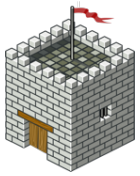
𝔽oundations of Cybersecurity
Exercise Sheet 5
Singapore University of Technology and Design
October 11, 2017



- 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 11, 10:00 PM

Question 1

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

Question 2

Using the `aes_enc()` function (see below) 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)
```

Question 3

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#1 and #4).

Homework due on Wednesday October 25, 6:59 PM

Question 1

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.

Question 2

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 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').

Question 3

Let P_1, P_2 be a message that is two blocks long, and let P_1' be a message that is one block long. Let C_0, C_1, C_2 be the encryption of P_1, P_2 using CBC mode with a random IV and a random key, and let C_0', C_1' be the encryption of P_1' using CBC mode with a random IV and the same key. Suppose an attacker knows P_1, P_2 and suppose the attacker intercepted and thus know C_0, C_1, C_2 and C_0', C_1'. Further suppose that, by random chance, $C_1' = C_2$. Show that the attacker can compute P_1'.