信息安全 微课堂

信息安全概论

Introduction to Information Security

主讲教师：赵 彦 锋
院　　系：信息工程学院 软件工程系
邮　　箱：c_zhaoyf@163.com

2021 年 03 月

第四周

第四章 公钥密码体制

- 公钥密码体制的产生
- 数论基础
- 公钥密码体制的基本原理
- RSA公钥密码体制
- 其他公钥密码算法

传统密码体制在应用中的缺陷

- **密钥管理的麻烦**

  一个拥有10万用户的民用密码通信网就要拥有近50亿个密钥。

- **密钥难以传输**

- **不能提供法律证据**

  信息的证实是指两个方面：一方面是指对发送方的证实，另一方面是指对接收方的证实， 也就是能够确认接收方所收到和保存的信息确实是由发送方发出的。既不是伪造的，也没有经过包括接收方在内的其他人所篡改。

- **缺乏自动检测密钥泄密的能力**

- 1976年由当时在美国斯坦福大学的迪菲（Diffie）和赫尔曼(Hellman)发表了“New Direction in Cryptography”论文，第一次提出了公钥密码体制的概念。从此开创了密码学的新时代。
- 自1976年以来，已经提出了多种公钥密码算法，其安全基础是基于一些数学问题， 专家们认为这些问题在短期内不可能得到解决，因为一些问题（如因子分解问题）至今已有数千年的历史。

- 数论中的许多概念在设计公钥密码算法时是必不可少的。掌握这些基础知识对于理解公钥密码体制的原理和应用十分重要。

整 除

- 定理：设整数a和b，如果存在整数k，使b=ak，则说b能被a整除，记作：a|b
- 例：3|15，-15|60
- 性质：

  对所有整数a≠0， a|0、 a|a成立

  对任意整数b， 1|b成立

素数(prime number)

- 定义：如果整数p(p>1)只能被1或者它本身整除，而不能被其他整数整除，则其为素数，否则为合数。
- 素数定理：

设$\pi(x)$是小于x的素数的个数,则

$$\pi(x) \approx \frac{x}{\ln x}, \text{且当} x \to \infty, \frac{\pi(x)}{\frac{x}{\ln x}} \to 1$$

- 在各种应用中，我们需要大的素数,如100位的素数
- 素数是构成整数的因子，每一个整数都是由一个或几个素数的不同次幂相乘得来的。

2	101	211	307	401	503	601	701	809	0	1009	1103	1201	1301
3	103	223	311	409	509	607	709	811	911	1013	1109	1213	1303
5	107	227	313	419	521	613	719	821	919	1019	1117	1217	1307
7	109	229	317	421	523	617	727	823	929	1021	1123	1223	1319
11	113	233	331	431	541	619	733	827	937	1031	1129	1229	1321
13	127	239	337	433	547	631	739	829	941	1033	1151	1231	1327
17	131	241	347	439	557	641	743	839	947	1039	1153	1237	1361
19	137	251	349	443	563	643	751	853	953	1049	1163	1249	1367
23	139	257	353	449	569	647	757	857	967	1051	1171	1259	1373
29	149	263	359	457	571	653	761	859	971	1061	1181	1277	1381
31	151	269	367	461	577	659	769	863	977	1063	1187	1279	1399
37	157	271	373	463	587	661	773	877	983	1069	1193	1283	
41	163	277	379	467	593	673	787	881	991	1087		1289	
43	167	281	383	479	599	677	797	883	997	1091		1291	
47	173	283	389	487		683		887		1093		1297	
53	179	293	397	491		691				1097			
59	181			499									
61	191												
67	193												
71	197												
73	199												
79													
83													
89													
97													

最大公约数

- a和b的**最大公约数**是能够同时整除a和b的最大正整数，记为gcd(a,b)。
- 如果gcd(a,b)=1，则说a和b是**互素**的。
- 定理：

设a和b是两个整数(至少一个非0)， d=gcd(a,b)，则存在整数x和y，使得ax+by=d

特殊地，如果a和b互素，则有整数x和y，使得ax+by=1

同余

- 设整数a，b，n(n ≠0)，如果a-b是n的整数倍，则a≡b(mod n)，即a同余于b模n。也可理解为a/n的余数等于b/n的余数。
- (mod n)运算将所有的整数(无论小于n还是大于n)，都映射到{0,1,...,n-1}组成的集合。
- 模算术的性质：

$$(a \bmod n) + (b \bmod n) \equiv (a+b) \bmod n$$

$$(a \bmod n) - (b \bmod n) \equiv (a-b) \bmod n$$

$$(a \bmod n) * (b \bmod n) \equiv (a*b) \bmod n$$

- 设x= a mod n， y= b mod n。

  即$a=x+k_1n$，$b=y+k_2n$，k_1和k_2为整数。

  也就是： $x=a-k_1n$，$y=b-k_2n$

那么：

$(a \bmod n) \times (b \bmod n)$

$=xy= (a-k_1n)(b-k_2n)$

$=ab+(-ak_2-bk_1+k_1k_2n)n$。

- 因为a，b，k_1，k_2，n皆为整数，所以

  $(-ak_2-bk_1+k_1k_2n)=K$也是整数，即：

- $(a \bmod n) \times (b \bmod n)=ab+Kn$，

  即$(a \bmod n) \times (b \bmod n) \equiv (a \times b) \bmod n$。

得证。

性质1

- 有整数a，b，c，n(n ≠0)：

  如果a≡b(mod n)，b≡c(mod n)

  那么a≡c(mod n)

- 证明：

  因为a≡b(mod n)，b≡c(mod n)，

  即$a=b+k_1n$，$b=c+k_2n$，

  所以$a=c+k_2n+k_1n=c+(k_1+k_2)n$，

  即a等于c加上n的整数倍，即a≡c(mod n)。

性质2

- 有整数a，b，c，n(n ≠0)：

  如果a≡b(mod n)， c≡d(mod n)

  那么a+c≡b+d， a-c≡b-d， ac≡bd (mod n)

