Project 1 - Hacking the Cipher

Network Security
By Wei-Ti Su & Xin-Yu Wang

Outline

- RSA: introduction
- Chosen ciphertext attack
- PEM format
- The decrypter on the server
- Summary

RSA: introduction

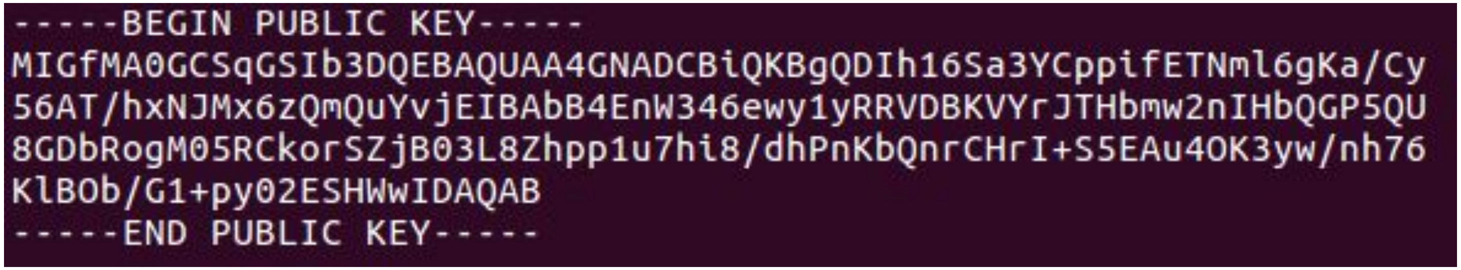
- Public key encryption
  - Key pair: public and private key
    - Public key: open to the public
    - Private key: confidential
  - Messages encrypted with one key can only be decrypted by the other key
- Components of RSA
  - n - the modulus of the keys, created as a product of two large prime numbers, p and q
  - (n, e) - the public key
  - (n, d) - the private key
- Encryption with public key
  - ciphertext = plaintext^{e} mod n
- Decrytption with private key
  - plaintext = cipthertext^{d} mod n
  - cipthtext^{d} mod n = plaintext^{ed} mod n = plaintext^{1} mod n

Chosen ciphertext attack

- Components of RSA
  - C - the ciphertext you want to attack ($C = P^e \bmod n$)
  - n - the modulus of the keys, created as a product of two large prime numbers, p and q
  - (n, e) - the public key
  - (n, d) - the private key
- Attack steps:
  - choose X where X is relatively prime to n
  - create $Y = C*X^e \bmod n$
  - get Z = decrypted Y
  - $Z = Y^d = (C*X^e)^d = C^d*X^{ed} = C^d*X = P^{ed}*X = P*X \bmod n$
  - find out X^{-1}, the modular inverse of X
  - $P = Z*X^{-1} \bmod n$

PEM format

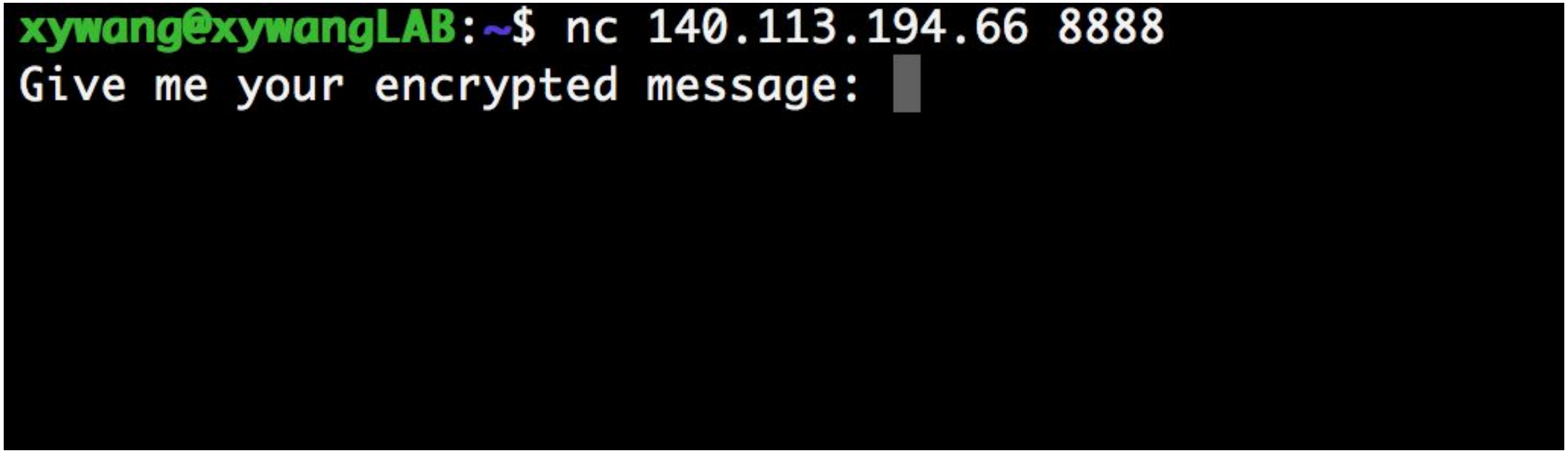
- The public key is in PEM format
- Extract n and e from the public key



```
-----BEGIN PUBLIC KEY-----
MIGfMA0GCSqGSIb3DQEBAQUAA4GNADCBiQKBgQDIh16Sa3YCppifETNml6gKa/Cy
56AT/hxNJMx6zQmQuYvjEIBAbB4EnW346ewy1yRRVDBKVYrJTHbmw2nIHbQGP5QU
8GDbRogM05RCkorSZjB03L8Zhpp1u7hi8/dhPnKbQnrCHrI+S5EAu4OK3yw/nh76
KlBOb/G1+py02ESHWwIDAQAB
-----END PUBLIC KEY-----
```

The decryper on the server

- nc 140.113.194.66 8888 (linux command)
- input ciphertext and you’ll get the decrypted one back



```
xywang@xywangLAB:~$ nc 140.113.194.66 8888
Give me your encrypted message: 
```

Summary

- You are given:
  - pub.pem: the RSA public key
  - flag.enc: the encrypted message
  - decrypter.py: the source code of the decrypter running on the server
- Your goal:
  - to retrieve flag, it should be like FLAG{.......}
- You should deliver:
  - flag: the decrypted message
  - report.pdf: a report about how you decrypt flag.enc
  - any code or script you write
  - Pack all the files into STUDENT_ID.zip
- You should finish this project and upload to e3 platform before the deadline: 2018/04/03 (Tue) 23:59:59

All kind of plagiarism is strictly forbidden. If you plagiarize, you will fail the course and/or face disciplinary action. Also, do not DoS our server!