* 1. Kerchhoff原则

密码系统的安全性不依赖于加密体制或算法的保密，而依赖于密钥的安全性

* 1. 加密算法的安全性

假设攻击者已知加密算法的实现细节，在未知密钥的情况下，攻击密码系统的强度由弱到强的四种基本攻击为：

唯密文攻击：仅知道给定密文的情况下进行攻击

已知明文攻击：得到了给定明文密文对的情况下进行攻击

选择明文攻击：攻击者可以选择明文消息得到相应的加密得到的密文

选择密文攻击：攻击者可以选择密文消息得到相应的解密得到的明文

安全目标（由低到高）：

攻击者不能获得解密密钥

攻击者不能获得明文

攻击者不能获得明文的任何部分信息

攻击者不能获得明文的任何函数

0.3唯密文攻击挑战

①受挑战者运行密钥生成算法Gen，确定密钥k

②受挑战者将加密任意的明文后发送给攻击者（可多次运行）

③攻击者发送明文空间中的两条明文m0和m1给受挑战者

④受挑战者随机加密其中一条明文，并将相应密文发送给攻击者

⑤受挑战者将加密任意的明文后发送给攻击者（可多次运行）

⑥攻击者根据密文猜测对应的明文是m0还是m1

0.4选择明文攻击挑战

①受挑战者运行密钥生成算法Gen，确定密钥k

②攻击者选择明文空间中的明文

③受挑战者将明文加密后发送给攻击者

2、3步可反复运行安全参数的多项式次

④攻击者发送明文空间中的两条明文m0和m1给受挑战者

⑤受挑战者随机加密其中一条明文，并将相应密文发送给攻击者

⑥攻击者选择明文空间中的明文

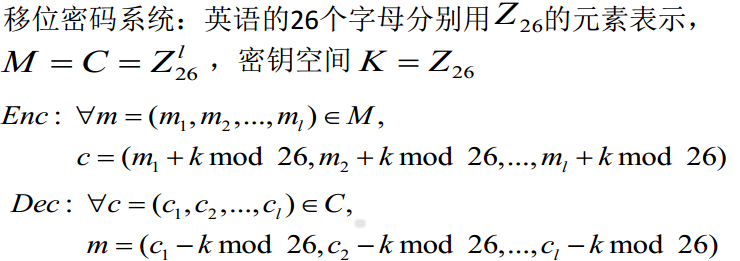
⑦受挑战者将明文加密后发送给攻击者

6、7步可反复运行安全参数的多项式次

⑧攻击者根据密文猜测对应的明文是m0还是m1

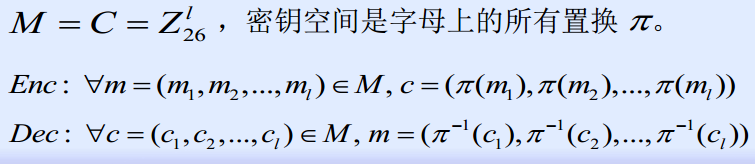
1. 古典密码

1.1移位密码



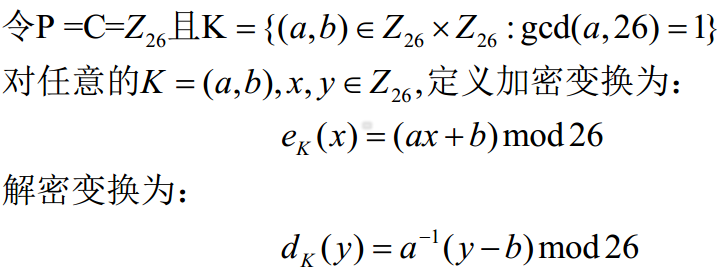
可用穷举攻击破解

1.2单字母替换



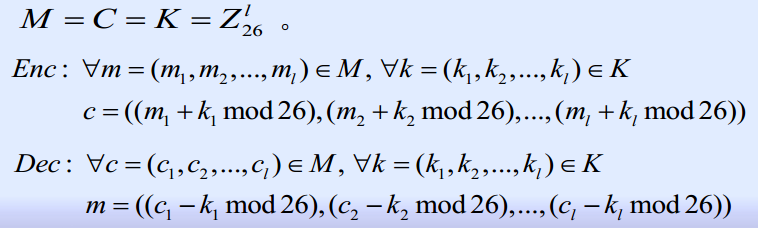
可利用英文字母常用频率不同进行攻击，其中E的概率最高约为0.12，T、A、O、I、N、S、H、R的概率为0.06-0.09，D、L概率约为0.04，C, U, M, W, F, G, Y, P, B的概率为0.015-0.023，V, K, J, X, Q, Z的概率小于0.01。还有常见的二字母、三字母组合。

1.3仿射密码



攻击方式同单字母替换

1.4维吉尼亚密码

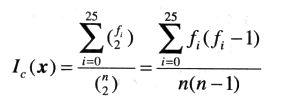


可将密文分段加密

在一个具有密钥长度为m的维吉尼亚密码中，一个字母可以被映射为m个字母中的某一个。这样的密码体制被称为多表代换。

确定密钥长度：

Kasiski测试法，两个相同的明文段加密成相同的密文段，则这两个明文段之间的间距很大概率是密钥长度的整数倍。需搜索长度至少为3的相同密文段，记下离起始点密文段距离，则可猜测密钥长度m为距离的最大公因子的因子。

重合指数：

重合指数法，对于一个完全随机串，其重合指数Ic=0.038，而对于正常文本串Ic≈0.065.对于一串维吉尼亚密文，将串分割成m个长度相等的子串（每隔m个），若m为密钥长度，则每个子串Ic都会约等于0.65。

确定了密钥长度后，转换成若干移位密码

1.5现代密码学特点

方案公开，有严格明确的安全定义

算法安全性依靠尽可能少的数学假设

附有严格的安全性证明

2. 完善保密加密机制

2.1加密算法定义

密钥生成子算法（Gen）：

输入：安全参数n；输出：满足特定分布的密钥k；

加密子算法（Enc）：

输入：密钥k和明文m；输出：密文c，c=Enc(k,m)

解密子算法（Dec）：

输入：密钥k和密文c；输出：明文m，m=Dec(k,c)

2.2无条件安全（完善保密）：即使攻击者具有无限的计算资源，也无法攻破密码体制。

当前所学的算法里只有一次一密是无条件安全的。

定义：一个加密算法（Gen,Enc,Dec）在明文空间M上是无条件安全的，如果对于M的每种概率分布，其中每个消息m和每个可能出现的密文c，均满足：

Pr[M=m|C=c]=Pr[M=m]

显然，移位密码和单字母替换均非无条件安全。

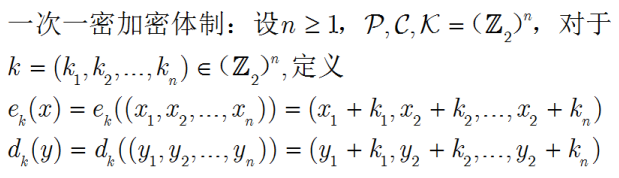
维吉尼亚密码在确定密钥长度后才可找到无条件安全的反例。

定理：一个加密算法在明文空间M上是无条件安全的，当且仅当对于M的每种概率分布，其中任意两个消息m0和m1，和每个可能出现的密文c，如下条件均满足：

Pr[C=c|M=m0]=Pr[C=c|M=m1]

如果加密方案在唯密文攻击下是完善保密的，那么攻击者猜对的概率是1/2

2.4一次一密密码体制



密钥长度和明文一样长

密钥只能使用一次

密钥管理异常复杂

从AI角度来看，是不可学习的。

2.5计算安全：攻击者具有有限的计算资源，很难攻破密码体制，我们称这种密码体制是计算安全的。

将敌手视作一个算法，具有多项式时间复杂度。

安全参数n

多项式q(n)

可忽略函数negl(n),常为分数形式，极限趋于零

如果加密方案在唯密文攻击下是计算安全的，那么攻击者在唯密文攻击挑战中获胜（猜对）的概率是1/2+negl(n)

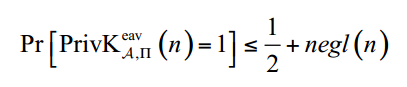
2.6加密算法的安全定义：

安全参数n

唯密文攻击eav

密码算法π

攻击实验Privk

若加密算法在唯密文攻击下是计算安全的，那么

该不等式等价为

注意：表示攻击方获胜

表示在被挑战方选择m0时攻击方选择m1

3对称加密与伪随机性

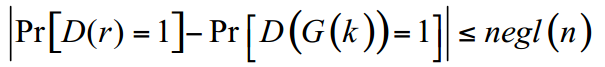
3.1伪随机数生成器

n,安全参数

l(n),扩展因子，n的多项式,l(n)>n

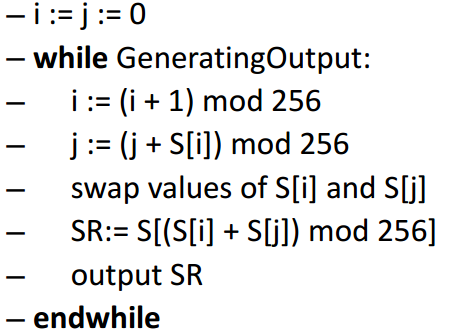
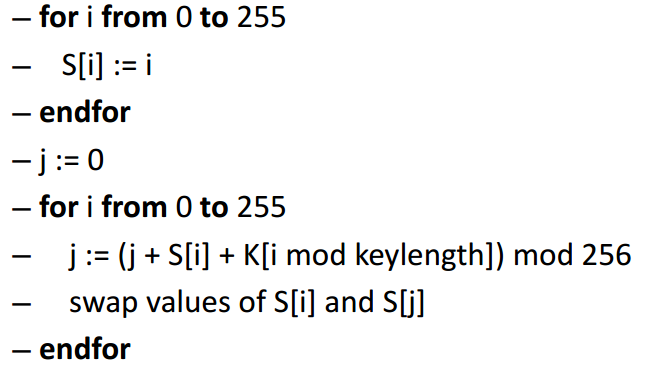
k:密钥，长度为n