- 证明：

证明 ac≡bd (mod n)。

因为 a≡b(mod n)， c≡d(mod n)，

即 $a=b+k_1n$， $c=d+k_2n$，

所以， $ac=(b+k_1n)(d+k_2n)=bd+(bk_2+dk_1+nk_1k_2)n$，

其中 $K=(bk_2+dk_1+nk_1k_2)$为整数，

即： $ac=bd+Kn$， 即 ac≡bd (mod n)。

计算$11^7 \bmod 13$

如果a≡b(mod n)， c≡d(mod n)，则ac≡bd (mod n)

$\because 11 \equiv 11 \pmod{13}$

$\therefore 11^2 \equiv (11 \times 11) \pmod{13} \equiv 121 \pmod{13} \equiv 4 \pmod{13}$

$\therefore 11^4 \equiv 4^2 \pmod{13} \equiv 3 \pmod{13}$

$\therefore 11^7 \equiv (11 \times 4 \times 3) \pmod{13} \equiv 132 \pmod{13} \equiv 2 \pmod{13}$

$\therefore 11^7 \pmod{13} = 2$。

没有必要先计算11^7，然后除以13求余数。

除法

- 设整数a，b，c，n(n ≠0)，且gcd(a,n)=1。

  如果ab≡ac (mod n)，那么b≡c (mod n)

证明：∵ gcd(a,n)=1，∴有x和y，使ax+ny=1

两边同乘以(b−c)：　(b−c)(ax+ny)=b−c

即：(ab−ac)x+n(b−c)y=b−c　……①

∵ ab≡ac (mod n), 即ab=ac+k_1n, ∴ab−ac 是n的倍数

同时，n(b−c)y显然也是n的倍数

所以，：(ab−ac)x+n(b−c)y也是n的倍数，假设是k_2倍

则①式变为：b−c= k_2n

即b≡c (mod n)

欧几里得算法(The Euclidean Algorithm)

- 用欧几里德算法求最大公约数。欧几里德算法基于以下的定理：对于任意非负整数a和任意正整数b，有：　　gcd(a,b)=gcd(b,a mod b)
- 求：gcd(482,1180)

  1180=2*482+216

  482=2*216+50

  216=4*50+16

  50=3*16+2

  16=8*2+0

  所以gcd(482,1180)=2

乘法逆元

- 用如果gcd(a,b)=1，那么：

  存在a^{-1}，使$a* a^{-1} \equiv 1 \bmod b$

  存在b^{-1}，使$b* b^{-1} \equiv 1 \bmod a$

- 这里，把a^{-1}称为a模b的乘法逆元， b^{-1}称为b模a的乘法逆元

用扩展的欧几里得算法求乘法逆元

- gcd(11111,12345)

  12345=1*11111+1234

  11111=9*1234+5

  1234=246*5+4

  5=1*4+1

  4=4*1+0

- 1=5-1*4=5-1*(1234-246*5)=247*5-1*1234

  =247*(11111 - 9*1234) -1*1234

  =247*11111 - 2224*1234

  =247*11111 - 2224*(12345 -1*11111)

  =2471*11111 - 2224*12345

中国剩余定理(The Chinese Remainder Theorem)

- 我国古代数学名著《孙子算经》中，记载这样一个问题：“今有物不知其数，三三数之剩二，五五数之剩三，七七数之剩二，问物几何。”
- 明朝数学家程大位把这一解法编成四句歌诀：

三人同行七十（70）稀，
五树梅花廿一（21）枝，
七子团圆正月半（15），
除百零五（105）便得知。

歌诀中每一句话都是一步解法：第一句指除以3的余数用70去乘；第二句指除以5的余数用21去乘；第三句指除以7的余数用15去乘；第四句指上面乘得的三个积相加的和如超过105，就减去105的倍数，就得到答案了。即：

$$70\times2+21\times3+15\times2-105\times2=23$$

中国剩余定理(The Chinese Remainder Theorem)

- 中国剩余定理是指若有一些两两互素的整数$m_1,m_2,...,m_n$，则对任意的整数：$a_1,a_2,...a_n$，以下联立同余方程组对模$m_1*m_2*...*m_n$有公解：

$$\begin{cases} x \equiv a_1 \pmod{m_1} \\ x \equiv a_2 \pmod{m_2} \\ \quad \vdots \\ x \equiv a_n \pmod{m_n} \end{cases}$$

费尔马小定理(Fermat's Theorem)

- 如果p是一个素数,a不是p的倍数，
  则：$a^{p-1} \equiv 1 \pmod p$

证明：

设有一整数空间S={1,2,...,p-1}

再设有一函数Ψ(x)=ax(mod p) x∈S

(1)对于任何x∈S，有Ψ(x)∈S

(2)对于x和y(x≠y),有Ψ(x)≠Ψ(y)

(3)根据乘法定理和除法定理

$(p-1)!a^{p-1} \equiv (p-1)! \bmod p$

欧拉函数和欧拉定理

- Φ(n)：小于n且与n互素的正整数的个数
- 显然，对于素数p，有Φ(p)=p-1
- 设有两个素数p和q，p ≠q，那么对于n=pq，有：

  Φ(n)= Φ(pq)= Φ(p)* Φ(q)=(p-1)*(q-1)

欧拉定理(Euler's Theorem)

- 对于任意互素的a和n，有$a^{\Phi(n)} \equiv 1 \bmod n$

证明：对于整数n，与n互素的数有Φ(n)个：

令这些数为：$R=\{x_1, x_2, \ldots, x_{\Phi(n)}\}$

用a与R中的每个元素相乘模n，得到集合S：

$S=\{ax_1 \bmod n, ax_2 \bmod n, \ldots, ax_{\Phi(n)} \bmod n\}$

其实S就是R：

$(ax_1 \bmod n) \in R$

S中的元素是唯一的

那么：R中各元素相乘就等于S中各元素相乘：

$$\prod_{i=1}^{\phi(n)} x_i = \prod_{i=1}^{\phi(n)} ax_i \bmod n$$

离散对数(Discrete Logarithms)

