科普新知

RSA 密碼系統

楊儒民*

在傳統對稱式密碼系統，發送端及接收端需各自擁有加／解密金匙，若 A 欲與 n 人通訊則需擁有 n 把加／解密金匙，在 n 人相乎通訊的系統則需產生 C(n,2) 把加／解密金匙，隨通訊人數增加，如何管理金匙成為一重要課題。

公開金匙密碼系統為所謂非對稱式密碼系統，A 擁有一把加密金匙 e 及一把解密金匙 d，其將 e 公開，而任何人欲與 A 通訊時，使用 e 將明文 m 加密產生密文 c，將 c 由不安全之通道(如網路等)傳送給 A，A 利用 d 將 c 還原成 m．由上知在公開金匙密碼系統中，任何人只要管理一把加密金匙及一把解密金匙就能在其系統中完成通訊的功能．簡化了金匙管理的問題，且有些公開金匙密碼系統除提供加／解密功能外，還可以作數位簽章（digital signature）的應用。

RSA 系統介紹

a, 金匙產生：

1:A 選擇二大質數 p ,q,且計算 n=p×q

2:A 選擇一整數 e 使得(e,n)=1 作為加密金匙,同時計算 d 使得 cd=1(m od (p-1)(q-1)) 作為解密金匙

3:A 將(e,n)公開,將 d 作為其私有解密之秘密金匙

b, 加密：

若 B 欲將明文 m(0≦m ≦n)傳送予 A ，B 利用公開之(e,n)計算密文 C，其中

* 楊儒民，南台科技大學通識教育中心自然科學組副教授。

南台通識電子報
2012 年 4 月 15 日出版
南台科技大學通識教育中心 發行
34

C=me(mod n)，將 C 傳送予 A

C, 解密

A 得到 C 後利用其秘密金匙 d 還原明文 m，計算

cd=med=m(modn)

Example 1:

設 A 之公開金匙(e,n)=(5,119)，119=7x17，則其秘密金匙 d=77，因 5x77=1(m od 6 x16)，設明文 m =19，則密文 c=195(m od 119)=66,之後解密計算 m =6677(m od 119)=19 可還原明文。

Exam ple 2:

設 A 之公開金匙(e,n)=(71,3233)，3233=53x61, 則其秘密金匙

d=791 ， 因 71 x 791=1(m od52 x 60) ， 設 明 文 m =1704 ， 則 密 文 c=170471(mod3233)=3106, 之後解密計算 m =3106791(m d3233)=1704 可還原明文·

R SA 密碼系統之證明有興趣之讀作者請參考〔4〕.

欲解此密碼系統,須先知 d 為何?而欲知 d 須由 p,q,e 得知.如何得知 p,q?須自 n 分解因數得到,但要將一大數分解因數自古以來是困難的.

Reference:

1:R ivest,R .;Sham ir,A .;and A delm an,L. “A m ethod for obtaining digital signatures and public key cryptosystem s.”C om m unications of the A C M ,February 1978.

2:W .D iffie and M .H ellm an,“N ew directions in C ryptography,”IEEE Trans.O n Info.Theory,V ol.IT-22(6),pp.644-654,N ov.1976.

3:D enning,D .E.,C ryptography and D ata Security,A ddison-W esley,R eading,M assachusetts,1982.

4:K .H .R osen,Elem entary N um ber Theory and Its A pplications,2nd ,A ddison W esley,1988.

5:賴溪松,張真誠等:近代密碼學及其應用.松崗.1995.

6: 張真誠:電腦密碼學與資訊安全. 松崗.1990.