Introduction to Information Security
2020 Spring
Assignment 02

Instructor: Po-Wen Chi

Due: 2020.04.26 PM 11:59

Policies:

- **Zero-tolerance to delay** unless you can persuade me with some good reasons.
- Please pack all your submissions in one zip file.
- I only accept ".pdf" format. MS Word ".doc" and hard-copy are not allowed in this class.
- You can answer complete homework in Chinese or English. Copy and paste is not allowed. You can reference some data but write the answers in your own words. I will randomly picks someone to explain his/her answer in class.
- I will randomly picks someone to demonstrate labs in class. The demonstrator will get one additional point. If fail, the student will get no lab scores. I promise that everyone will be picked at most once.

1 Modular Multiplicative Inverse (9 pts)

Please find the modular multiplicative inverse of the following number. Please write down how you find it. If you give the answer directly without the process, you will get zero points.

1. 135 mod 61
2. 7465 mod 2464
3. 42828 mod 6407

2 Fermat's Theorem (6 pts)

Please get the following answers:

- 4^{255} mod 13.
- 7^{1013} mod 93.

3 Chinese Remainder Theorem (15 pts)

In number theory, the Chinese remainder theorem states that if one knows the remainders of the Euclidean division of an integer n by several integers, then one can determine uniquely the remainder of the division of n by the product of these integers, under the condition that the divisors are pairwise coprime. That is, given

$$n \equiv \begin{cases} n_1 \bmod p_1 \\ n_2 \bmod p_2 \\ \vdots \\ n_k \bmod p_k \end{cases},$$

where $p_1, \ldots, p_k$ are pairwise coprime, n is unique in $\mathbb{Z}_{p_1 \ldots p_k}$.

1. Please prove this theorem and show how to get n (10 pts).
2. Why do we need the condition that $p_1, \ldots, p_k$ are pairwise coprime? Please give an example to show that when $p_1, \ldots, p_k$ are not pairwise coprime, you cannot get a unique n (5 pts).

4 Complement (15 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)

5 Polynomial Ring (15 pts)

In mathematics, especially in the field of algebra, a polynomial ring or polynomial algebra is a ring formed from **the set of polynomials** in one or more variables with coefficients in another ring, often a field.

Since this is a ring, Euclidean Algorithm also works. Now please determine the gcd of the following pairs of polynomials:

1. $(x^3 + 1)$ and $(x^2 + x + 1)$, where the coefficient is in $\mathbb{Z}_2$.
2. $(x^3 + x + 1)$ and $(x^2 + 1)$, where the coefficient is in $\mathbb{Z}_3$.
3. $(x^4 + 8x^3 + 7x + 8)$ and $(2x^3 + 9x^2 + 10x + 1)$, where the coefficient is in $\mathbb{Z}_{11}$.

Please write down how you calculate the answers. Do not give your answer directly.

6 Programming: Padding Oracle Attack (20 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://140.122.185.173:8080/`
- `http://140.122.185.173:8080/oracle/xxx`

7 Lab: RSA (20 pts)

In this class, I have introduced how RSA works. Now it is your term to see how to use RSA in your programming. Please follow the links here.

`http://www.cis.syr.edu/~wedu/seed/Labs_16.04/Crypto/Crypto_RSA/Crypto_RSA.pdf`

As before, you need to write down a report.