- 由Euler定理可知，互素的a和n，有$a^{\Phi(n)} \equiv 1 \bmod n$

也就是说，至少存在一个整数m，使$a^m \equiv 1 \bmod n$成立

- 使得$a^m \equiv 1 \bmod n$成立的最小正幂m，称为a的阶、a所属的模n的指数，或a所产生的周期长。
- 本原根：如果使得$a^m \equiv 1 \bmod n$成立的最小正幂m：

$m=\Phi(n)$，则称a是n的本原根。

离散对数(Discrete Logarithms)

$7^1 \bmod 19=7$

$7^2 \bmod 19=11$

$7^3 \bmod 19=1$

$7^4 \bmod 19=(7^1\times7^3) \bmod 19=7\times1=7$

$7^5 \bmod 19=11$

因此，m=3，即7所属的模19的指数等于3.

a	a^2	a^3	a^4	a^5	a^6	a^7	a^8	a^9	a^{10}	a^{11}	a^{12}	a^{13}	a^{14}	a^{15}	a^{16}	a^{17}	a^{18}
1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1
2	4	8	16	13	7	14	9	18	17	15	11	3	6	12	5	10	1
3	9	8	5	15	7	2	6	18	16	10	11	14	4	12	17	13	1
4	16	7	9	17	11	6	5	1	4	16	7	9	17	11	6	5	1
5	6	11	17	9	7	16	4	1	5	6	11	17	9	7	16	4	1
6	17	7	4	5	11	9	16	1	6	17	7	4	5	11	9	16	1
7	11	1	7	11	1	7	11	1	7	11	1	7	11	1	7	11	1
8	7	18	11	12	1	8	7	18	11	12	1	8	7	18	11	12	1
9	5	7	6	16	11	4	17	1	9	5	7	6	16	11	4	17	1
10	5	12	6	3	11	15	17	18	9	14	7	13	16	8	4	2	1
11	7	1	11	7	1	11	7	1	11	7	1	11	7	1	11	7	1
12	11	18	7	8	1	12	11	18	7	8	1	12	11	18	7	8	1
13	17	12	4	14	11	10	16	18	6	2	7	15	5	8	9	3	1
14	6	8	17	10	7	3	4	18	5	13	11	2	9	12	16	15	1
15	16	12	9	2	11	13	5	18	4	3	7	10	17	8	6	14	1
16	9	11	5	4	7	17	6	1	16	9	11	5	4	7	17	6	1
17	4	11	16	6	7	5	9	1	17	4	11	16	6	7	5	9	1
18	1	18	1	18	1	18	1	18	1	18	1	18	1	18	1	18	1

本原根的性质

- 如果a是n的本原根，且：

  $x_1=a^1 \bmod n$，$x_2=a^2 \bmod n$，…，$x_{\Phi(n)}=a^{\Phi(n)} \bmod n$

- 则：

  $x_1 \neq x_2 \neq \ldots \neq x_{\Phi(n)}$，且$x_{\Phi(n)}=1$

- 特别的：对于素数p，若a是p的本原根，则：

  $(a^1 \bmod p) \neq (a^2 \bmod p) \ldots \neq (a^{p-1} \bmod p)$。

指标

- 某素数p，有本原根a，且：

$x_1=a^1 \bmod p$， $x_2=a^2 \bmod p$，…， $x_{p-1}=a^{p-1} \bmod p$，

则：$x_1 \neq x_2 \neq \ldots \neq x_{p-1}$

令：$S=\{x_1,x_2,\ldots,x_{p-1}\}$，$P=\{1,2,\ldots,p-1\}$

则：$S=P$

对于任意整数b，有$b \equiv r \bmod p$ $(0 \leqslant r \leqslant p-1)$

所以，对于b和素数p的本原根a，有唯一的幂i，使得：$b \equiv a^i \bmod p$，$0 \leqslant i \leqslant p-1$

指数i称为**a模p的b的指标**，或称离散对数,记为$\mathrm{ind}_{a,p}(b)$

指标的性质

$ind_{a,p}(1)=0$

$ind_{a,p}(a)=1$

乘法性质

$ind_{a,p}(xy)\equiv[ind_{a,p}(x)+ ind_{a,p}(y)] \bmod \Phi(p)$

幂性质

$ind_{a,p}(y^r)\equiv[r\times ind_{a,p}(y)] \bmod \Phi(p)$

离散对数的计算

- 对于方程$y=g^x \bmod p$

给定g,x,p,计算y比较容易。

但给定y,g,p,求x非常困难。$X=\mathrm{ind}_{g,p}(y)$

其难度与RSA中因子分解素数之积的难度有相同的数量级。

$ind_{a,p}(xy) \equiv [ind_{a,p}(x) + ind_{a,p}(y)] \bmod \Phi(p)$

因为 $x = a^{ind_{a,p}(x)} \bmod p$

$$y = a^{ind_{a,p}(y)} \bmod p$$

$$xy = a^{ind_{a,p}(xy)} \bmod p$$

所以 $a^{ind_{a,p}(xy)} \bmod p = a^{ind_{a,p}(x)+ind_{a,p}(y)} \bmod p$

根据欧拉定理，对于互素的整数a和p，有$a^{\Phi(p)} \equiv 1 \bmod p$，即$a^{p-1} \equiv 1 \bmod p$。

所以对于任意整数i，有$a^{i+k(p-1)} \bmod p = (a^i \bmod p)(a^{k(p-1)} \bmod p) = a^i \bmod p$。

所以：$ind_{a,p}(xy) = [ind_{a,p}(x) + ind_{a,p}(y)] + k(p-1) = [ind_{a,p}(x) + ind_{a,p}(y)] + k\Phi(p)$

即$ind_{a,p}(xy) \equiv [ind_{a,p}(x) + ind_{a,p}(y)] \bmod \Phi(p)$，得证。

- **公钥密码学与其他密码学完全不同：**
  - 公钥算法基于数学函数而不是基于替换和置换
  - 使用两个独立的密钥
- **公钥密码学的提出是为了解决两个问题：**
  - 密钥的分配
  - 数字签名
- 1976年Diffie和Hellman首次公开提出了公钥密码学的概念，被认为是一个惊人的成就。

1. **Plaintext:**
   - This is the readable message or data that is fed into the algorithm as input.
2. **Encryption algorithm:**
   - The encryption algorithm performs various transformations on the plaintext.
3. **Public and private keys:**
   - This is a pair of keys that have been selected so that if one is used for encryption, the other is used for decryption. The exact transformations performed by the algorithm depend on the public or private key that is provided as input.

