same classwork and homework.

Classwork due on Friday November 2, 10:00 PM

Exercise 1
Hash `"51.505-Foundations-of-Cybersecurity-MSSD"` and `"51.505-Foundations-of-Cybersecurity-MSSd"`, respectively using SHA1. Observe the difference of these 2 hash values.

Exercise 2
Compute any official test vector of HMAC-SHA256 (see `https://tools.ietf.org/html/rfc4868#section-2.7.2.1`).

Exercise 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.

Exercise 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 Friday November 9, 6:59 PM

Exercise 1
Design a new mechanism to defend the length extension attack against MD-based hash functions.

Exercise 2
Find two messages that produce the same tag for AES-based CBC-MAC. Show code to demonstrate that.

Exercise 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.

Exercise 4
Suppose message a is one block long. Suppose that an attacker has received the MAC t for a using CBC-MAC under some random key unknown to the attacker. Explain how to forge the MAC for a two block message of your choice. What is the two-block message that you chose? What is the tag that you chose? Why is your chosen tag a valid tag for your two-block message?