电子科技大学
University of Electronic Science and Technology of China

计算机系统与网络安全技术

第一章 信息安全概述

-RSA算法

周世杰

计算机科学与工程学院

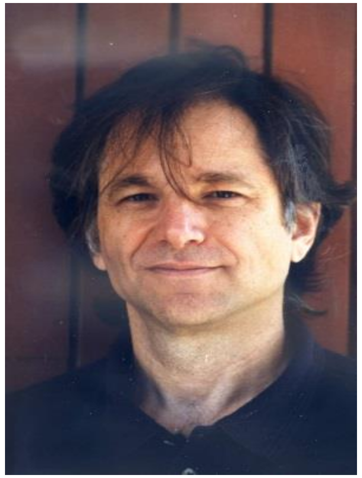
EMail: sjzhou@uestc.edu.cn

RSA算法的提出

- 1977年由Ron Rivest、Adi Shamir和Len Adleman发明，1978年公布。

Ronald L. Rivest

Adi Shamir



Leonard M. Adleman

RSA算法的描述

- 公钥：n（两素数p和q的乘积）和 e（与(p-1)(q-1)互素）
- 私密：d（ed≡1(mod(p-1)(q-1))
- 加密 $c=m^e \bmod n$
- 解密 $m=c^d \bmod n$

RSA算法密钥的生成原理

- 令$n=pq$, $p\neq q$都是素数,$\phi(n)=(p-1)(q-1)$是n的Euler数
- Euler定理推论:
  - 若$n=pq$, $p\neq q$都是素数, k是任意整数,则
  - $m^{k(p-1)(q-1)+1} \equiv m \bmod n$, 对任意$0\leq m\leq n$
- 只要选择公钥e, 则私钥d满足$ed=k\phi(n)+1$,即

  $ed \equiv 1 \bmod \phi(n)$ ➡ $d \equiv e^{-1} \bmod \phi(n)$
- 公钥: $K_U=\{e,n\}$, 私钥: $K_R=\{d,n\}$

使用RSA算法的过程

- 每个用户生成一对密钥（公钥和私钥）：
  - （1）用户选择两个大的随机素数 p， q
  - （2）计算N=p.q
  - （3）计算n的欧拉数： ø(N)=(p-1)(q-1)
  - （4）随机算则一个加密密钥e：1<e<ø(n)，gcd(e,ø(n))=1
  - （5）解以下方程得到解密密钥 d： e.d=1 mod ø(n) and 0≤d≤n
  - （6）加密消息M得到密文 $C=M^e \bmod N$
  - （7）解密密文得到明文 $M=C^d \bmod N$

RSA算法示例

1. 算则两个素数: p=17 & q=11
2. 计算 $n = pq$ =17×11=187
3. 计算 $\varnothing(n)=(p-1)(q-1)$=16×10=160
4. 选择e:gcd(e,160)=1; 其中e=7
5. 计算d: de=1 mod 160 and d < 160

   d=23 （因为23×7=161= 10×160+1）
6. 公布公钥KU={7,187}
7. 保存私钥KR={23,17,11}

RSA算法示例

- 如果待加密的消息 M = 88 (注意： 88<187)
- 加密： $C = 88^7 \bmod 187 = 11$
- 解密:$M = 11^{23} \bmod 187 = 88$

RSA算法示例

1. 若Bob选择了p=101和q＝113
2. 那么，n=11413, φ(n)=100×112＝11200
3. 然而11200＝2^6×5^2×7，一个正整数e能用作加密指数，当且仅当e不能被2，5，7所整除。
4. 假设Bob选择了e=3533，那么用扩展的Euclidean算法将求得：

   $d=e^{-1}\equiv 6597 \pmod{11200}$, 于是Bob的解密密钥d=6597

RSA算法示例

5. Bob在一个目录中公开n=11413和e=3533

6. 现假设Alice想发送明文9726给Bob，她计算：

7. 9726^{3533}(mod 11413)=5761，且在一个信道上发送密文5761。

8. 当Bob接收到密文5761时，他用他的秘密解密指数（私钥）d＝6597进行解密：

   5761^{6597}（mod 11413)=9726

RSA算法正确性证明

- 理论： 欧拉定理（Euler‘s Theorem）：
  - $a^{\varnothing(n)} \bmod N = 1$
  - $\gcd(a,N)=1$
- 在RSA中有:
  - $N=p.q$
  - $\varnothing(N)=(p-1)(q-1)$
  - 如果仔细选择 e & d 使得对某些k有： $e.d=1+k.\varnothing(N)$ 成立
- 于是就有:

$$C^d = (M^e)^d = M^{1+k.\varnothing(N)} = M^1.(M^{\varnothing(N)})^q = M^1.(1)^q = M^1 = M \bmod N$$

RSA算法的安全性

- RSA算法加密的安全性是基于加密函数$e_k(x)=x^e(\text{mod } n)$是一个单向函数，所以对攻击的人来说求逆计算不可行。
- 而Bob能解密的陷门是分解n=pq，知φ (n)=(p-1)(q-1)，从而用欧几里得算法根据公钥e解出解密私钥d。

因此，**RSA算法的安全性是基于大整数因子分解的困难性这个数学难题！**


谢谢！