4. Ciphertext:

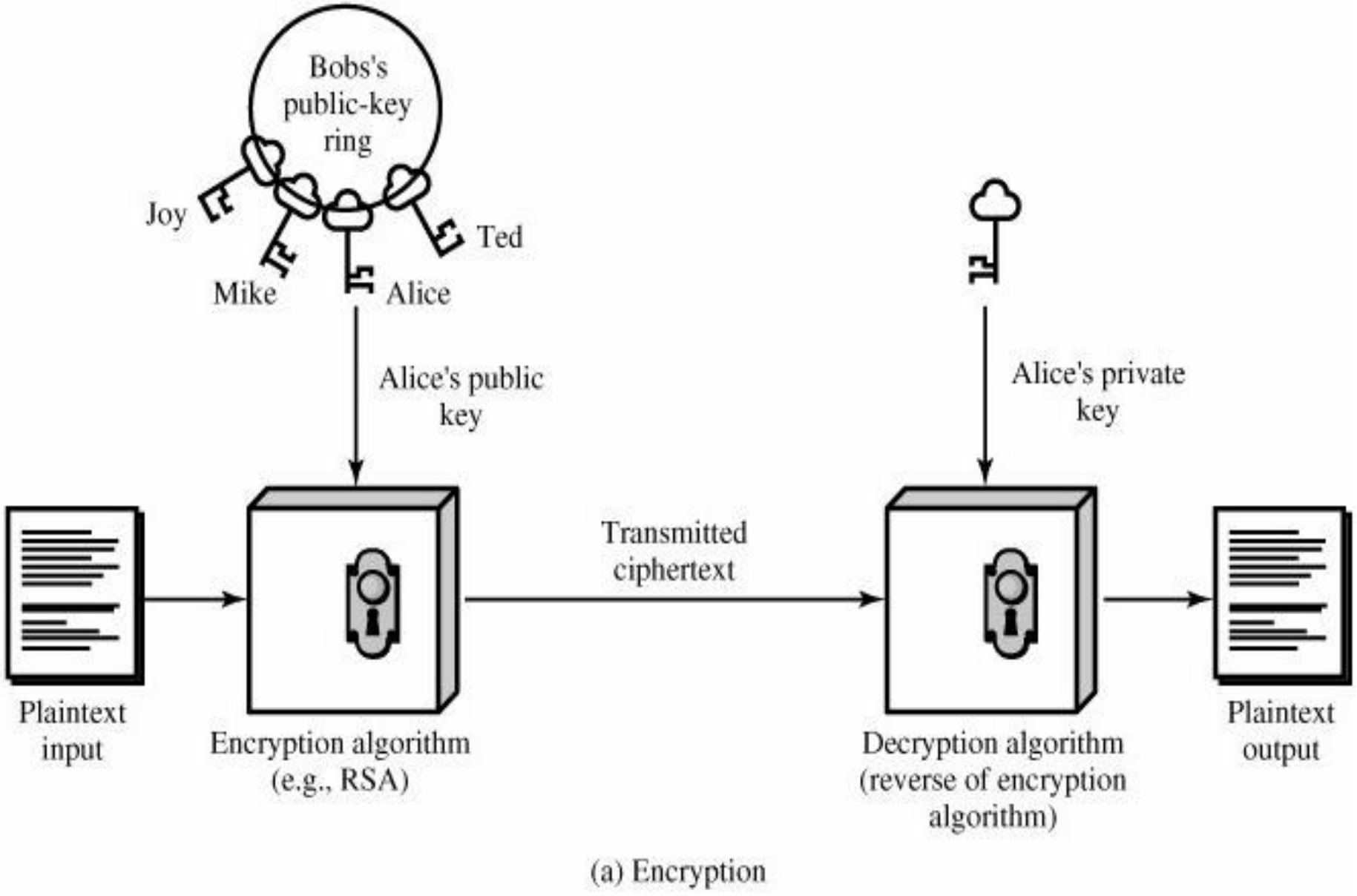
- This is the scrambled message produced as output. It depends on the plaintext and the key. For a given message, two different keys will produce two different ciphertexts.