G(k)，多项式时间算法k→l(n)

伪随机性

其中D为判断是否为真随机数的函数，r为真随机数

伪代码（左为初始化）：



3.2 流密码(序列加密)

使用伪随机数发生器将密钥扩展到与密文等长，常用异或操作加密。

其安全性主要在于密钥扩展后的随机性。

序列加密算法：

明文m，随机数r，r与密钥k等长

Gen：n→k，k为一个[0,2^n]均匀分布中随机取的整数

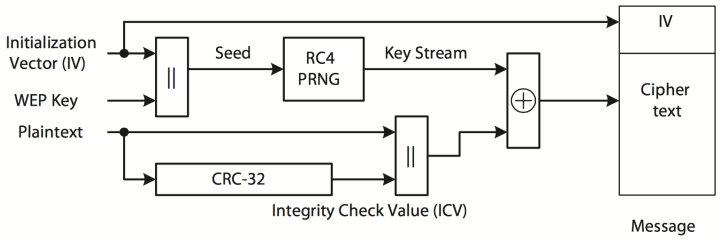
Enc：(k,m)→c; c=(c1,c2)=(r,G(k⊕r)⊕m)

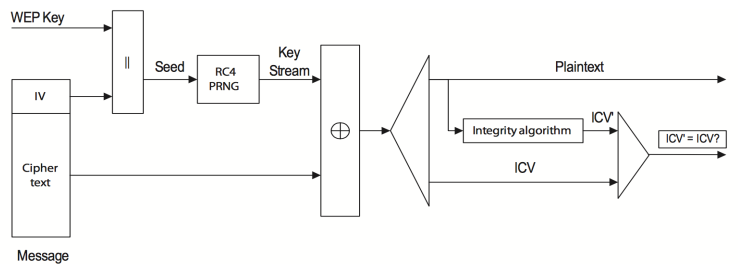
Dec: (k,(c1,c2))→m；m= G(k⊕c1)⊕c2

3.3 RC4与WEP

RC4序列加密算法：是确定性算法，其密钥长度为1-256字节，通常取4-16字节（32-128位）

WEP数据加密方案：40-bit key + 24-bit IV（初始化向量，即随机数）





Wep数据帧中第一个字节消息相同，攻击者可以得到第一个字节的G(k)值

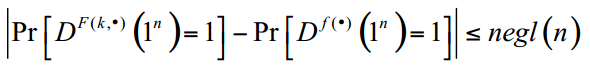
IV只有24bits，2^12个消息就可能出现碰撞

3.4伪随机函数

函数：y=F(k,x)

K确定了x和y的一种映射关系

N表示安全参数，k为密钥，一个函数F(k,x)为伪随机函数，当且仅当对于概率多项式时间算法D，下式成立：



3.5分组密码

将明文分成等长的分组（例如64、128位），并对每个分组采用相同的加密算法进行加密。

其实现算法一般是交替使用混乱和扩散技术。

分组加密算法：

明文m，随机数r，r与密钥k等长

Gen：n→k，k为一个[0,2^n]均匀分布中随机取的整数

Enc：(k,m)→c; c=(c1,c2)=(r,F(k,r)⊕m)

Dec: (k,(c1,c2))→m；m= F(k,c1)⊕c2

3.6代换-置换网络SPN

设l和m都是正整数，明文和密文都是长为lm的二元向量。一个SPN包括两个变换：

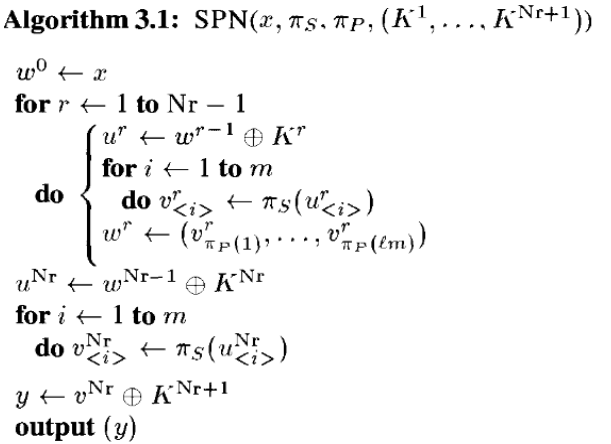
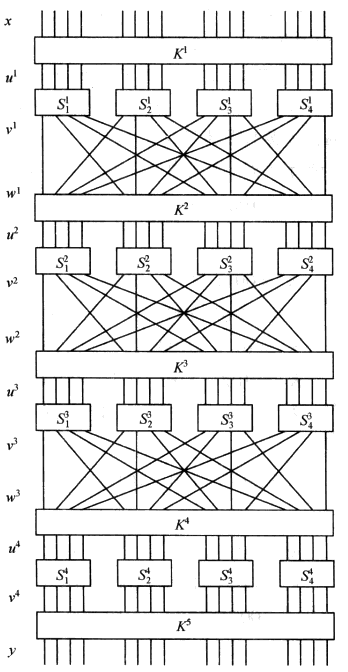
代换盒

置换

给定长为lm比特的二元串x=(x1,…,xlm),将其看做m个长为l比特的子串串联，即

SPN由Nr轮组成，在每一轮先用异或操作混入该轮的轮密钥，再进行m次代换，再进行一次置换，算法伪代码和结构如下：

轮密钥是初始密钥K经过密钥编排算法生成，SPN第一个和最后一个操作都是异或轮密钥，这叫做白化。

3.7菲斯特尔密码结构

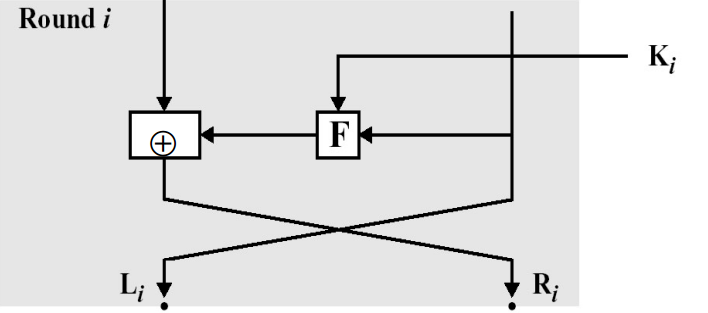
明文分组为L0和R0，通过n次循环处理后，再组合生成密文分组。

每次循环都以上一循环产生的Li-1和Ri-1和K产生的子密钥Ki作为输入

所有循环结构相同,加密解密可以采用相同方法。

加密：Li=Ri-1；Ri=Li-1⊕F(Ri-1,Ki)

解密: Ri-1=Li;Li-1=Ri⊕F(Li,Ki)

F不要求可逆

3.8雪崩效应

严格雪崩准则SAC：当任何输入位被反转时，输出中的每一位均有50%概率发生变化

3.9系数在Z2上的多项式运算

多项式的系数从高到低依次对应到字节的相应比特，例如下



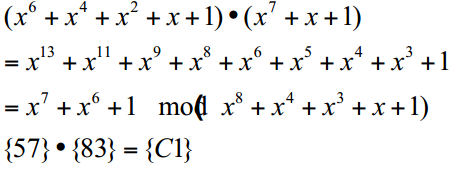
多项式相加：





多项式相乘：

需要对不可约多项式取余，

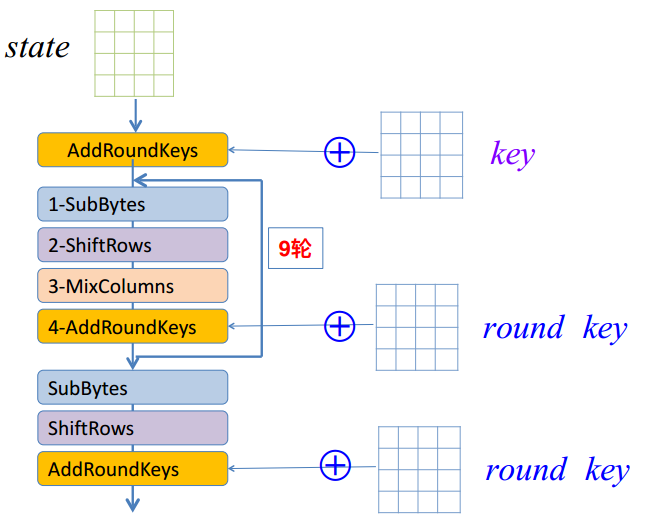


3.10高级加密标准AES

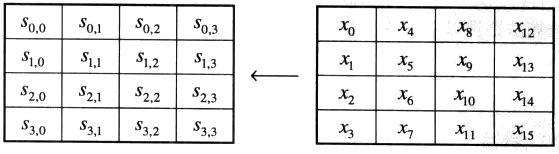
128比特分组，128、192和256位密钥。多轮操作，若密钥长度为128比特，则轮数是10，如果密钥长度是192比特，则轮数是12，如果密钥长度是256比特，则轮数是14.

