National Taiwan Normal University
CSIE Information Security

Instructor: Po-Wen Chi
Due Date: April 12, 2021, PM 11:59

Assignment 2

Policies:

- Zero tolerance for late submission.
- Please pack all your submissions in one zip file. **RAR is not allowed!!**
- I only accept **PDF**. MS Word is not allowed.
- Hand-writing is not allowed.
- Please use **Chinese.**

2.1 Pseudo Random Function (10 pts)

Let F be a secure PRF defined over $(\mathcal{K}, \mathcal{X}, \mathcal{Y})$, where $\mathcal{K} = \mathcal{X} = \mathcal{Y} = \{0,1\}^n$. Prove that $F_2(k,(x,y)) := F(k,x) \oplus F(k,y)$ is insecure.

2.2 PRF in Feistel Network (10 pts)

Please prove that if the function F in the feistel network is a secure PRF (pseudo random function), then the feistel network based PRP (pseudo random permutation) is secure.

2.3 Slide Attack (10 pts)

In this class, I have told you that a mandatory requirement of a Feistel network encryption is that the key in each round must be independent. If not, there will be an attack called slide attack.

So what is a slide attack? Please read the reference paper and describe it in your own words.

2.4 DES Complement (10 pts)

Let $\bar{X}$ be the bitwise complement of X and $\mathbf{DES}_k$ be the DES encryption function with the key k.

1. If $Y = \mathbf{DES}_k(X)$, please prove that $\bar{Y} = \mathbf{DES}_{\bar{k}}(\bar{X})$. (10 pts)

   - Hint: In this class, I did not use too much time on DES key expansion and data expansion. You may need more information to prove this. All you need is in the wikipedia. https://en.wikipedia.org/wiki/DES_supplementary_material
   - Hint: $\overline{A \oplus B} = \bar{A} \oplus B$.
   - Do not forget! DES is based on the Fiestel Network.

2. We say that if we want to launch a brute force attack on DES, we need to try 2^{56} keys. Will the result of the previous question change this claim? (5 pts)

2.5 Ciphertext Stealing (10 pts)

In cryptography, ciphertext stealing (CTS) is a general method of using a block cipher mode of operation that allows for processing of messages that are not evenly divisible into blocks **without resulting in any expansion of the ciphertext**, at the cost of slightly increased complexity. Figure 2.1 is how encryption works.

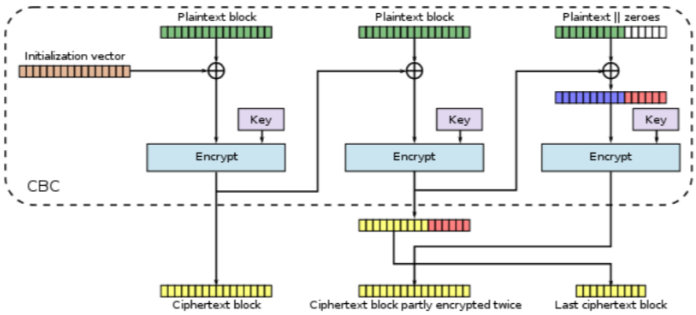

FIGURE 2.1: Ciphertext Stealing.

Please write down how decryption works.

2.6 Fermat's Theorem (10 pts)

Please get the following answers:

- $4^{255} \bmod 13$.
- $7^{1013} \bmod 93$.

2.7 Euler's Theorem and RSA (10 pts)

In this class, I have introduced Euler's Theorem to you as follows.

THEOREM 2.1. *For every a and n that are relatively prime, then*

$$a^{\phi(n)} \equiv 1(mod\ n).$$

However, when we run RSA permutation, m and $N = pq$ may not be relatively prime. When m and $N = pq$ are not relatively prime, will the reverse permutation still work? Why or why not?

Hint: I do not know how you will prove. As for me, I use the Chinese remainder theorem.

2.8 Programming: Padding Oracle Attack (15 pts)

In this class, I have introduced why we need padding. In fact, there is a specification about padding. In PKCS#7, the padding is working as follows. Padding is in whole bytes. The value of each added byte is the number of bytes that are added, i.e. N bytes, each of value N are added. For example, if you need to pad three bytes, you will append [0x03 0x03 0x03] to the message. If you need to pad five bytes, you will append [0x05 0x05 0x05 0x05 0x05] to the message. This is a very smart way, right?

Unfortunately, someone may misuse this padding technique. For example, the receiver may send a response to the sender to tell if the ciphertext is valid padding or not. The attacker can use this mechanism to decrypt the whole ciphertext. How to do this? I put a reference on my site and you can reference it. Of course, you can also reference wikipedia or other information from Internet.

Now I prepare a server for you to **play** this attack. Note that the encryption is AES CBC mode.

- http://140.122.185.210:8080/
- http://140.122.185.210:8080/oracle/xxx

2.9 Lab: Random Number Generator (15 pts)

In this class, I have told you that there is no real pseudo random number generator (PRG). However, PRG is very important to us. How does a

system generate a random number? This lab will guide you to see how your system works.

- Lab: https://seedsecuritylabs.org/Labs_20.04/Crypto/Crypto_Random_Number/

You need to submit a detailed lab report, with screenshots, to describe what you have done and what you have observed. You also need to provide explanation to the observations that are interesting or surprising. Please also list the important code snippets followed by explanation. Simply attaching code without any explanation will not receive credits.