Khoa Khoa học & Kỹ thuật máy tính
Trường ĐH Bách Khoa TP.HCM

Cryptography and Network Security
Tutorial 3
RSA Algorithm

Hieu Nguyen

Ngày 3 tháng 3 năm 2015

Questions
1. What are the roles of the public and private key?
2. What are the roles of the public and private key?
3. What is a one-way function?
4. What is a trap-door one-way function?

Exercises
1. Perform encryption and decryption using the RSA algorithm, as in Figure 9.5 (text book), for the following:

   a. p = 3; q = 11, e = 7;M = 5

   b. p = 5; q = 11, e = 3;M = 9

   c. p = 7; q = 11, e = 17;M = 8

   d. p = 11; q = 13, e = 11;M = 7

   e. p = 17; q = 31, e = 7;M = 2

2. In a public-key system using RSA, you intercept the ciphertext C = 10 sent to a user whose public key is e = 5, n = 35.What is the plaintext M?

3. In an RSA system, the public key of a given user is e = 31, n = 3599.What is the private key of this user? Hint: First use trial-and-error to determine p and q; then use the extended Euclidean algorithm to find the multiplicative inverse of 31 modulo $\phi(n)$.

Extended Euclidean algorithm

```
Procedure Euclid_Extended (a,m)
int,  y0=0,y1:=1;

While a>0 do {
     r:= m mod a
     if r=0 then Break
     q:= m div a
     y:= y0-y1*q
     m:=a
     a:=r
     y0:=y1
     y1:=y
  }
 If a>1 Then Return null
 else Return y
```