Network Security Project 1 Report

An-Fong Hwu 胡安鳳 0416324

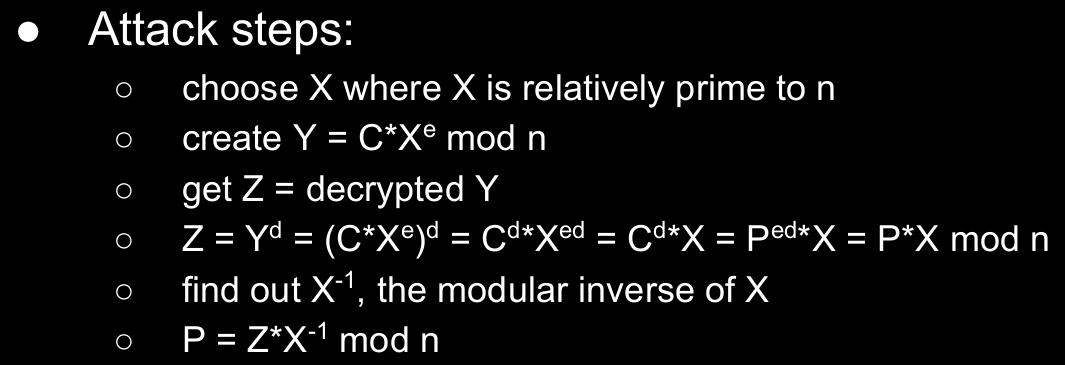
\* What is the “Chosen Ciphertext Attack?”

The chosen cipher attack is an attack where the cryptanalyst can gather information by obtaining the decryptions of chosen ciphertexts. From these pieces of information the adversary can attempt to recover the hidden secret key used for decryption.

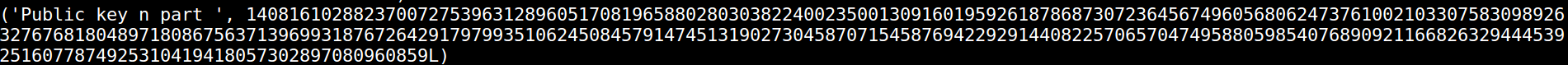
\*Algorithm implementation of CCA in this project



Algorithm procedure as shown in pdf from TA.



Step 1. As shown on above, the rsa-n is a huge integer, and X should be relatively prime to N, since N is odd number



and we have to choose an X for co-prime, the smallest select I will try 2(the forged number in source code).

Step 2. We get Y with the mathematical operation below.



Since the encrypted data are written in the base64 form, hence the following step is needed:

a. decode with base64.b64decode (base64-->ASCII).

b. re-encode with hex, every byte(ASCII is encoded byte-wisely) can be convert to 2 hex number.

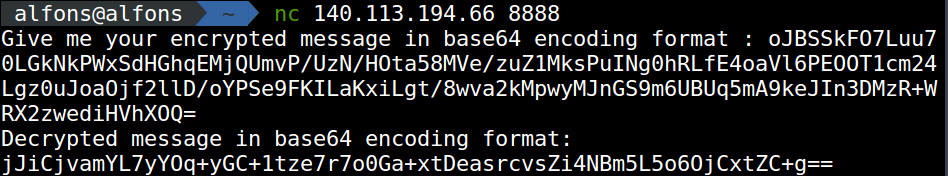
c. do chosen\_ciphertext operation , that is chosen\_ciphertext = ciphertext \* (forged\_number ^ rsa\_e) % rsa\_n

d. re-dncode with ASCII, every 2 hex can be converted to a byte,namely ASCII-encoded data.

e. encode with base64.b54encode (ASCII-->base64).

in that, the a b and d e are reverse operations to each other.

Step 3. Input the chosen\_ciphertext into TA’s server to get Z = decrypted Y from TA’s public key.



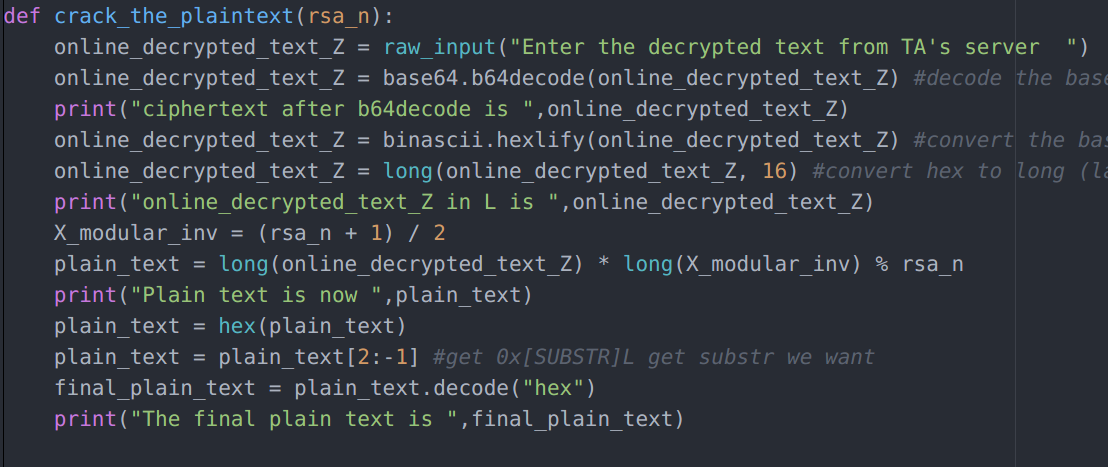
Z is jJiCjvam…...+g== (this is also encoded in base64)

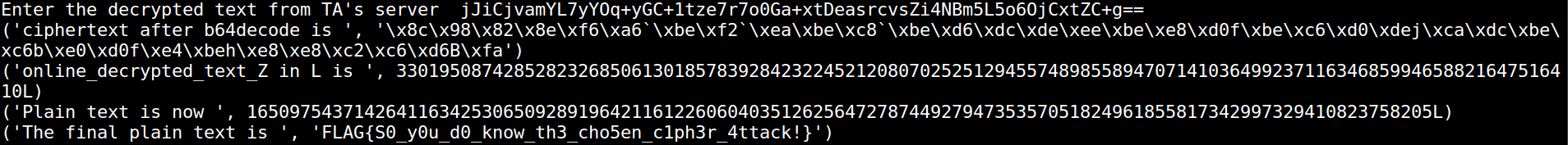
Step 4.

P , the plaintext equals to Z\*X^-1 mod n, where X is the modular inverse of X under N.

Since X = 2, then X^-1 under N will be (N+1)/2. So the final plaintext can be acquired.

We just need to be cautious about the encoding as well, the decoding is similar to that of above, but we decode with hex to ASCII for final FLAG information.





\*More thoughts about this project

1. Why will the CCA work? What is the mathematical theory behind it?

2. Why do we use the base-64 encoding in this project?