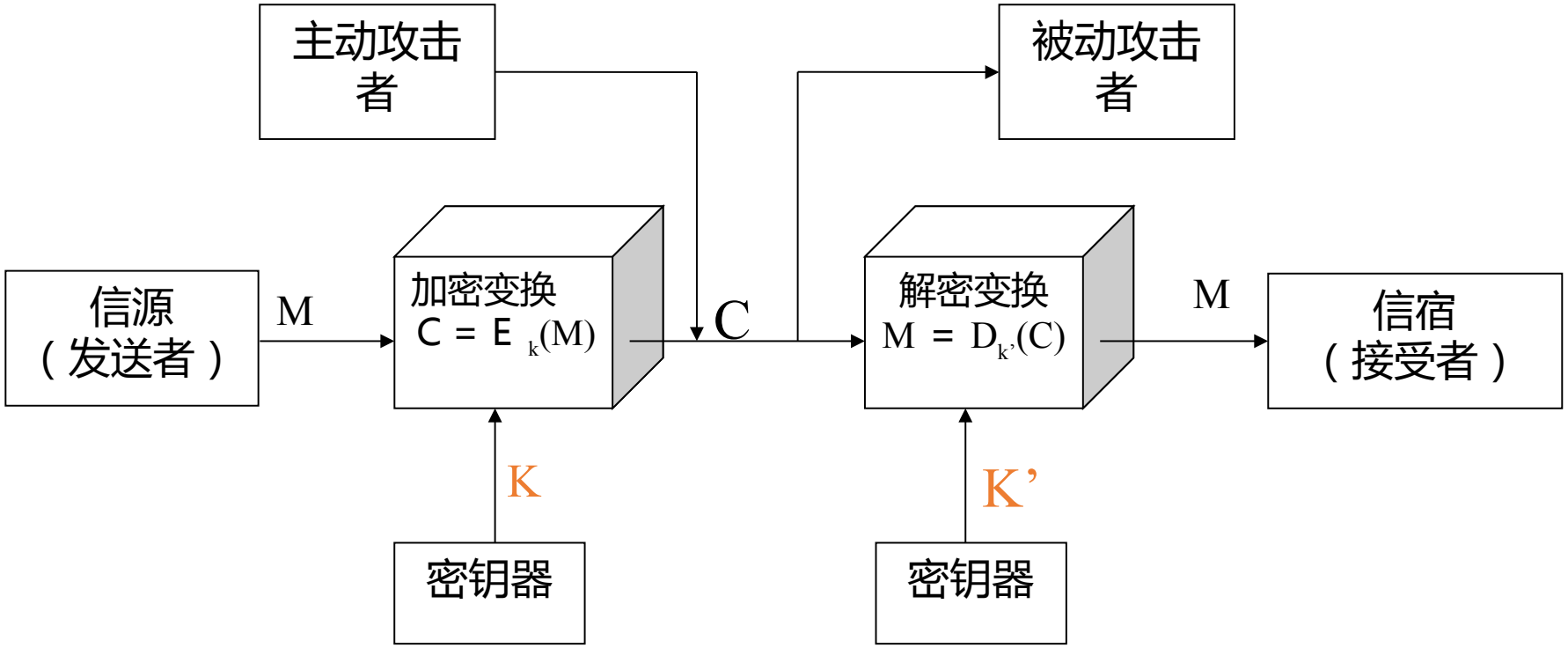
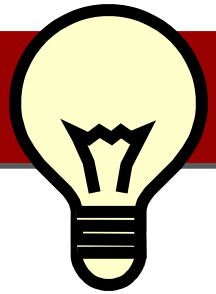
密码学算法