AES每一轮用了密钥混合、代换、置换、MixColumn，操作单元以字节为单位

算法过程：

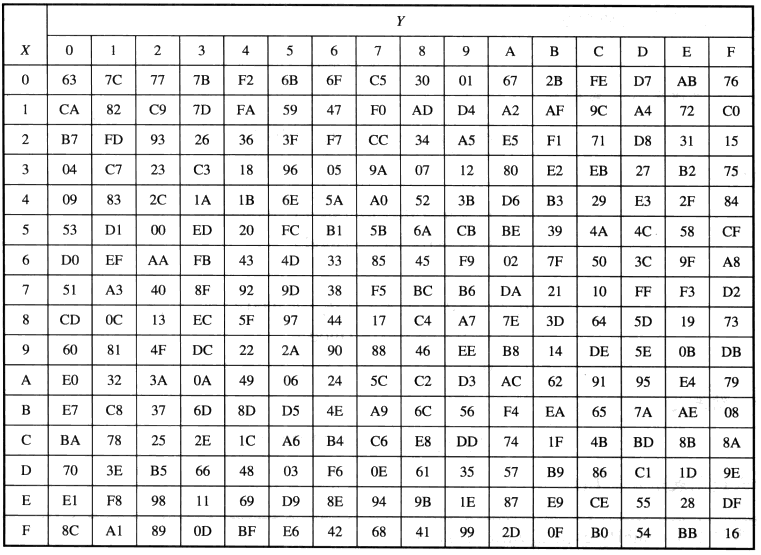


给定明文x，将State初始化为x，对密钥k做相同操作，State为如下4\*4字节矩阵

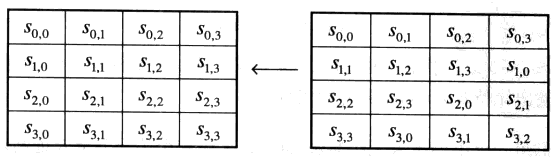


密钥和state做异或和

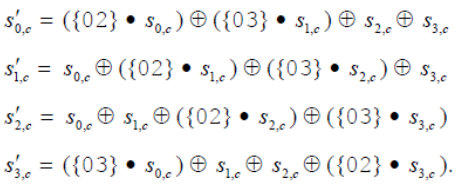
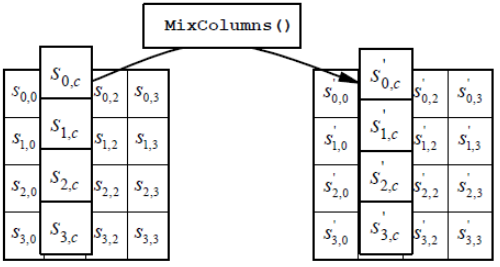
对前Nr-1轮中的每一轮，用S盒对State进行一次代换操作SubBytes，S盒如下



对代换后的State做一次置换ShiftRows，操作如下所示，大致为第i行循环左移i位



对置换后的State做一次操作MixColumns，MixColumns对State中每一列进行系列操作，



注意：·{02}表示二进制左移1位；·{03}表示二进制左移后异或二进制左移前二进制

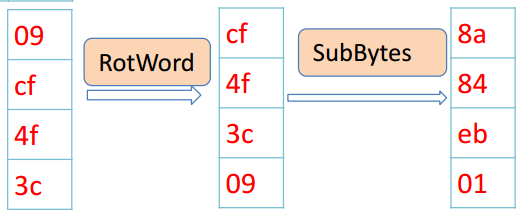
进行AddRoundKey

重复SubBytes、ShiftRows、MixColumns、AddRoundKey，最后得到State为密文，注意最后一轮没有MixColumns

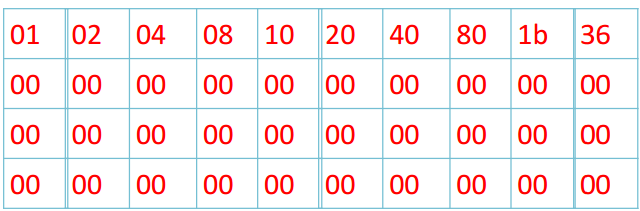
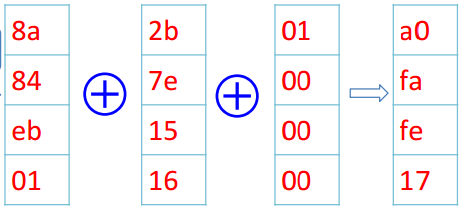
子密钥生成算法，例如下：



取最后一列w3，循环上移一位，用S盒做SubBytes处理，获得临时列wt



第一列w0和wt和子密钥计算字典对应行做异或和（第i轮子密钥对应第字典第i列），获得子密钥第一列w0’，如下为计算方法和字典

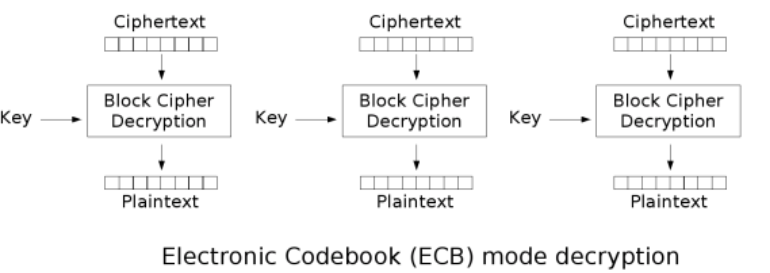
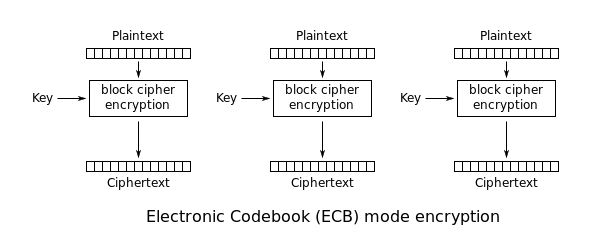


第二列w1和w0’做异或得到w1’, 第三列w2和w1’做异或得到w2’，第四列w3和w2’做异或得到w3’，即获得了新的轮密钥。

3.11AES工作模式

电子密码本ECB：

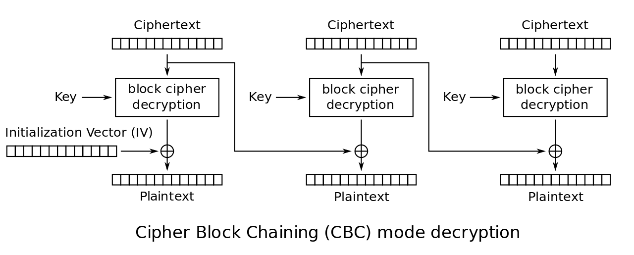
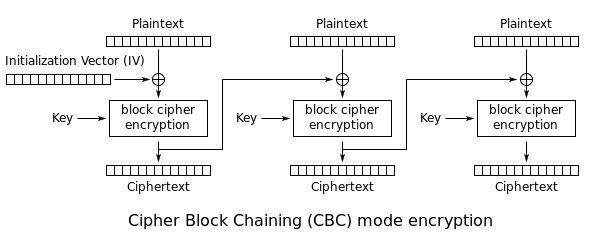
将整个密文切分成若干相同长度的小段，对每段进行加密。



缺点是缺少混淆，会将相同数据加密为相同的密文，无法很好的隐藏数据模式，不推荐在加密协议中进行使用，但操作简单，且分组之间相互独立，所以加密解密可并行。

密文分组链接CBC：

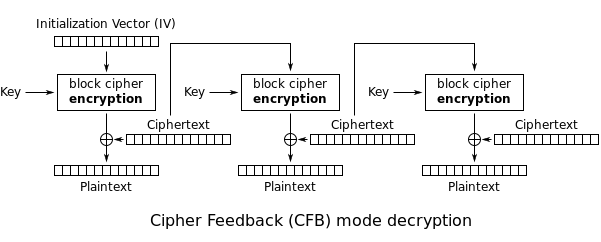
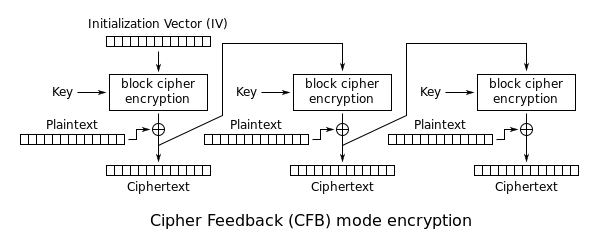
先将明文切分成若干小段，每一小段 初始块或上一段密文段进行异或运算后再与密钥进行加密。



这种模式在加密时无法实现并行计算，但解密的时候可以。优点在于可以掩盖明文结构。

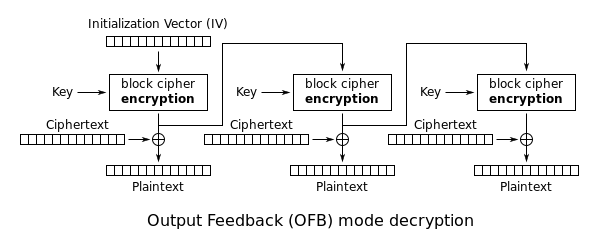
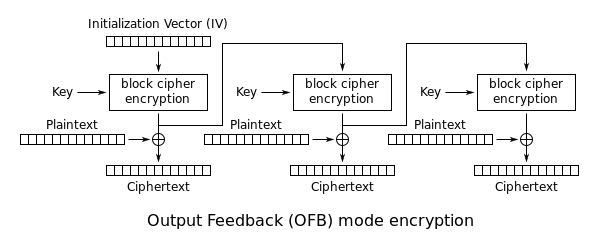
密文反馈CFB：

CFB与CBC类似将分组密码成为自同步流密码。



输出反馈OFB

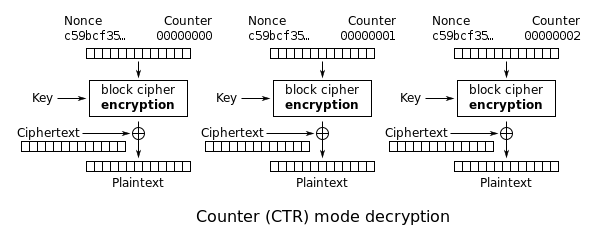
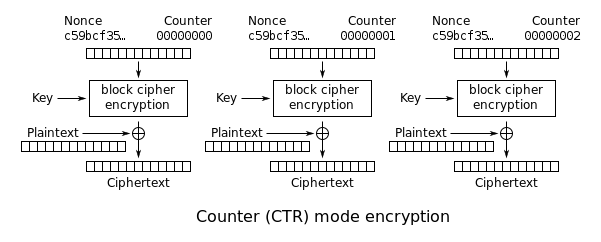
与CFB相比，将密码算法的输出作为每次blockciphper的输入



