Project 1 - Hacking the Cipher

Network Security
By Po-Hsing Wu & Te-Yu Chang

Outline

- RSA: introduction
- Common Factor Attacks
- PEM format
- Summary

RSA: introduction

- Public key encryption
  - Key pair: public and private key
    - Public key: public knowledge
    - 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
  - e - the public key
  - d - the private key
- Encryption with public key
  - encrypted_text = plaintext^e mod n
- Decryption with private key
  - plaintext = encrypted_text^d mod n

RSA: introduction

- Factoring N
  if we can factoring *N* into *p* and *q*, we can easily get the private key *d* by calculating

$$d \equiv e^{-1} \pmod{(p-1)(q-1)}$$

- But factoring integers is believed to be a NP problem. There is no algorithm has been published that can factor all integers in polynomial time.

Common Factor Attacks

- Suppose there are four different primes, a, b, c, and d. The first two are used in one key, in the public value $n_1 = a \times b$. The other two are used in another key, in the public value $n_2 = c \times d$.

  $gcd(n_1, n_2) = 1$

- In the other scenario, there are now only three different primes a, b, and c. The public values are $n_1 = a \times b$ and $n_2 = b \times c$.

  $gcd(n_1, n_2) = b$

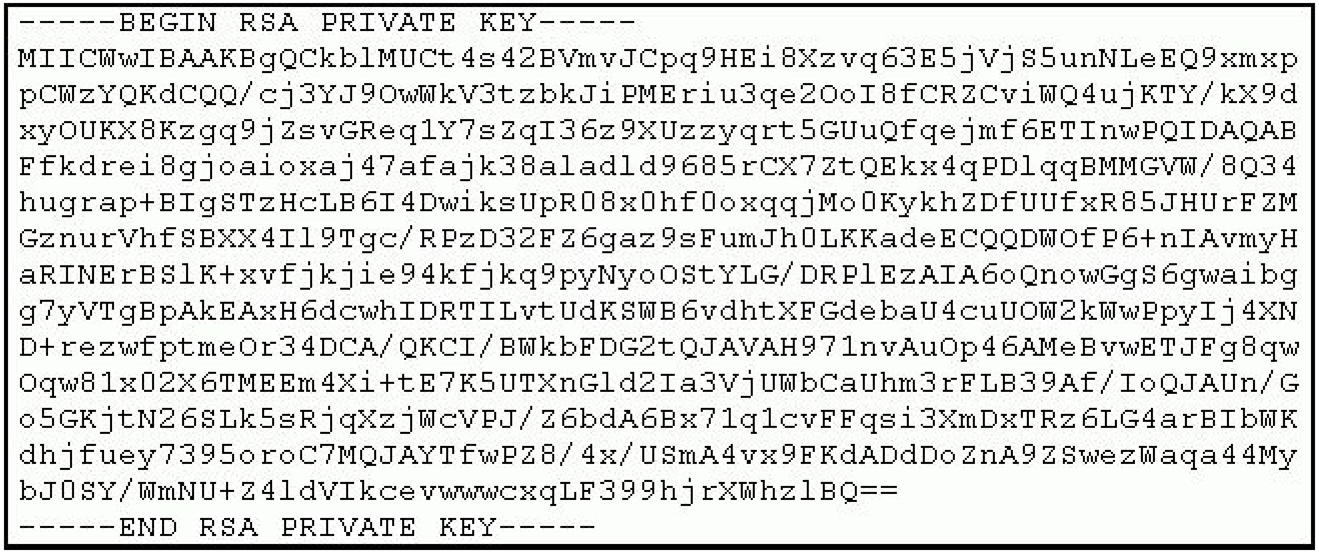
After we know *b* is one of the prime, we can easily get the other by divide *N* by *b*

$a = n_1 / b$,   private key = $e^{-1} \pmod{(a-1)(b-1)}$

For more details, please refer to http://www.loyalty.org/~schoen/rsa/

PEM format

- Please submit the private keys in PEM format
- There are many tools able to generate private keys in PEM format. You are free to use any tools or libraries to solve this project.



```
-----BEGIN RSA PRIVATE KEY-----
MIICWwIBAAKBgQCkblMUCt4s42BVmvJCpq9HEi8Xzvq63E5jVjS5unNLeEQ9xmxp
pCWzYQKdCQQ/cj3YJ9OwWkV3tzbkJiPMEriu3qe2OoI8fCRZCviWQ4ujKTY/kX9d
xyOUKX8Kzgq9jZsvGReq1Y7sZqI36z9XUzzyqrt5GUuQfqejmf6ETInwPQIDAQAB
Ffkdrei8gjoaioxaj47afajk38aladld9685rCX7ZtQEkx4qPDlqqBMMGVW/8Q34
hugrap+BIgSTzHcLB6I4DwiksUpR08x0hf0oxqqjMo0KykhZDfUUfxR85JHUrFZM
GznurVhfSBXX4Il9Tgc/RPzD32FZ6gaz9sFumJh0LKKadeECQQDWOfP6+nIAvmyH
aRINErBSlK+xvfjkjie94kfjkq9pyNyoOStYLG/DRPlEzAIA6oQnowGgS6gwaibg
g7yVTgBpAkEAxH6dcwhIDRTILvtUdKSWB6vdhtXFGdebaU4cuUOW2kWwPpyIj4XN
D+rezwfptmeOr34DCA/QKCI/BWkbFDG2tQJAVAH971nvAuOp46AMeBvwETJFg8qw
Oqw81x02X6TMEEm4Xi+tE7K5UTXnGld2Ia3VjUWbCaUhm3rFLB39Af/IoQJAUn/G
o5GKjtN26SLk5sRjqXzjWcVPJ/Z6bdA6Bx71q1cvFFqsi3XmDxTRz6LG4arBIbWK
dhjfuey7395oroC7MQJAYTfwPZ8/4x/USmA4vx9FKdADdDoZnA9ZSwezWaqa44My
bJ0SY/WmNU+Z41dVIkcevwwwcxqLF399hjrXWhzlBQ==
-----END RSA PRIVATE KEY-----
```

An example of PEM formatted private key

Summary

- You are given:
  - 12 RSA public keys in publicKeys.zip
- Your goal:
  - Generate the private key within those 12 public keys, since two keys of them share a common factor
- You should deliver:
  - Report in the PDF format about how to get the private keys.
  - The two private keys have a common factor, named by ‘private<N>.pem’, where N is the number in ‘public<N>.pub’.
    For example, if you restore the private key of ‘public2.pub’, the private key filename is ‘private2.pem’.
  - Pack all the files into **STUDENT_ID.zip**
- You should finish this project and upload to e3 platform before the deadline: 2017/10/17 (Tuesday) 23:59:59

All kind of plagiarism is strictly forbidden. If you plagiarize, you will fail the course and/or face disciplinary action.