密码系统及基本术语



古典密码学算法回顾

- 凯撒密码
- Vigenere 密码
- Hill 密码
- 置换密码



现代密码算法

现代密码体制的**Kerckhoff's**原则是：所有加密解密算法都是公开的，保密的只是密钥。

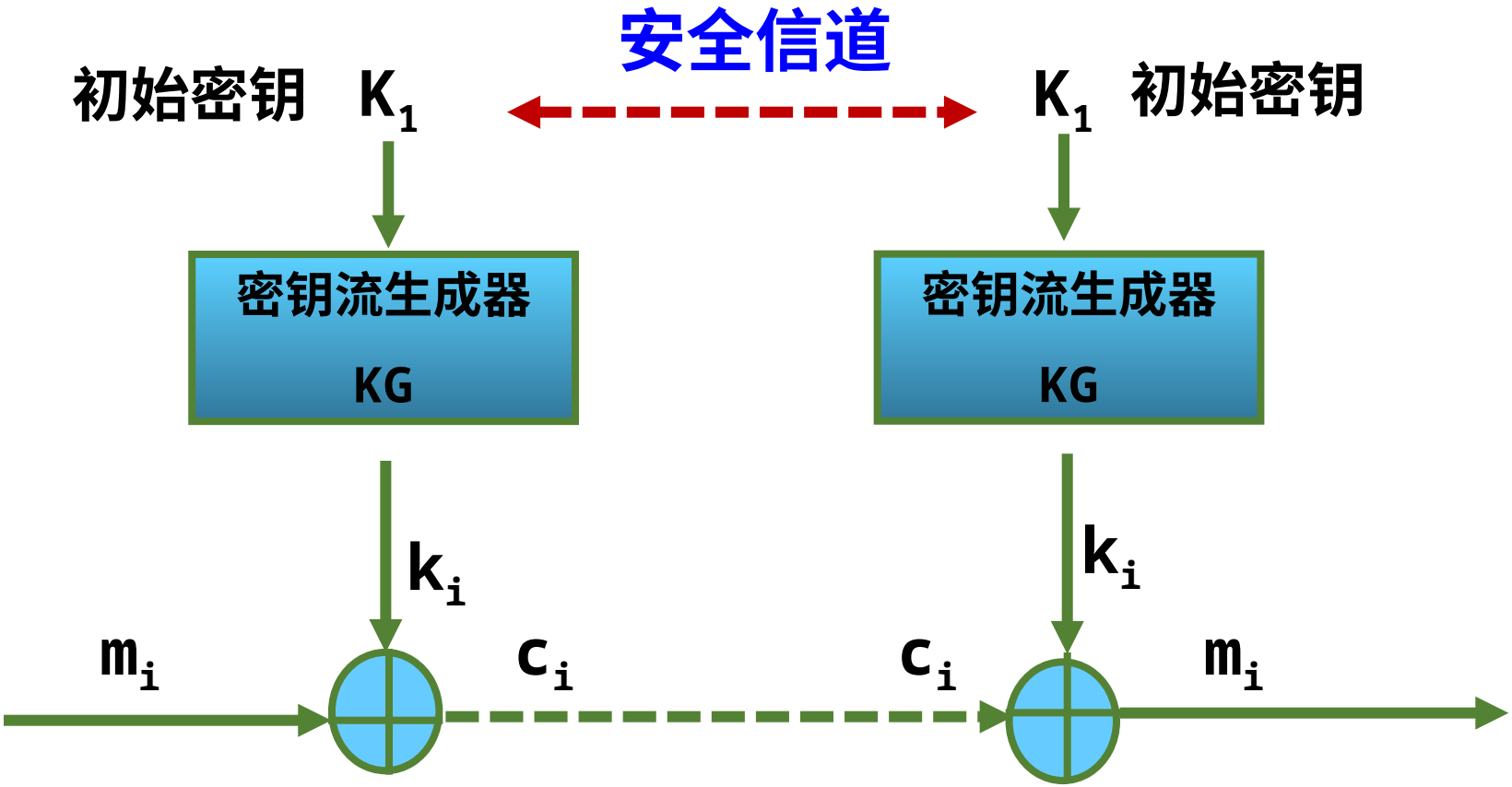
- 算法的公开和密钥的保密

现代密码算法回顾

- 对称密码体制：
  - 序列密码算法（流密码）：RC4
  - 分组加密算法（Block Cipher）：DES，SM4，SM1，SM7
- 非对称密码体制
  - 基于因子分解难题：RSA，SM2，SM9
  - 基于离散对数难题：ECC
- 消息摘要算法：MD5、SHA1，SHA256，SM3
- 密钥交换算法：Diffle-Hellman