5. Decryption algorithm:

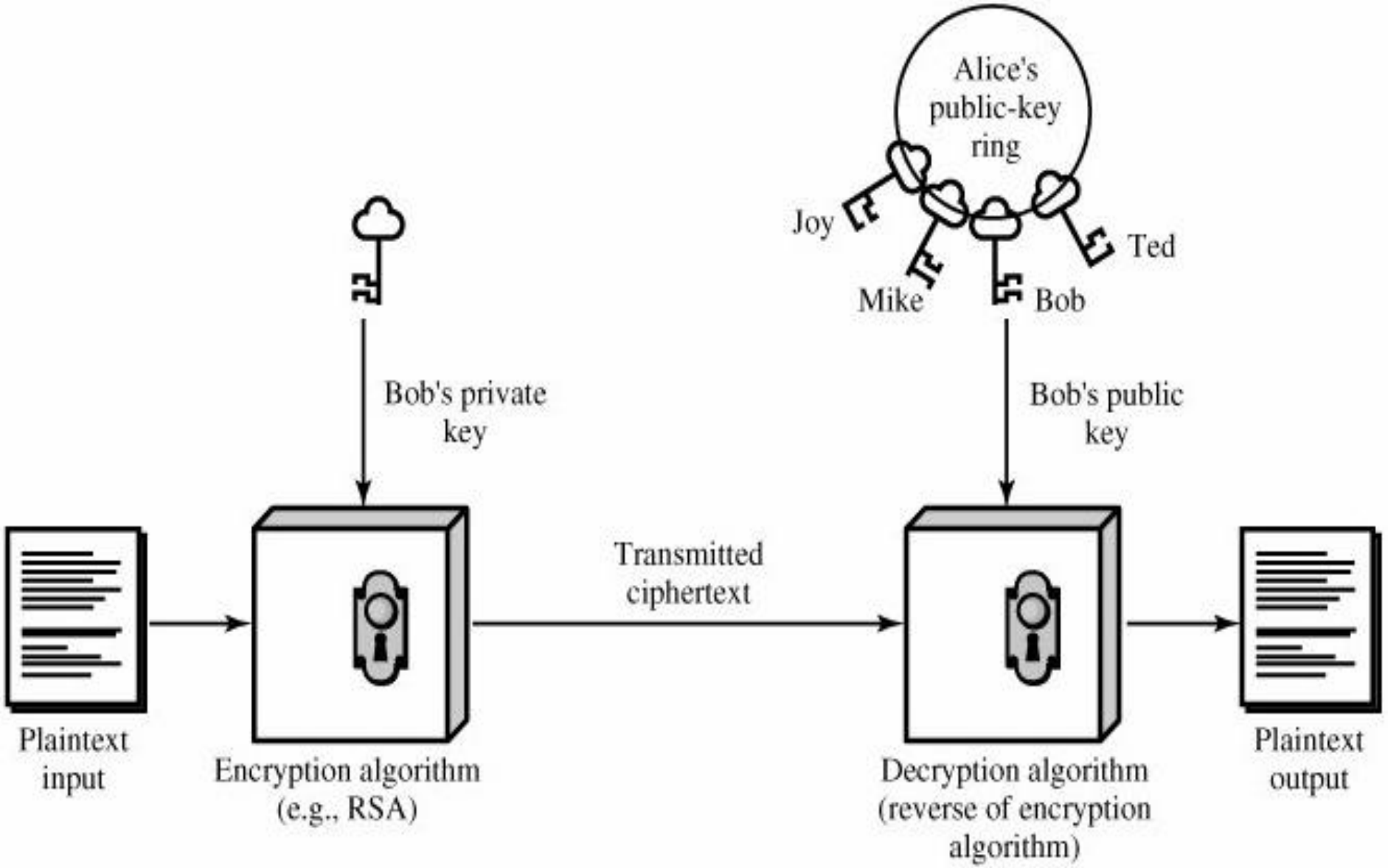
- This algorithm accepts the ciphertext and the matching key and produces the original plaintext.

Characteristic of Algorithms

- It is computationally infeasible to determine the decryption key given only knowledge of the cryptographic algorithm and the encryption key.
- Either of the two related keys can be used for encryption, with the other used for decryption.