加密和解密均不可并行，但是好处在于可以即使加密传输小于分组的数据。且其流密码的特性允许一些错误纠正码在加密前也可以正常运用。

计数器CTR

完全的流模式，将瞬时值与计数器连接，然后对此进行加密产生密钥流的一个密钥块，再进行异或操作。



可以实现并行计算，但要保证IV初始化向量Nonce唯一性。

3.12线性密码分析

线性密码分析是已知明文攻击

攻击者具有大量的明-密文对

3.13差分密码分析

差分密码分析是选择明文攻击

差分密码分析与线性密码分析的主要差别在于包含了将两个输入的异或与其相对应的两个输出的异或相比较

4.消息认证码（MAC）与散列函数（HASH）

4.1消息认证码MAC

加密算法不能抵抗消息篡改或伪造。

消息认证码是保证消息完整性的基本算法，利用密钥计算消息的认证信息。

消息认证码算法包含三个子算法：

密钥生成子算法（Gen）：

算法输入：安全参数n；输出：满足特定分布的密钥k；

消息认证码子算法（Mac）：

输入：密钥k和消息m；输出：Mac标签t

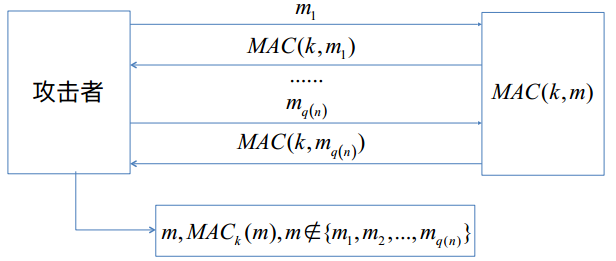
验证子算法（Vrfy）：

输入：密钥k，消息m，标签t；输出b=Vrfy(k,m,t)验证通过为1，验证失败为0；

4.2抵抗选择消息攻击的消息认证码

攻击者通过查询获得一些消息的消息认证码，不能构造出没有查询过的消息的消息认证码。

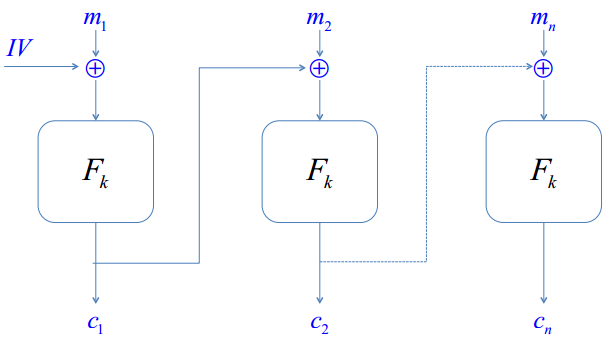
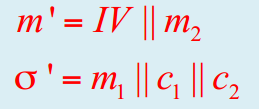
Mac-forge实验流程

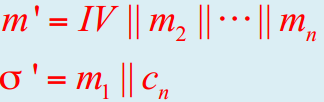


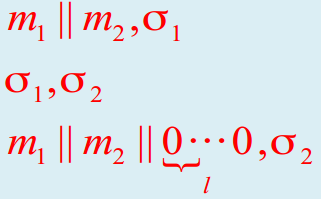
当，消息认证码算法可以抵抗选择明文攻击。

4.3CBC-MAC

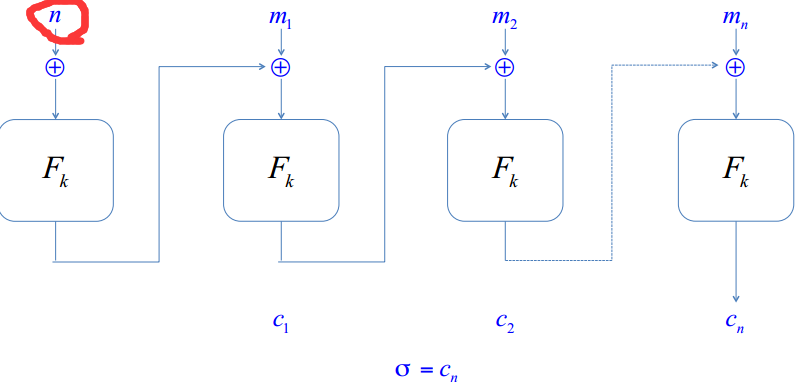
基于加密方式的消息认证码算法

  
这种格式不安全，其破解格式为

格式不安全，其破解格式为

格式不安全，其破解格式为，为Fk(c2)

安全消息验证码结构为：

n不可放在结尾

4.4散列Hash

消息M是任意长度的数据，hash函数产生定长的输出。

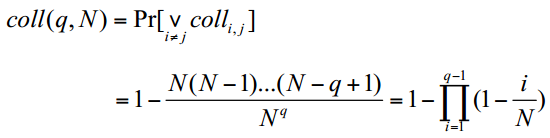
要求给定消息M，计算h=hash(M)容易，但给定h，则很难找到M使得h=H(M),即要求运算过程不可逆，这种性质称为函数的单向性。

抗弱碰撞性：给定消息M和hash值h(M)，要找到另一个M’，使得h(M)=h(M’)在计算上是不可行的。保证无法找到替代的消息M’，这一性质可以用于防伪造。

抗强碰撞性：对于任意两个不同消息M、M’，他们的h值不可能相同。安全性要求更高，保证了对生日攻击的防御能力。

4.5生日攻击

q个元素在[1,N]内随机取值，出现碰撞的概率是：



对于哈希函数H(x)如果具有N位输出，攻击者计算2^(N/2)个哈希值，当n足够大时，出现碰撞的概率为1-e^(-1/2)=0.3934。计算128位需要巨量时间发生碰撞。

4.6 迭代hash函数

将压缩函数延拓为具有无限定义域的Hash函数h。

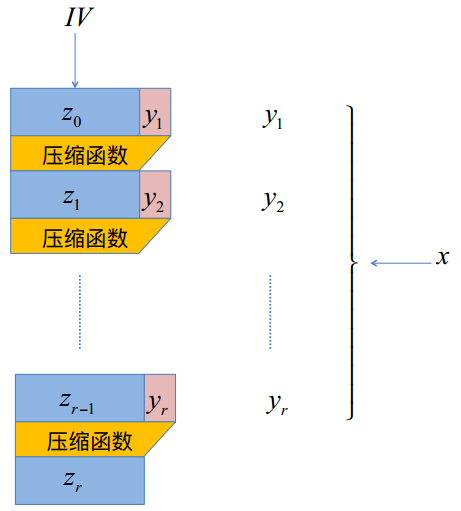
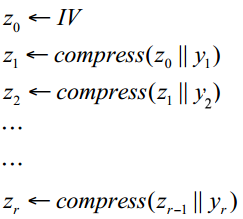
压缩函数：定长输入，定长输出

预处理：

给定一个比特串x，其中|x|≥m+l+1,用公开算法构造比特串y，使得|y|为l的整数倍，记为y=y1||y2||…||yr,|y|=rl，通常对x使用填充函数构造y。

处理：

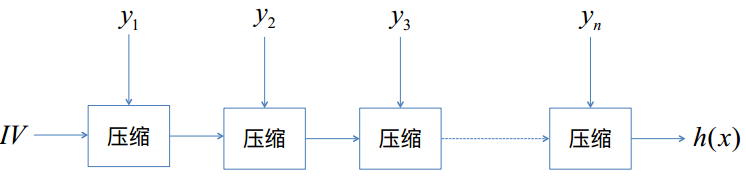
IV为长度为rl的初始化向量比特串，计算：



输出变换：m=rl

4.7 Merkle-Damgard结构

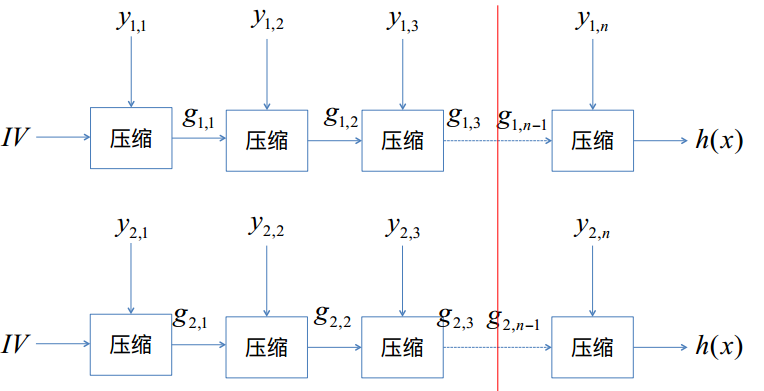
当压缩函数安全时，h是抗碰撞的



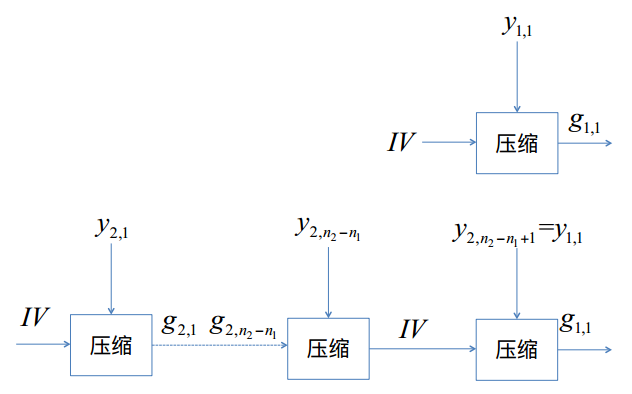
抗碰撞性例子

y1与y2等长但值不等，若两者哈希值相等，则压缩函数不安全。

若y1,n与y2,n不等，则压缩函数不安全，可往前推。



Y1与y2不等长



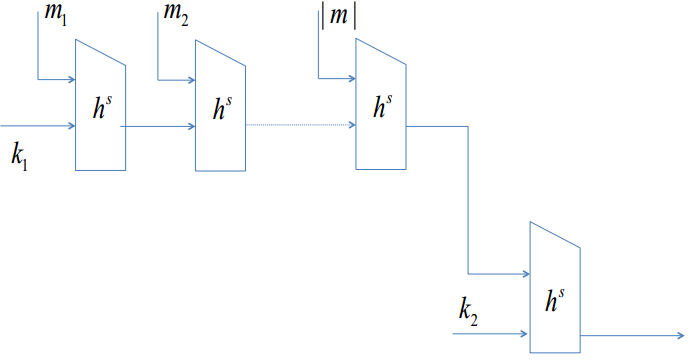
4.8 hash算法的安全性

对于长度为n的理想hash算法，找到原像需要穷举的消息数为2^n，抗弱碰撞性为2^n，抗强碰撞性为2^(n/2)，实际上任何具体的hash算法实现都不是理想的hash算法。