序列密码

流密码原理框图



RC4 算法

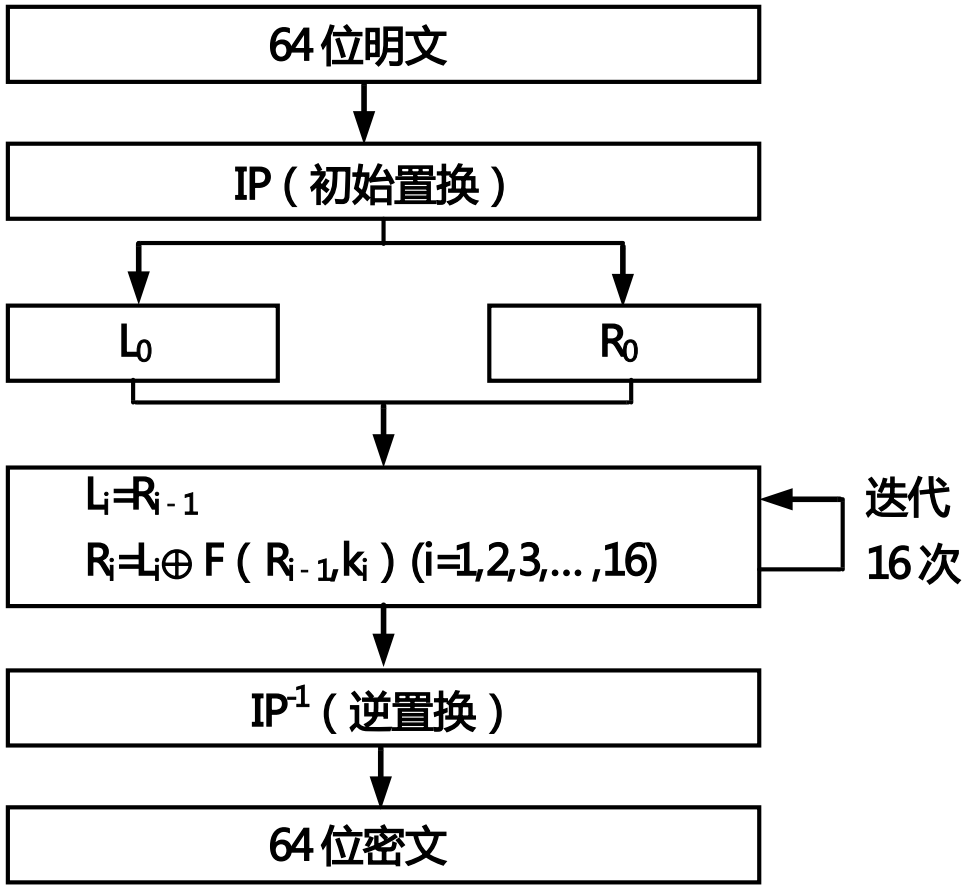
- 1. 用 Key
- 成 S 盒

```
1.   for i from 0 to 255
2.       S[i] := i
3.   endfor
4.   j := 0
5.   for i from 0 to 255
6.       j := (j + S[i] + key[i mod keylength]) mod 256
7.       swap values of S[i] and S[j]
8.   endfor
```

- **2. 利用 S 盒**
- **生成密钥流**

```
i := 0
j := 0
while GeneratingOutput:
    i := (i + 1) mod 256  // a
    j := (j + S[i]) mod 256 // b
    swap values of S[i] and S[j]  // c
    K := S[(S[i] + S[j]) mod 256] // d
    output K
endwhile
```

