SUTD 51.505: 𝔽oundations of Cybersecurity (2018)

Exercise Sheet 5
October 12, 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 October 12, 10:00 PM

Exercise 1

Estimate the security level of your credit card (assume that an adversary knows your name).

Exercise 2

Consider a group of 30 users who wish to establish pair-wise secure communications using symmetric-key cryptography. How many keys each user will have? How many keys in total are needed for 30 users?

Exercise 3

Suppose a chosen-cyphertext attacker cannot recover the secret decryption key for an encryption scheme. Does this mean the encryption scheme is secure? Why?

Exercise 4

Use the `aes_enc()` function (see below) to encrypt the *BLK.BMP* file from `http://www.fileformat.info/format/bmp/sample/index.htm`. Do you see any patterns in the ciphertext?

```
from Crypto.Cipher import AES

def aes_enc(key, msg):
    cipher = AES.new(key, AES.MODE_ECB)
    return cipher.encrypt(msg)
```

Exercise 5

Use `aes_enc()` to implement the encryption function of AES-CBC. Verify your implementation against the official test vectors (`https://tools.ietf.org/html/rfc3602#section-4`, Case#4).

Homework due on Friday October 26, 6:59 PM

Exercise 1

Encrypt the following plaintext P (represented with 8-bit ASCII) using AES-ECB, with the key of 128-bit 0. You may use an existing crypto library for this exercise.

P = `SUTD-MSSD-51.505*Foundations-CS*`

a) What is the ciphertext C?

b) Swap the two blocks of C, what is the plaintext P1?

c) Change the last bit of C, what is the plaintext P2?

d) Discuss possible attacks against AES-ECB based on the results of a) - c).

e) How would you address those attacks?

Exercise 2

The ciphertext (in hex)

```
87 F3 48 FF 79 B8 11 AF 38 57 D6 71 8E 5F 0F 91
7C 3D 26 F7 73 77 63 5A 5E 43 E9 B5 CC 5D 05 92
6E 26 FF C5 22 0D C7 D4 05 F1 70 86 70 E6 E0 17
```

was generated with the 256-bit AES key (also hex)

```
80 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 01
```

using CBC mode with a random IV. The IV is included at the beginning of the ciphertext. Decrypt this ciphertext. You may use an existing crypto library for this exercise.

Exercise 3

With your AES-CBC implementation encrypt 160MB of zeros:

```
"\x00"*int(1.6*10**8)
```

under 128-bit long zeroed key and IV. What is the last 128 bits of the ciphertext? Compare efficiency (time) of your implementation with a chosen library or tool that offers AES-CBC.

Exercise 4

Let P be the plaintext, and $l(P)$ be the length of P in bytes. Let b the block size of the block cipher in bytes. Explain why the following is not a good padding scheme.

a) Determine the minimum number of padding bytes necessary in order to pad the plaintext to a block boundary.

b) This is a number n which satisfies $0 \leq n \leq b - 1$ and $n + l(P)$ is a multiple of b.

c) Pad the plaintext by appending n bytes, each with value n.

Exercise 5

Compare the security and performance advantages and disadvantages of each variant of CBC mode with a) fixed IV, b) counter IV, c) random IV, and d) nonce-generated IV.

Exercise 6

An adversary observes the communication encrypted using CTR mode with the same fixed nonce. The nonce is hardcoded, so it is not included in the ciphertext. The adversary knows the following 16-byte ciphertext C

```
46 64 DC 06 97 BB FE 69 33 07 15 07 9B A6 C2 3D,
```

the following 16-byte ciphertext C'

```
51 7E CC 05 C3 BD EA 3B 33 57 0E 1B D8 97 D5 30,
```

and the plaintext P corresponding to C

```
43 72 79 70 74 6F 67 72 61 70 68 79 20 43 72 79.
```

What information, if any, can the adversary infer about the plaintext P' (corresponding to C')?