4.8 NMAC嵌套式MAC算法

无需修改现有的散列函数，对更新更安全的散列函数，可以轻易地进行替换。保持散列函数的原有性能不会导致算法性能降低。使用和处理密钥的方式简单。

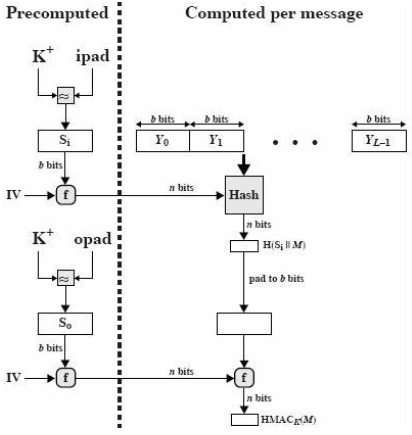
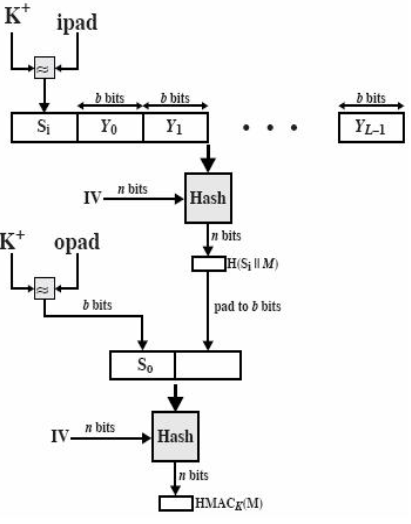
m1、m2……为明文段，密钥k拆分为k1、k2，k1作为初始化向量加入hash，|m|为m的段数



4.8 HMAC

HMAC(k,x)=H((k⊕opad)||H(k⊕ipad||x))

Ipad与opad为确定值



4.9 Mac和Hash的关系

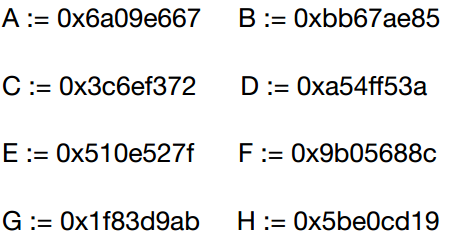
基于hash算法的mac构造方法是一种主要算法

选择密文攻击安全需要先加密，再对密文使用mac算法

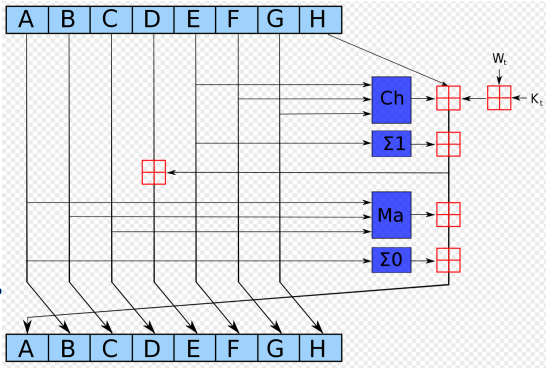
4.10安全Hash算法 SHA

当前版本是SHA2，IV向量可变，在SHA2中IV可以是224或256，对于SHA256，

IV包含八个32位二进制数，是首八个素数的平方根



每轮计算过程为



红色十字框为模2^32加法

Kt为确定的轮密钥，每个Kt都为32位，为首64个素数的立方根，定死。

Wt为

5. RSA密码体制

5.1公钥密码体制

对称密码体制中加密采用的密钥和解密采用的密钥相同，其缺点是加密方和解密方必须在传输密文前使用一个安全信道交换密钥。

公钥密码体制中，已知加密密钥无法计算得到解密秘钥。

可以抽象为一种陷门单向函数，已知明文x和加密密钥k很容易计算出密文y，且已知密文y和公钥k很难计算出明文x。且已知密文y和解密秘钥d，很容易算出明文x。

非对称加密算法比对称加密算法慢1000倍

5.2 RSA加密方案

需要扩展欧几里得算法求逆，其密码体制描述如下

设N=p\*q，p、q均为素数，设P=C=Zn，

定义K={(n,p,q,a,b),ab≡1(mod φ(n)),φ(n)=(p-1)(q-1)}

加密eK(x)=x^b mod n

解密dK(y)=y^a mod n

公钥为n,b ; 私钥为 p,q,a

其参数生成算法为：

①生成大素数p、q

②计算n，φ(n)

③选择随机数b，使得gcd(b, φ(n))=1

④计算b的逆a

RSA密码体制的安全性是基于相信加密函数为单向函数。

对RSA密码的攻击就是密码分析者试图分解n，即通过n获得p、q，如果要使得RSA密码体制安全，那么n=pq必须足够大，使得分解它是计算上不可行的

效率问题：

假设x、y分别为k位和l位二进制正整数，且k大于等于l，则各运算时间复杂度为

x+y：O(k) ; x-y：O(k) ; x\*y:O(kl); gcd(x,y)：O(k^2);

Euclidean算法迭代次数O(k),每次迭代时间O(k^2)

指数运算可以采用平方乘算法，对于x^c mod n，假设c的二进制长度为l，则时间复杂度为O(lk^2)

RSA参数生成算法第二步时间复杂度为O(k^2),第三、四步时间复杂度为O(k^3),k=log(n)

5.3素性监测

素数个数定理：，π（n）为小于N的素数个数

非确定性算法（概率算法）：

蒙特卡洛算法，解不一定正确，但一定可以得到解

拉斯维加斯算法，解一定正确，但不一定总能得到解

偏是的蒙特卡洛算法，当回答“是”时，总是正确的，当回答“否”时，不一定正确。

素性监测：对于一个不小于2的正整数a，a是一个合数吗？

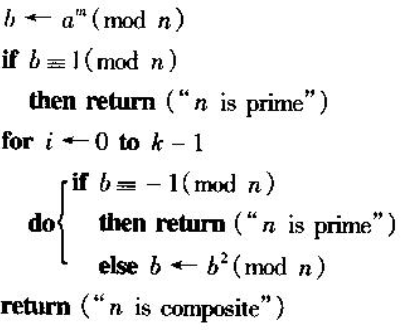
对于偏“是”的蒙特卡洛算法：如果算法输出合数，则a一定是合数；如果算法输出素数，则a可能是合数。

二次剩余：p为奇素数，a为正整数，如果a≠0 mod p，且同余方程y^2=a mod p有一个属于Zp的解y，则称a是模p的二次剩余，例如在Z11中，1,3,4,5,9都是模11的二次剩余。

Euler准则：p为奇素数，a为正整数，a是模p的二次剩余当且仅当

Miller-Rabin（n）算法，对于合数问题是一个偏是的蒙特卡洛算法

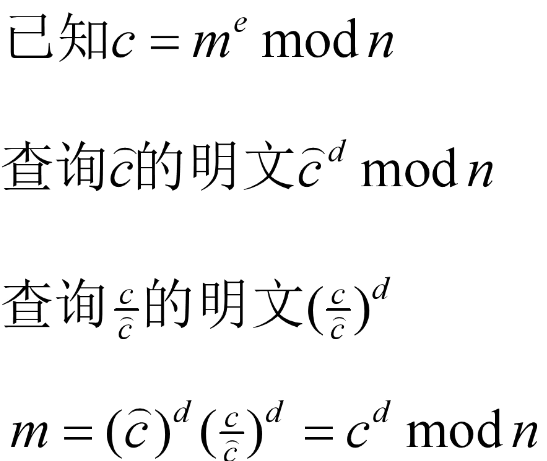
将n-1写成n-1=m\*2^k,其中m为奇数，选取随机正整数a，a≤n-1

时间复杂度为O(log(n)^3)

