CTF Design Report

Xiang Lingzhi-20457448

Statement:

1. Alice sent Bob a cipher message: U2FsdGVkX19Xq0vznMbGKI20gaBIprP5DxGhy2LrRRCQFRO7uDfzc53sLbyZ5SmFEEPrRyTEZS7dsVO5AAW9LesiFzHhbVmJHiLS2webaR0JG9rqLR7FUmmuN038ptNdb/t8WbHAspw7CzFiCmsdTg==
2. Bob needs a key to decrypt the cipher message, so Alice uses Bob’s public key to encrypt the key as cipher\_key to Bob.
3. However, Alice made some mistakes when encrypting the key, the key decrypted from the cipher\_key is not the original key.
4. You need to find the true key to help Bob decrypt the cipher message.
5. Please input the plain message to capture the flag or input Hint1 or Hint2 to get hints.

Hint:

1. The cipher message and cipher\_key may be encoded by base64 or md5, the cipher message may be encrypted by symmetric encryption.
2. You can check these two websites to find inspiration of the original key:
   1. <https://www.wikiwand.com/en/Thomas_Edison>
   2. <https://www.inc.com/kevin-daum/37-quotes-from-thomas-edison-that-will-bring-out-your-best.html>

Flag:

I spent ninety-nine percent perspiration on COMP 7170 but failed on one percent inspiration

Program:

1. Open cmd or powershell or terminal
2. Cd destination of program file, like cd ~/desktop
3. Input java -jar test.jar
4. Input the plain message to capture the flag or input Hint1 or Hint2 to gain hints.
5. Github: https://github.com/yinb2/7170

# CTF Write Up Template

|  |  |
| --- | --- |
| CTF Challenge Number | CTF Design |
| Date of completion | 4.9 |
| CTF Team | Grou7 |
| CTF Flag | I spent ninety-nine percent perspiration on COMP 7170 but failed on one percent inspiration |

## Describe the steps involved to find out the CTF Flag.

Ans: (attached image when necessary)

1. Decrypted the cipher\_key with PriKey.pem to gain the symmetric key:
   1. openssl rsautl -decrypt -in cipher\_key -inkey PriKey.pem -out plain
   2. R2VuaXVzIGlzIG5pbmV0eS1uaW5lIHBlcmNlbnQgaW5zcGlyYXRpb24gYW5kIG9uZSBwZXJjZW50IHBlcnNwaXJhdGlvbg0K
2. Decode the plain by base64:
   1. echo "R2VuaXVzIGlzIG5pbmV0eS1uaW5lIHBlcmNlbnQgaW5zcGlyYXRpb24gYW5kIG9uZSBwZXJjZW50IHBlcnNwaXJhdGlvbg0K" | openssl enc -base64 -d
   2. Genius is ninety-nine percent inspiration and one percent perspiration
3. Find the true key then encode by base64:
   1. Genius is one percent inspiration and ninety-nine percent perspiration
   2. R2VuaXVzIGlzIG9uZSBwZXJjZW50IGluc3BpcmF0aW9uIGFuZCBuaW5ldHktbmluZSBwZXJjZW50IHBlcnNwaXJhdGlvbg0K
4. Decrypt the cipher message with key by AES-128-CBC then gain the plain message:
   1. echo "U2FsdGVkX19Xq0vznMbGKI20gaBIprP5DxGhy2LrRRCQFRO7uDfzc53sLbyZ5SmFEEPrRyTEZS7dsVO5AAW9LesiFzHhbVmJHiLS2webaR0JG9rqLR7FUmmuN038ptNdb/t8WbHAspw7CzFiCmsdTg==" | openssl aes-128-cbc -d -k "R2VuaXVzIGlzIG9uZSBwZXJjZW50IGluc3BpcmF0aW9uIGFuZCBuaW5ldHktbmluZSBwZXJjZW50IHBlcnNwaXJhdGlvbg0K" -base64
   2. I spent ninety-nine percent perspiration on COMP 7170 but failed on one percent inspiration

## Describe any theory involved this CTF challenge.

Ans: (attached image when necessary)

1. RSA:
   1. According to number theory, it is relatively simple to find two large prime numbers, but it is extremely difficult to factorize their product, so the product can be disclosed as an encryption key
   2. Anyone can encrypt the plaintext with public key, but only authorized users can decrypt the ciphertext with private key.
2. AES:
   1. AES is working on the 4x4 byte-matrix which is called state and for each state it will take following four steps:
      1. AddRoundKey: In each encryption cycle, a round key (generated by the Rijndael key generation scheme) will be generated by the master key. This key will have the same size as the original matrix to match each corresponding word in the original matrix.
      2. SubBytes: S-box is constructed by combining the inverse elements of multiplication and a reversible affine transformation matrix. In addition, when constructing the S-box, fixed points and anti-fixed points were deliberately avoided, that is, the result of replacing bytes with S-box would be equivalent to the result of misalignment.
      3. ShiftRows: Shift each row in the matrix circularly.
      4. MixColumns: This step uses linear transformation to mix each inline four bytes
3. Base64: One of the most popular encoding method for transmitting 8Bit.

## Describe any bad practices/area to improve in this challenge to make it more secure.

Ans: (attached image when necessary)

1. The symmetric key encrypted by public key are binary characters which cannot be directly copied on the terminal.
2. Using RSA to encrypt the symmetric key to ensure the security of symmetric key when symmetric is leaked during the transmission. Without private key of Bob, it’s hard to obtain the symmetric key for intruders.

## References

(optional)