(a) Encryption

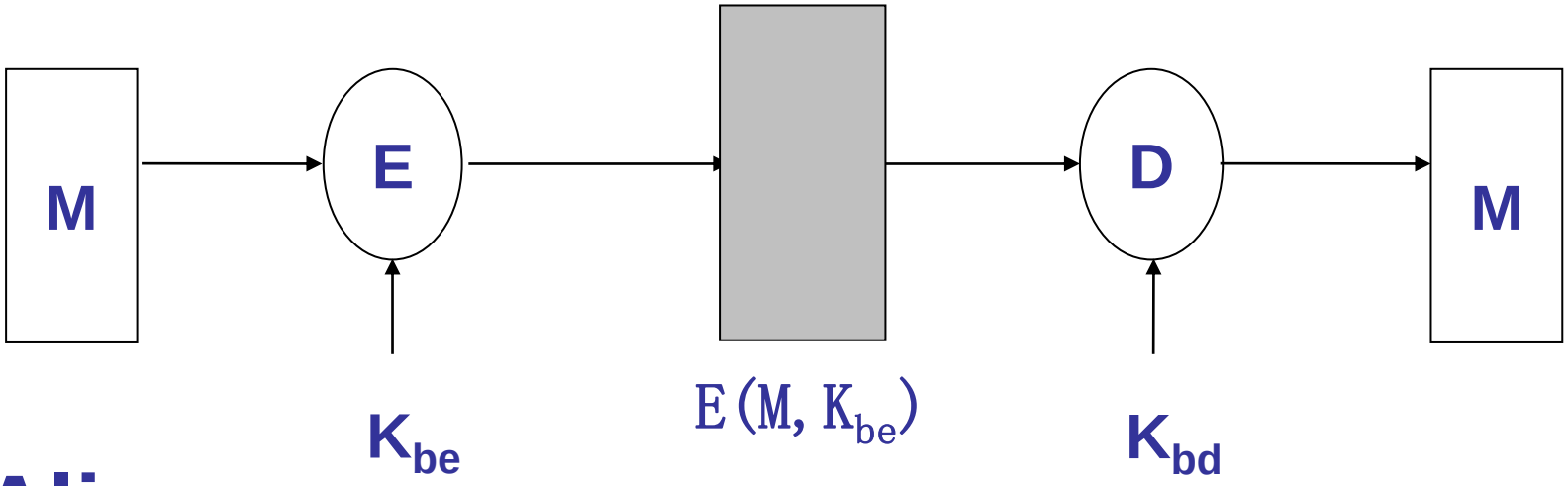


(b) Authentication

公钥密码体制的特点

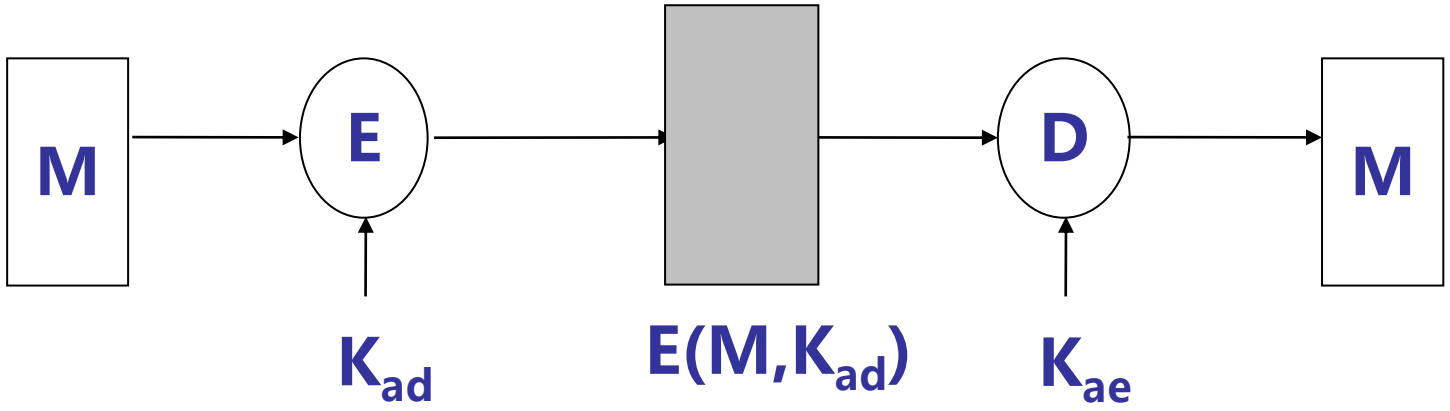
- 加密和解密能力分开
- 多个用户加密的消息只能由一个用户解读，可用于公共网络中实现保密通信
- 用私钥加密的消息可以用对应的公钥解密，所以由一个用户加密消息而使多个用户可以解读，可用于认证系统中对消息进行数字签字
- 无需事先分配密钥
- 密钥持有量大大减少
- 提供了对称密码技术无法或很难提供的服务：如与哈希函数联合运用可生成数字签名，可证明的安全伪随机数发生器的构造，零知识证明等

保证机密性



K_{be}： Bob的公钥
K_{bd} ： Bob的私钥

保证真实性



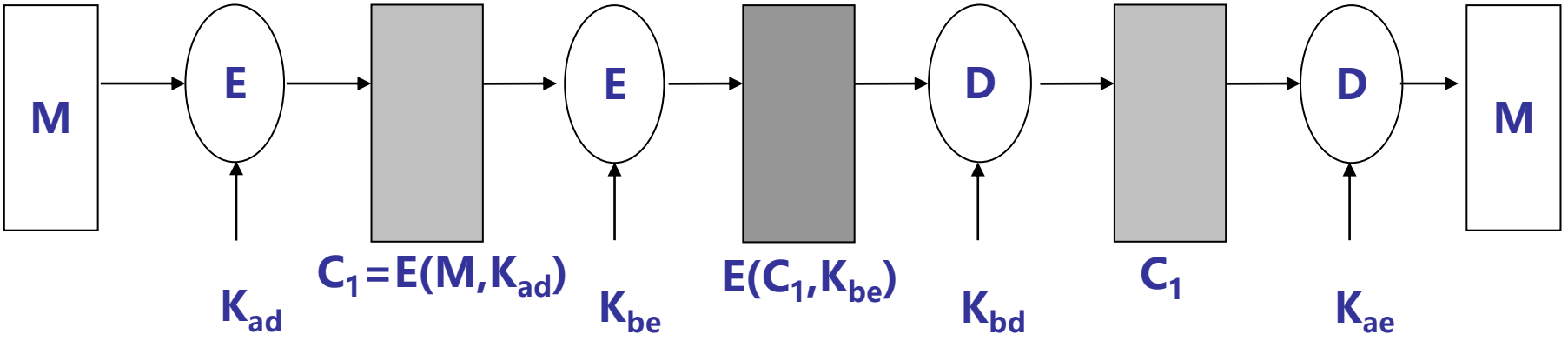
Alice

Bob

K_{ad}： Alice的私钥

K_{ae} ： Alice的公钥

既保证机密性又保证真实性



Alice

Bob

K_{ad}： Alice的私钥
K_{ae} ： Alice的公钥
K_{be}： Bob的公钥
K_{bd} ： Bob的私钥

- 产生密钥对在计算上是容易的
- 发送方A用收方的公钥对消息m加密以产生密文c在计算上是容易的。
- 收方B用自己的私钥对密文c解密在计算上是容易的。
- 敌手由密文c和B的公钥恢复明文在计算上是不可行的。
- 敌手由密文c和B的公钥恢复秘密密钥在计算上是不可行的
- 加解密次序可换，即$E_{PKB}[D_{SKB}(m)]=D_{SKB}[E_{PKB}(m)]$，不是对任何算法都做此要求。

- 和单钥密码体制一样，如果密钥太短，公钥密码体制也易受到穷举攻击。因此密钥必须足够长才能抗击穷搜索攻击。然而又由于**公钥密码体制所使用的可逆函数的计算复杂性与密钥长度常常不是呈线性关系，而是增大得更快。**所以密钥长度太大又会使得加解密运算太慢而不实用。因此公钥密码体制目前主要用于**密钥管理和数字签字**。
- 对公钥密码算法的第2种攻击法是寻找从公钥计算私钥的方法。目前为止，对常用公钥算法还都未能够证明这种攻击是不可行的。

4.4 RSA公钥密码体制---概况

- MIT三位年青数学家R.L.Rivest，A.Shamir和L.Adleman[Rivest等1978，1979]发现了一种用数论构造双钥的方法，称作MIT体制，后来被广泛称之为RSA体制。
- 它既可用于加密、又可用于数字签名。
- RSA算法的安全性基于数论中大整数分解的困难性。
- RSA密码已经成为目前应用最广泛的公钥密码。许多国际化标准组织，如ISO，ITU和SWIFT等都已经接受RSA作为标准。Internet网的E-mail保密系统以及国际VISA和MASTER组织的电子商务协议SET协议中都将RSA作为传送会话密钥和数字签名的标准。
- 迄今为止理论上最为成熟完善的公钥密码体制

- RSA算法使用了乘方运算。
- 要求：
  - 明文M经过加密得到密文C： $C=M^e \bmod n$
  - 密文C经过解密得到明文M：

$$C^d \bmod n=(M^e \bmod n)^d \bmod n= M^{ed} \bmod n=M$$

即：必须存在e，d，n，使$M^{ed} \bmod n=M$成立

- The RSA scheme is a block cipher in which the plaintext and ciphertext are integers between 0 and n-1 for some n.
- A typical size for n is 1024 bits, or 309 decimal digits. That is, n is less than 2^{1024}.