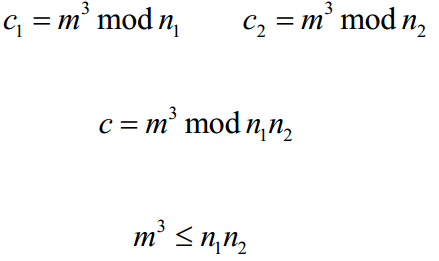
5.4 RSA算法的安全性

大整数因式分解容易则RSA一定容易，反之未知。RSA不是CPA安全的，在以下几种攻击下也不安全

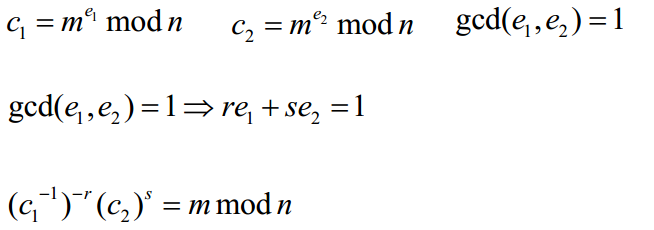
选择密文攻击（CCA）：



低加密指数攻击（e很小的情况）

穷举开根即可

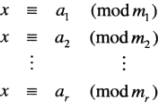
公共模数攻击（共用n）

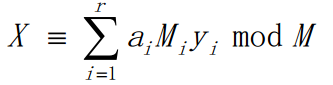


5.5中国剩余定理

是求解某类特定同余方程组的好方法。

假定m1，m2，…mr为两两互素的正整数，对于以下同余方程

该方程组有模的唯一解。

该解为

其中 ，且

5.6 Rabin密码体制

设n=pq，p、q为素数，且p，q≡3(mod4)，设P=C=Zn

定义K={(n,p,q)}，

加密ek(x)=x^2 mod n

解密dk(y)= mod n

N为公钥，p、q为私钥

条件p，q≡3(mod4)是为简化计算，可以省去

其缺点是加密函数ek不是一个单射，其解密的时候可能存在四个解，除非明文中包含足够的冗余信息，否则解密方不能区分四个可能的明文中哪个是正确的

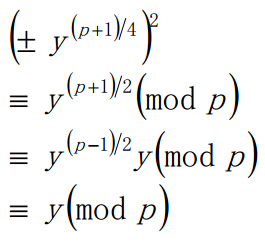
解密过程如下：

解密方得到密文y，需要找出x，使得x^2≡y mod n。

等价于求x^2≡y mod p 且 x^2≡y mod q

当p≡3(mod4)时，根据欧拉准则

有如下公式

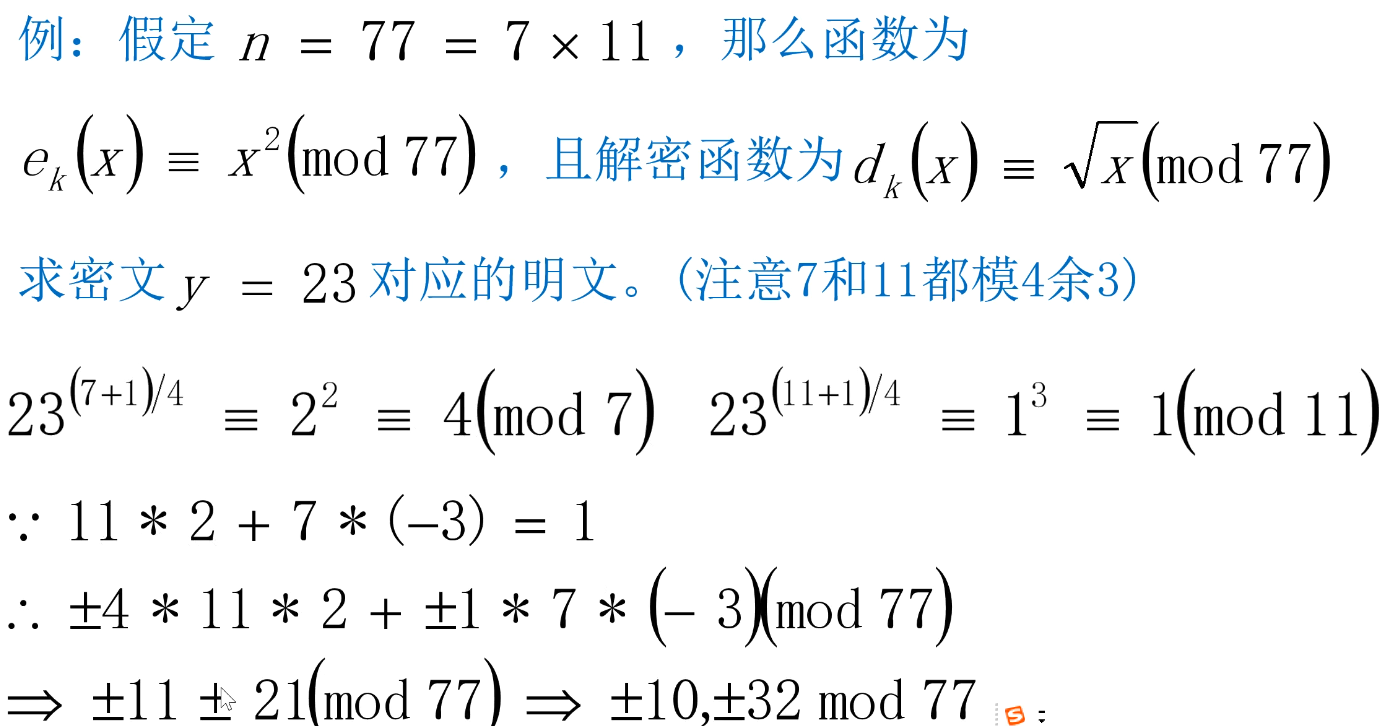


因此，y模p的两个平方根为

同理，y模q的两个平方根为

最后可以利用中国剩余定理得到y模n的四个平方根

例如下



通过图灵规约，可以得到Rabin对CCA不安全，对CPA是安全的

大整数因式分解难则Rabin算法安全

6. 离散对数

6.1 ElGamal密码体制

定义K={(p,α,a,β)：}

P, α,β是公钥，a是私钥

加密ek(x)=(y1,y2), y1= , y2=

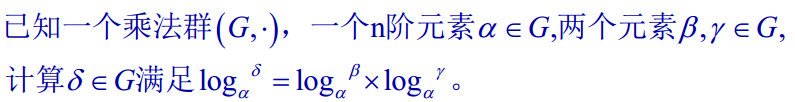
解密dk(y1,y2)=y2() mod p

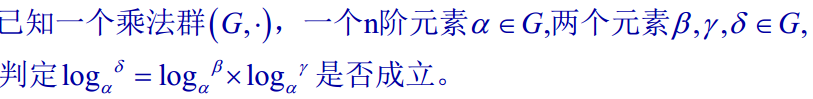
显然如果其他人可以计算Zn上的的a=logαβ，那么ElGamal密码体制不安全

6.2ElGamal的安全性

Diffie-Hellman问题：

离散对数问题，已知一个乘法群G，一个n阶元素α和β，计算

CDH问题

DDH问题

若ElGamal加密算法无法抵挡选择明文攻击，那么DDH问题不是计算困难的。

ElGamal体制的解密等价于求解CDH问题，求出明文则解决了CDH问题，区分出明文则解决了DDH问题。

6.2有限域

当p是素数时，定义Zp[x]是变元x的所有多项式的集合，按照通常多项式的乘法和加法定义构造一个环。对于f(x)和g(x)∈Zp[x]，如果存在q(x)∈Zp[x]，满足g(x)=q(x)f(x),则说f(x)整除g(x)，记作f(x)|g(x)。

对f(x)∈Zp[x]，f的次数为deg(f)定义为f的项中最高次数。

假定f(x),g(x),h(x)∈Zp[x]，且deg(f)≥1。如果f(x)|(g(x)-h(x))则定义g(x)h(x)(mod f(x))

假定g(x)=q(x)f(x)+r(x)，r(x)为余

定义环Zp[x]/(f(x))的元素是Zp[x]中所有次数不超过n-1的多项式。加法和乘法与Zp[x]中相同，并且模f(x)约化。

如果不存在f1(x),f2(x)∈Zp[x]，满足f(x)∈f1(x)f2(x)，则称f(x)∈Zp[x]不可约

Zp[x]/(f(x))是域当且仅当f(x)是不可约的，其中乘法逆元可通过改进的欧几里得算法计算。

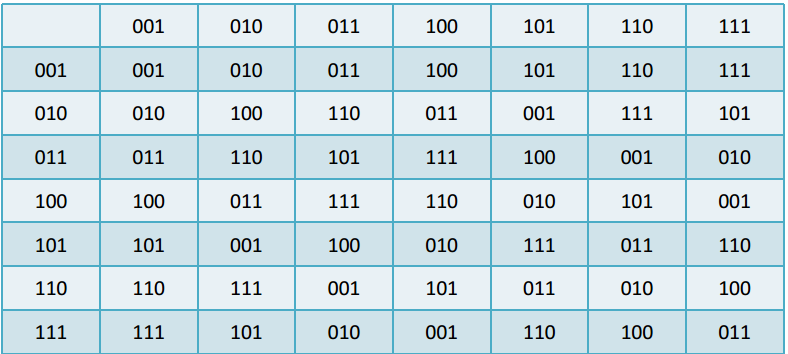
以下为一计算实例

构造一个具有八个元素的域，首先选取f(x)=x^3+x+1构造域Zp[x]/( x^3+x+1)

得到8个域元素:0,1,x,x+1,x^2,x^2+1,x^2+x,x^2+x+1

任意两个域元素模x^3+x+1乘积后，余式属于该域，运算封闭

将a2\*x^2+a1\*x+a0简写为有序三元组a2a1a0，乘法运算表如下



6.3椭圆曲线

定义：设a，b∈R是满足4a^3+27b^2≠0的常实数

方程y^2=x^3+ax+b的所有解(x,y)∈R×R连同一个无穷远点O组成的集合E，称为一个非奇异椭圆曲线。

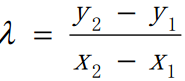
假定E为非奇异椭圆曲线，在E上定义一个二元运算，使其成为一个阿贝尔群，这个二元运算常用加法表示。无穷远点O为单位元。对于P∈E，P+O=O+P=P

假设P，Q∈E，其中P(x1,y1),Q(x2,y2)，定义P+Q，加法在集合E上是封闭的、可交换的，且每个点都有关于加法的逆元

分三种情况

①x1≠x2

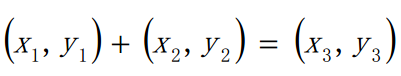
定义L是过P和Q的直线，L交E于P和Q，且与E交于第三点R’，对x轴反射R’得到点R，定义P+Q=R

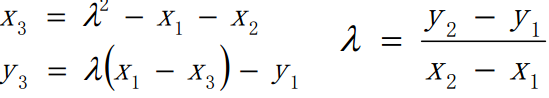
直线L方程为y= λx + v，其斜率，且

将L方程与E方程联立，得到

设R=(x3,y3),R’(x3,-y3)

由于R’在直线上，所以

P+Q计算公式为

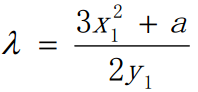
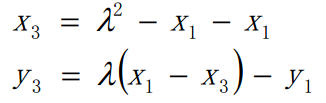
其中

②x1=x2，y1=-y2

定义P+Q=O

(x,y)与(x,-y)关于椭圆曲线加法运算互逆。

③x1=x2，y1=y2



模素数的椭圆曲线：

设a，b∈R是满足4a^3+27b^2≠0的常实数，

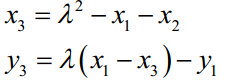
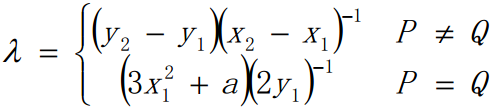
Zp上的同余方程y^2=(x^3+ax+b) mod p的所有解联通无穷远点构成椭圆曲线E。

