Introduction to Information Security
HW4 report

B10832018
官澔

[Structure tree]

github : 110-Information-Security
| ----HW1
| ----HW2
| ----HW4
| ---- RSA.py
| ---- Report.pdf

- Key generation:

  Here's my method in the key generator:

  1. First, define a table that stores prime numbers from 2 to 1000. This step is to accelerate by testing the small prime number first.
  2. Randomly generate a large number for p and q. When the number pass the prime number table test, the Miller Robin test will be used.
  3. After finding p and q, then follow the step of RSA to find the last variables.
  4. The generate test of public key e is start from 65537.
- Encrypt:
  1. Transform the plaintext into interger.
  2. Count the ciphertext by **plaintext ^ e mod n** where n is p * q
  3. Encode ciphertext into base64
- Decrypt:
  1. Decode ciphertext into interger.
  2. Count **ciphertext ^ d mod n = plaintext**
  3. Transform back into ascii
- CRT:
  1. The CRT method simplify the calculation of modulo and exponential to big numbers using Chinese remainder theorem.
- Square and multiply:
  1. First convert the exponential number into binary and do the iteration. If 1 is iterated, do square and multiply. Otherwise just do multiplication.
  2. Each step modulo the result number by **n,** finally we get the result of **a^b mod n**