如何确定e,d,n

- 确定n：
  - 独立地选取两大素数p和q(各100～200位十进制数字)
  - 计算 $n=p\times q$，其欧拉函数值$\varphi(n)=(p-1)(q-1)$
- 确定e：
  - 随机选一整数e，$1\le e<\varphi(n)$，$\gcd(\varphi(n), e)=1$
- 确定d：
  - 根据$ed \equiv 1 \bmod \varphi(n)$在模$\varphi(n)$下，计算$d$

密钥

- 以n，e为公钥。秘密钥为d。(p, q不再需要，可以销毁。)

这样确定的e,d,n是否能使$M^{ed} \bmod n = M$成立呢?

- 因为$ed \equiv 1 \bmod \varphi(n)$ 即$ed = k\varphi(n)+1$

  所以：$M^{ed} = M^{k\varphi(n)+1}$

- **如果M和n互素**，即gcd(M,n)=1 那么，

根据欧拉定理(如果gcd(a,n)=1，则 $a^{\Phi(n)} \equiv 1 \bmod n$)：

有：$M^{\varphi(n)} \equiv 1 \bmod n$

所以：$M^{ed} \equiv M^{k\varphi(n)+1} \equiv M[M^{\varphi(n)}]^k \bmod n$

$\equiv M[1]^k \bmod n$

$\equiv M \bmod n$

- 如果M和n不互素，即gcd(M,n)≠1，即M和n有大于1的公约数。

因为n=pq，而p、q都是素数，不可再分解，所以M一定包含了p或q为因子。

又因为M<n，所以M不可能既是p的倍数又是q的倍数。

- 不妨设M是p的倍数，M=cp。

由于M不是q的倍数，所以gcd(M,q)=1，则

$M^{\varphi(q)} \equiv 1 \bmod q$，所以：$[M^{\varphi(q)}]^{\varphi(p)} \equiv 1 \bmod q$

即$M^{\varphi(n)} \equiv 1 \bmod q$，进而有$M^{k\varphi(n)} \equiv 1 \bmod q$

$M^{k\varphi(n)} \equiv 1 \bmod q$

所以：$M^{k\varphi(n)} = 1+bq$ （b为整数）

两边同乘以M： $M^{k\varphi(n)+1} = M+Mbq$

因为 $M=cp$

所以 $M^{k\varphi(n)+1} = M+cpbq = M+cbn$

因为cb为整数，令cb=K，即：

$M^{k\varphi(n)+1} = M+Kn$

因为$ed=k\varphi(n)+1$

所以$M^{ed} = M+Kn$ 即$M^{ed} \equiv M \bmod n$

➢ 加密和解密

无论是加密还是解密都需要计算某个整数的模n整数次幂，即$C=M^e \mod n$、$M=C^d \mod n$。但不需要先求出整数的幂再对n取模，而可利用模运算的性质：

$$(a \bmod n) * (b \bmod n) = (a*b) \bmod n$$

对于$M^e \mod n$，可先求出$M^1 \mod n$，$M^2 \mod n$，$M^4 \mod n$……，再求$M^e \mod n$

产生密钥

- 由于n是公开的，为了避免攻击者用穷举法求出p和q（根据n=pq），应该从足够大的集合中选取p和q，即p和q必须是大素数。
- 目前还没有有效的方法可以产生任意大素数，通常使用的方法是：随机挑选一个期望大小的奇数，然后测试它是否是素数，若不是，则挑选下一个随机数直至检测到素数为止。

素性检验

- **引理：如果p为大于2的素数，则方程$x^2 \equiv 1 \bmod p$的解只有$x \equiv 1 \bmod p$ 和$x \equiv -1 \bmod p$**
- **证明:**

$x^2 \equiv 1 \bmod p \rightarrow x^2 - 1 \equiv 0 \bmod p$

$(x+1)(x-1) \equiv 0 \bmod p$

所以,$p|(x+1)$或$p|(x-1)$

或$p|(x+1)$且$p|(x-1)$→存在k,j，$x+1=kp$，$x-1=jp$

→$2=(k-j)p$， 这是不可能的。

或者这样说

- p为大于2的素数，如果有x使得

$x^2 \equiv 1 \bmod p$成立，那么：

$x \bmod p = 1$

或者$x \bmod p = p-1$

素数的性质1

- Let ***p*** be a prime number greater than 2. We can then write $p-1 = 2^k q$, with $k > 0, q$ odd. Let a be any integer in the range $1 < a < p-1$. Then one of the two following conditions is true:

  $a^q \bmod p = 1$, or equivalently, $a^q \equiv 1 \bmod p$.

  One of the numbers $a^q, a^{2q}, a^{4q}, \ldots, a^{2^{k-1}q}$ is congruent to -1 modulo p.

素数的性质2

Proof

- 根据Fermat's theorem，如果p是一个素数,a不是p的倍数，则：$a^{p-1} \equiv 1 \pmod{p}$
- 又因为$p-1 = 2^k q$，所以：

$$a^{p-1} \bmod p = a^{2^k q} \bmod p = 1$$

- 考察下列数列：

$$a^q \bmod p, a^{2q} \bmod p, a^{4q} \bmod p, \ldots, a^{2^{k-1} q} \bmod p, a^{2^k q} \bmod p$$

要么所有数均为1，要么其中必有一个数为p-1

TEST (p)----is p composite?