E上的加法运算定义如下（以下所有运算都模p进行）

设P(x1,y1),Q(x2,y2)，

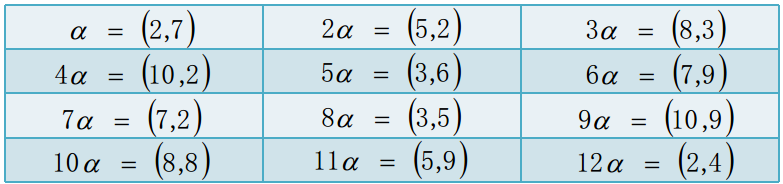
若x1=x2且y1=-y2，则P+Q=O

否则P+Q=(x3,y3)

例：E是Z11上的椭圆曲线

对生成元α=(2,7)，可用累加运算得到



私钥是7，则β=7α=(7,2)

则加密运算ek(x)=(k(2,7),x+k(7,2))，k为随机数

解密运算为dk(y1,y2)=y2-7y1

7.数字签名

7.1数字签名算法

密钥生成子算法(Gen)

输入：安全参数n；输出：签名密钥sk，验证密钥pk

数字签名子算法(Sig)

输入：签名密钥sk和消息m；输出：签名s=Sig(sk,m)

验证子算法(Vrfy)

输入：验证密钥pk，消息m，签名s；输出：b=Vrfy(pk,m,s)验证通过为1，验证失败为0

7.2签名方案的安全性

攻击模型：

唯密钥攻击：攻击者拥有公钥，即验证函数Vrfy

已知消息攻击：攻击者拥有一系列消息签名对

选择消息攻击：攻击者可以选择一系列消息并获得对应签名

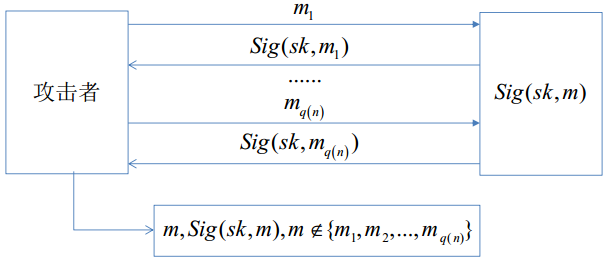
攻击目标：

完全破译：确定私钥，即签名函数Sig

选择性伪造：攻击者能以某一不可忽略的概率对另外某个人选择的消息产生一个有效签名。

存在性伪造：攻击者至少能为一则消息产生一个有效签名

抵抗选择消息攻击的数字签名算法挑战过程如下：



该算法可以抵抗选择明文攻击当且仅当

7.3 RSA签名方案

设定K={(n,p,q,a,b):n=pq,p和q是素数, ,ab≡1(mod φ(n)),φ(n)=(p-1)(q-1) }

(n,b)为公钥，(p,q,a)为私钥

Sig(x)=x^a mod n

ver(x,y)=1当且仅当x=y^b mod n

伪造签名的方法如下

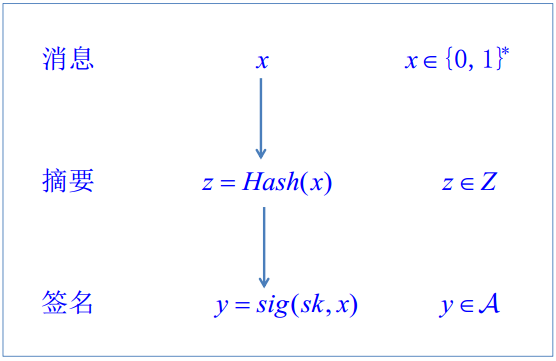
①选择y并计算x=sig(y)=y^b,则y是x的有效签名

②已知合法消息对(x1,y1),(x2,y2)可以构造消息x1x2的签名为y1,y2

③已知x，计算x≡x1x2 mod n，分别请求计算x1和x2的签名y1和y2，则x的签名为y1y2

签名与hash函数：

签名方案需要与一种非常快的公开密码的hash函数结合使用，其使用过程如下：

当

7.4ElGamal签名方案

ElGamal签名方案是非确定性的，对任意给定的消息有很多有效签名

设α是Zp的生成元，定义K={(p,α,a,β):β=α^a}

(p,α,β)是公钥，a是私钥

Sig(x,k)=() , k为秘密随机数,  ,

Ver(x, ())=true当且仅当

随机值k如果泄露且gcd()=1，则可轻易计算

7.5 Schnorr签名方案

设p是一个素数，而q是能被p-1整除的素数（q|p-1）。设α是1模p的q次根，

定义K={(p,q,α,a,β)： }

其中(p,q,α,β)为公钥，a为私钥

设h是一个安全的hash函数

Sig(x,k)=()，k为秘密随机数, ,

Ver(x, ())=true当且仅当

7.6数字签名算法DSA

设p是一个素数，而q是能被p-1整除的素数（q|p-1）。设α是1模p的q次根，

定义K={(p,q,α,a,β)： }

其中(p,q,α,β)为公钥，a为私钥

Sig(x,k)=()，k为秘密随机数, ,

定义e1= ; e2=

Ver(x, ())=true当且仅当

7.7椭圆曲线数字签名算法ECDSA

设p是一个大素数，E是定义在Fp上的椭圆曲线，设A是E上阶为q的一个点，使得<A>上的离散对数问题是个困难问题

定义K={(p,q,E,A,m,B):B}

(p,q,E,A,B)是公钥，m是私钥

Sig(x,k)=() ，k为秘密随机数,kA=(u,v) ,

验证过程如下

,i=wSHA-1(x) mod q,j=wr mod q,(u,v)=iA+jB

Ver(x, ())=true当且仅当u mod q= r

8.实体认证

8.1实体认证协议

协议定义：协议是两个或更多参与者完成某项特定任务采取的一系列步骤。协议的每一步骤必须依次执行；协议至少需要两个参与者；协议必须能完成某项任务。

实体认证协议一般是2-3个参与者为完成1-2个参与者的身份认证任务而采取的1-5个步骤。

数字签名/消息认证码的目标是确认消息源，且对确认时间范围无规定。

实体认证协议的目标是确认实体身份，对确认时间范围有规定。

8.2一个不安全的协议

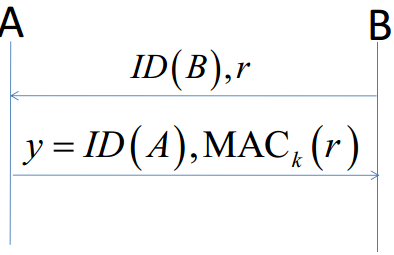
步骤：

①B选择一个随机挑战r，并传送给A

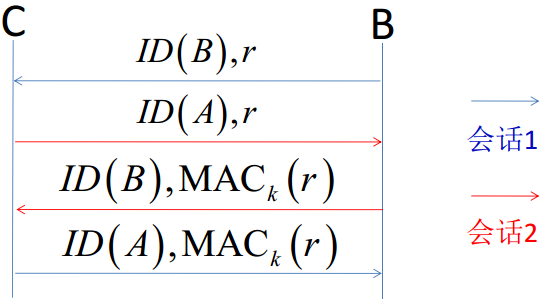
②A计算y=MACk(r)，并发送给B

③B计算y’=MACk(r)，如果y’=y那么B接受，否则拒绝

流程图：



这种协议是不安全的，其无法抵抗并行会话攻击，该攻击流程如下

C就可以冒充A进行认证。

8.3改进的实体认证协议

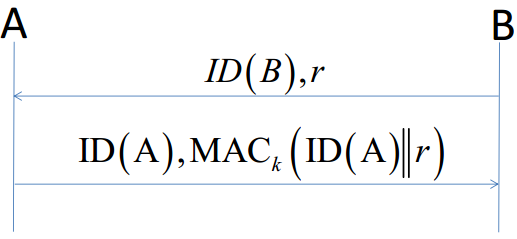
步骤：

①B选择一个随机挑战r，并传送给A

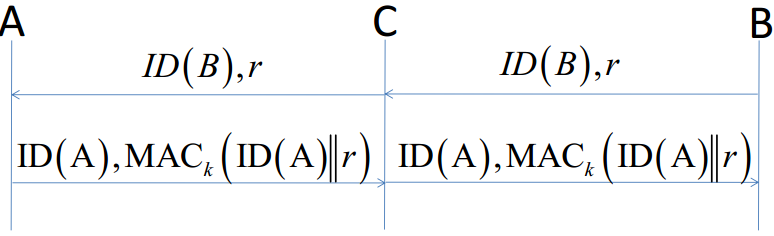
②A计算y=MACk(ID(A)||r)，并发送给B

③B计算y’=MACk(ID(A)||r)，如果y’=y那么B接受，否则拒绝

流程图



这种协议可以抵抗并行会话攻击，但攻击者可以通过以下方式存储转发

可将C视作路由器

8.4协议攻击的判定

对协议攻击的判定方法：

①协议中任意一个或多个参与者并未依次执行协议

②执行协议后并未完成任务

满足任意一条即视为攻击

8.5协议的安全性分析

安全性证明思路：

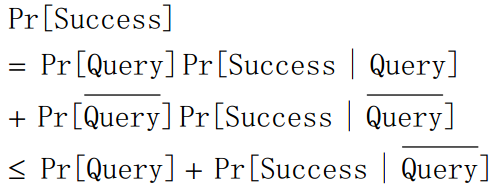
①定义安全：敌手在运行q(n)次协议后，攻陷协议的概率可以忽略

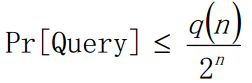
②假定协议中使用的算法是安全的，即查询q(n)个值对应的mac值后，敌手成功伪造出一个有效mac的概率不超过一个可忽略概率

