Project 1 - Hacking the cipher report

ID No.0656122
Name:陳奕佳

Programming enviroment: Python3.6

Dependency: pycrypto

Decrypt Steps:

A. Peparation

- Using Python Package: Crypto to extract n and e from public key.

```
n =  14081610288237007275396312896051708196588028030382240023500130916019592618786873072364567496056806247376100210330758309892632767681804897180867563713969931876726429179799351062450845791474513190273045870715458769422929144082257065704749588059854076890921166826329444539251607787492531041941805730289708096085965537
e =  65537
```

- Decode flag.enc with base64 and convert it to long type integer C.

B. Chosen X

- find a number X where X is relatively prime to n.
  In this case $X = 2$

C. Creating fake message and get decrypted message back

- Compute $msg = C * X^e \ (mod\ n)$
- Convert msg to byte string and encode with base64

```
==Fake message==
oJBSSkFO7Luu70LGkNkPWxSdHGhqEMjQUmvP/UzN/HOta58MVe/zuZ1MksPuINg0hRLfE4oaVl6PEOOT1cm24Lgz0uJoaOjf2llD/oYPSe9FKILaKxiLgt/8wva2kMpwyMJnGS9m6UBUq5mA9keJIn3DMzR+WRX2zwediHVhXOQ=
```

- Send to decryptor server and get decrypted message back.

```
Decrypted message in base64 encoding format:
jJiCjvamYL7yYOq+yGC+1tze7r7o0Ga+xtDeasrcvsZi4NBm5L5o6OjCxtZC+g==
```

- Decode decrypted message with base64 and convert it to long type integer Z.

D. Decrypting flag.enc

- Find the X^{-1} where X^{-1} is modular inverse of X

```
Modular Inverse of X =  70408051441185036376981564480258540982940140151911200117500654580097963093934365361822837480284031236880501051653791549463163838409024485904337818569849659383632145898996755312254228957372565951365229353577293847114645720411285328523747940299270384454605834131647222696258038937462655209709028651448540480430
```

- Decrypt flag by $P = Z * X^{-1} (mod\ n)$
- Convert long type integer to byte string. Completed!

```
FLAG{S0_y0u_d0_know_th3_cho5en_c1ph3r_4ttack!}
```

Script:

- createMessage.py - for step A, B, C
- decryptMessge.py - for step D