- Find integers k, q, with k > 0, q odd, so that (p-1 = $2^k q$);
- Select a random integer a, 1 < a < p-1;
- if a^q mod p = 1 then return("inconclusive");
- for j = 1 to k do

  if $a^{2^{j-1}q}$ mod p=p-1 then

  return("inconclusive");

return("composite");

Repeated Use of the Miller-Rabin Algorithm

- 算法对s个不同的a，重复调用，如果每次都返回inconclusive，则p是素数的概率大于等于$1-2^{-s}$

- Miller-Rabin算法可以确定一个整数是合数，但不能确定其一定是素数。
- 要找到一个2^{200}左右的素数，在找到素数之前大约要进行$\ln(2^{200})/2=70$次尝试
- 在N附近平均每隔lnN个整数就会有一个素数。

RSA算法在计算上的可行性

- 确定d和e
  - 有了p和q，可计算出$\varphi(n)=(p-1)(q-1)$
  - 根据gcd($\varphi(n)$,e)=1来选择e，这一步计算量也不大，因为两个随机数互素的概率约为0.6
  - 有了e，再计算$d=e^{-1} \bmod \varphi(n)$，这里用的是扩展的Euclid算法。

算法描述

① 选两个保密的大素数p和q。

② 计算n=p×q，φ(n)=(p-1)(q-1),其中φ(n)是n的欧拉函数值。

③ 选一整数e，满足1<e<φ(n)，且gcd(φ(n),e)=1。

④ 计算d，满足d·e≡1 mod φ(n),即d是e在模φ(n)下的乘法逆元，因e与φ(n)互素，由模运算可知，它的乘法逆元一定存在。

⑤ 以{e,n}为公开钥,{d,n}为秘密钥。

算法描述

选p=7，q=17。

求n=p×q=119，φ(n)=(p-1)(q-1)=96。

取e=5，满足1<e<φ(n)，且gcd(φ(n),e)=1。确定满足d·e=1 mod 96且小于96的d，因为77×5=385=4×96+1，所以d为77。

因此公开钥为{5，119}，秘密钥为{77，119}。设明文m=19，则由加密过程得密文为

$C=19^5 \mod 119 \equiv 2476099 \mod 119=66$

解密为$66^{77} \mod 119=19$

- 在RSA体制中，已截获发给某用户的密文C=10，该用户的公钥e=5，n=35，那么明文M等于多少？

- 在RSA体制中，已截获发给某用户的密文C=10，该用户的公钥e=5，n=35，那么明文M等于多少？

$$n = 35 = p \times q \Rightarrow n = 5 \times 7, \therefore \varphi(n) = 24, \text{且}(e, \varphi(n)) = 1 \Rightarrow ed \equiv 1 \bmod \varphi(n) \Rightarrow d = 5.$$

$$P = C^d \bmod n \Rightarrow P = 10^5 \bmod 35 = 5 \bmod 35$$

- RSA的安全性是基于分解大整数的困难性假定
- 如果分解$n=p\times q$，则立即获得$\varphi(n)=(p-1)(q-1)$，从而能够确定e的模$\varphi(n)$乘法逆d
- RSA-129历时8个月(曾经预言需要$4*10^{16}$年)被于1994年4月被成功分解，RSA - 130于1996年4月被成功分解
- 密钥长度应该介于1024bit到2048bit之间
- 由n直接求$\varphi(n)$等价于分解n

RSA-129的故事

- 鹍鸟（ossifrage），又名髭兀鹰（lammergeier），是阿尔卑斯山上一种稀有的肉食秃鹰。它的翅膀展开将近十米宽。鸟名的字面含义是“碎骨”。顾名思义，其习性令人毛骨悚然。
- Mirtin Gardner在1977年“Scientific American”的专栏文章中介绍了RSA码。为了显示这一技术的威力，RSA公司的研究人员用一个129位的数N和一个4位数e 对这个关于秃鹰的消息作了编码。Gardner刊登了那个密文，同时给出了N和e。RSA公司还悬赏100美元，奖给第一个破译这密码的人。
- 96869 61375 46220 61477 14092 22543 55882 90575 99911 24574 31987 46951 20930 81629 82251 45708 35693 14766 22883 98962 80133 91990 55182 99451 57815 154

- 一批松散组成的因子分解迷，大约有六百多人，分布在二十几个国家。他们经过八个月的努力最后于1994年4月为RSA-129找到了64位数和65位数两个素数因子。
- 11438 16257 57888 86766 92357 79976
  14661 20102 18296 72124 23625 62561
  84293 57069 35245 73389 78305 97123
  56395 87050 58989 07514 75992 90026
  87954 3541 = 34905 29510 84765 09491
  47849 61990 38981 33417 76463 84933
  87843 99082 0577 * 32769 13299 32667
  09549 96198 81908 34461 41317 76429
  67992 94253 97982 88533
- “The magic words are squeamish ossifrage”

来自两个方面的威胁

- 人类计算能力的不断提高
- 分解算法的进一步改进。分解算法过去都采用二次筛法，如对RSA-129的分解。而对RSA-130的分解则采用了一个新算法，称为推广的数域筛法，该算法在分解RSA-130时所做的计算仅比分解RSA-129多10%。将来也可能还有更好的分解算法，因此在使用RSA算法时对其密钥的选取要特别注意其大小。估计在未来一段比较长的时期，密钥长度介于1024比特至2048比特之间的RSA是安全的。

几个建议

- 为了防止可以很容易地分解n，RSA算法的发明者建议p和q还应满足下列限制条件：
  - P和q的长度应仅相差几位。对于1024位的密钥而言，p和q都应在10^{75}到10^{100}之间。
  - (p-1)和(q-1)都应有一个大的素因子。
  - Gcd(p-1,q-1)应该较小。

4.5 其它公钥密码算法

- ElGamal密码
  - ElGamal密码是由ElGamal于1985年提出。该密码系统可应用于加/解密、数字签名等，其安全性是建立于离散对数(discrete logarithm)问题之上的，即给定g，p与$y=g^x \bmod p$，求x在计算上不可行。

1．密钥产生

（1）任选一个大素数 p，使得 p−1 有大素因子。
（2）任选一个 mod p 的本原根 g。
（3）公布 p 与 g。

使用者任选一私钥 $x \in Z_p$，并计算公钥 $y = g^x \bmod p$。

2．加密程序(m 为明文)

（1）任选一个随机数 $r \in Z_p$ 满足 $\gcd(r, p-1)=1$，并计算：

$$c_1 = g^r \bmod p$$

$$c_2 = m \times y^r \bmod p$$

（2）密文为 $\{c_1, c_2\}$。

3．解密程序

（1）计算 $w = (c_1{}^x)^{-1} \bmod p$。

（2）计算明文 $m = c_2 \times w \bmod p$。

Thank you!

网络攻击是实现“不战而屈人之兵”最有效的武器之一

没有网络信息安全就没有国家安全