③证明：如果协议不安全，那么mac算法也一定不安全

运行q(n)次协议，等于敌手知道了q(n)个ID(A)||r对应的mac值

此时对于一个随机挑战r’，可以伪造出第二条消息的概率为：

Query表示r’曾经出现过

，可以忽略

如果r’未出现过，此时敌手如果成功伪造出协议的第二条消息等价于伪造出了mac值

8.6实体认证的攻击

主动攻击：

①敌手产生一个消息并放入信道

②敌手改变信道中的消息

③敌手转移信道中的消息，并发送给其他人，而不是指定接受者。

满足任意一条说明敌手进行了主动攻击

8.7交互认证

会话成功时，参与双方都为“接收”状态。

不安全的双向认证协议

步骤：

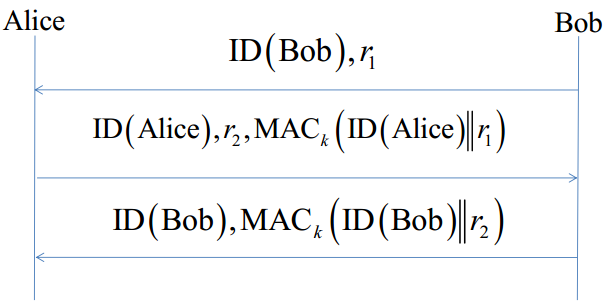
①B选择一个随机挑战r1，并传送给A

②A选择一个随机挑战r2，计算y1=MACk(ID(A)||r1)，并发送r2和y1给B

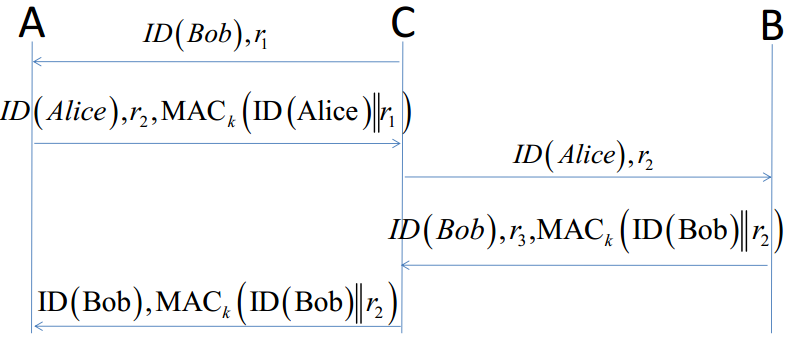
③B计算y1’=MACk(ID(A)||r1)，如果y1’=y1那么B接受，否则拒绝。同时B计算y2=MACk(ID(B)||r2)，并发送y2给A

④A计算y2’= MACk(ID(B)||r2)，如果y2=y2’，那么A接受，否则拒绝

流程图



这种协议不安全，C可以以下方式欺骗A



改进的双向实体认证协议：

步骤：

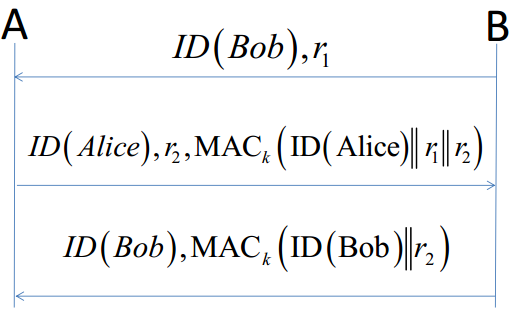
①B选择一个随机挑战r1，并传送给A

②A选择一个随机挑战r2，计算y1=MACk(ID(A)||r1||r2)，并发送r2和y1给B

③B计算y1’=MACk(ID(A)||r1||r2)，如果y1’=y1那么B接受，否则拒绝。同时B计算y2=MACk(ID(B)||r2)，并发送y2给A

④A计算y2’= MACk(ID(B)||r2)，如果y2=y2’，那么A接受，否则拒绝

流程图：



8,8公钥环境下的实体认证方案

在公钥环境下，Alice和Bob没有预先的共享秘密密钥。

假定他们针对特定的密码体制以及签名方案，他们都有相应的公钥和私钥。

证书Cert包含用户的身份信息、公钥以及签名，证书允许网络用户验证彼此公钥的真实性

用户通过公钥基础设施PKI，向认证中心CA出示身份证明与证书颁发申请，由CA制作证书后颁发给用户。公钥和私钥在用户端生成，CA只是通过签名认证用户提交的公钥。

双向实体认证协议：

步骤：

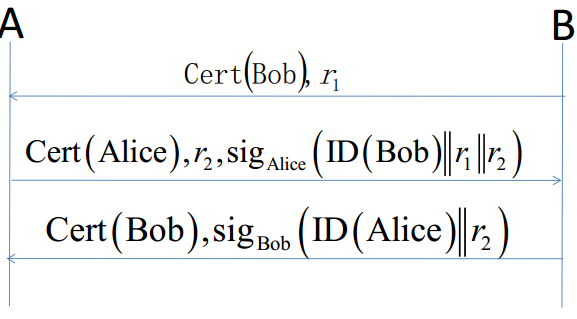
①B选择一个随机挑战r1，并传送给Cert(B)和r1给A

②A选择一个随机挑战r2，计算y1=sigA(ID(B)||r1||r2)，并发送Cert(A),r2和y1给B

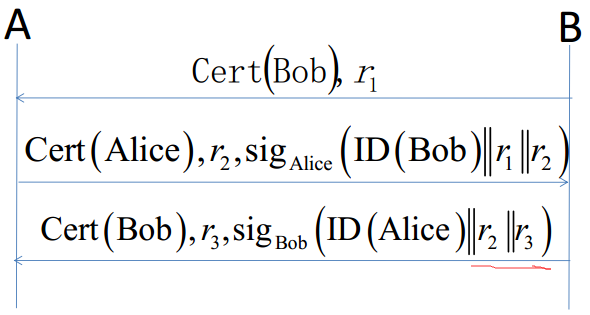
③B利用证书Cert(A)验证A的公钥verA,并验证verA(ID(B)||r1||r2,y1)=true是否成立，如果成立，那么B接受，否则拒绝。同时B计算y2=sigB(ID(A)||r2)，并发送y2给A

④A利用证书Cert(B)验证B的公钥verB,并验证verB(ID(A)||r2,y2)=true是否成立，如果成立，那么A接受，否则拒绝

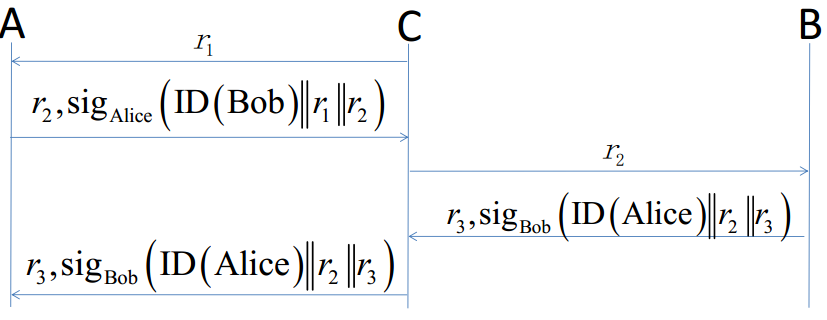
流程图：



不安全的双向实体认证协议



其攻击形式为



9安全规约

9.1概念区分

密码学Cryptography：密码学各个研究领域，比如公钥密码学

密码系统Cryptosystem：算法，提供一种安全性服务

方案Scheme：某种算法系统的具体构造方案

9.2安全模型Security Model

安全模型可以被视为对一密码系统多种攻击的摘要，如果某一方案在安全模型下是安全的，那么这个安全模型下所有攻击都是可以被这个方案抵抗的。抽象攻击关注敌手可以获得什么信息而不是如何攻击。

**安全模型可以被视作一个挑战者和敌手之间交互的挑战游戏。其定义如下：**

敌手能力：敌手可以询问的信息；敌手可以询问信息的时间；

敌手安全目标：敌手如何赢得游戏，攻破系统；

**安全模型的四个组成部分：**

初始化Setup：攻击者和挑战者之间初始化条件

能力Capabilities：描述攻击者的询问的内容和时间

安全目标Security Goal：对于攻击者来说的获胜条件

优势Advantage：一个参数，如果这个参数是可忽略的(negligible),则密码系统是安全的，否则是不安全的。

**在安全性模型定义中不考虑一下两个方面：**

攻击者可以直接攻破密码系统的简单攻击（trivial attack），比如直接询问私钥

攻击者获得信息片的策略(strategy)，因此挑战者必须对敌手询问诚实应答

**当定义安全模型时，优势是可忽略的**

例如：数字签名的安全模型

初始化：密钥对生成，并且敌手获知pk

能力：敌手获取一批消息的签名

安全目标：敌手不可伪造新签名

优势：成功伪造新签名的可能性

注意：

①一个密码系统可能有多个安全服务，每个安全服务都需要一个安全模型

②同一安全服务可能有不同安全模型，依赖于安全能力与安全目标，比如标准安全性模型，弱安全模型（敌手能力弱，抵抗少的攻击），强安全模型（敌手能力更强，可以抵抗更强的安全攻击）

9.3安全性规约security reduction

定义：从不安全性推导得到某困难问题是容易的一个过程。

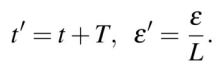
其核心为生成一个方案，概念区分为

安全模型：真实方案real scheme（安全方案），挑战者challenger，真实攻击 real attack

规约：模拟方案simulated scheme（困难问题的随机实例），模拟者simulator，模拟 simulation

模拟者模拟了挑战者与敌手进行交互

规约成本与规约丢失：

存在攻击者可以以多项式时间t和不可忽略的优势攻破一个方案，在安全规约中，可以构造一个模拟者去解决困难问题的时间和优势为，

则T为规约成本

L为规约丢失，L最小值为1

松规约(Loose)：L至少与询问数成线性关系

紧规约(Tight)：L是常数或更小

理想的安全规约包括：

安全性模型、困难问题、规约成本和规约丢失、对敌手计算量的限制

10.安全性证明security Proof

10.1证明组件

通过安全性规约进行安全性证明应该有一下组成部分：

模拟simulation：规约算法应该表明模拟者如何产生模拟方案与敌手交互

解决方案Solution：规约算法应该表明模拟者如何在敌手对模拟方案攻击的帮助下，通过返回问题实例的解决方案来解决困难问题

分析Analysis：在模拟和解决方案后，分析模拟与真实攻击的不可区分性、成功模拟的可能性Ps,解决困难问题的优势，规约成本、规约丢失等。