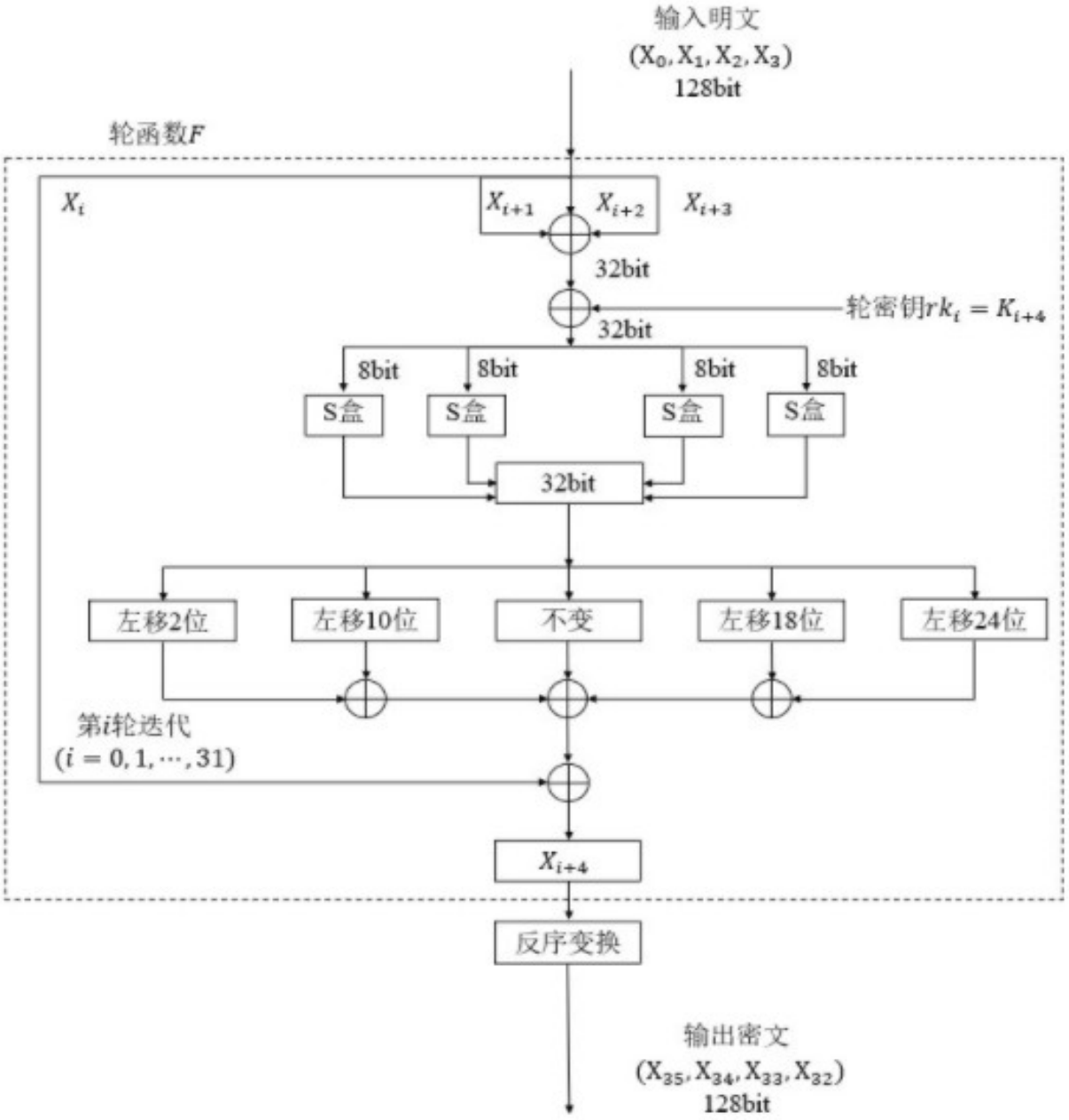
DES 加密算法



DES 加密运算过程

64 位明文首先进行初始置换（ IP ），初始置换结果被分成两部分： L_0 和 R_0 ，它们成为 Feistel 分组密码结构的原始输入。经过 16 次迭代运算的结果就是 Feistel 分组密码结构的输出 L_{n+1} 和 R_{n+1} ，对其进行初始置换对应的逆置换，逆置换结果就是 DES 加密运算后的密文。

SM4 加密算法


输入明文
(X_0, X_1, X_2, X_3)
128bit
轮函数F
X_i
X_{i+1}
X_{i+2}
X_{i+3}
32bit
轮密钥$rk_i = K_{i+4}$
32bit
8bit
8bit
8bit
8bit
S盒
S盒
S盒
S盒
32bit
左移2位
左移10位
不变
左移18位
左移24位
第i轮迭代
$(i = 0, 1, \cdots, 31)$
X_{i+4}
反序变换
输出密文
$(X_{35}, X_{34}, X_{33}, X_{32})$
128bit

DES 和 SM4 比较

	DES算法	SM4算法
计算基础	二进制	二进制
算法结构	使用标准的算术和逻辑运算、先代替后 置换，不含非线性变换	基本轮函数加迭代、含非线性变换
加解密算法是否相同	是	是
计算轮数	16轮（3des为16轮*3）	32轮
分组长度 64位 128位	64位	128位
秘钥长度	64位（3DES为128位）	128位
有效秘钥长度	56位（3des位112位）	128位
实现难度	易于实现	易于实现
实现性能	软件实现慢、硬件实现快	软件实现和硬件实现都快
安全性	较低（3des较高）	算法教新，还未经过现实校验

RSA 算法

1978 由 Rivest, Shamir, Adleman 提出。

- 其安全性依赖于大整数分解的难度（**integer factorization problem**）
- 参数有： n=pq, $\varphi(n)$ = (p-1)(q-1) 为欧拉函数
- 公钥为 e ，并满足 (e, $\varphi(n)$) = 1
- 私钥为 d ， $d=e^{-1} \bmod \varphi(n)$
- encryption: $m \to c = m^e \bmod n$
- decryption: $c \to c^d = m \bmod n$

ECC 密码

- 1．椭圆曲线和公共参数的选取

设p为一个大素数，选择一条基于有限域$\mathbb{F}_p$椭圆曲线E_p为：

$$y^2 = x^3 + ax + b \ mod \ p$$

$x, y \in \mathbb{F}_p, 4a^3 + 27b^2 \ mod \ p \neq 0$。$E(\mathbb{F}_p)$构成相应的 Abel 群

选取G为$E(\mathbb{F}_p)$上的一个基点，其阶为大素数q，即满足$qG = O^{\infty}$；

公共参数为$\{E(\mathbb{F}_p), p, q, G\}$.

- 2．密钥的生成：

随机选取d，使得 $2 \leq d \leq q-1$，利用公共参数G，计算$P = dG$。

d为私钥，P为公钥。

ECC 密码

- 3．加密

对明文$M=(m1,m2)\in \mathbb{F}_p^* \times \mathbb{F}_p^*$，具体的加密过程如下：

1)随机选取k，使得$2\le k\le q-1$，利用公钥P计算$Q=kP$，记$Q=(Q_x,Q_y)$，其中Q_x,Q_y为非零元素；

2)利用公共参数G，计算辅助解密参数：$C_0=kG$；

3)加密明文 $C_1=m1\cdot Q_x \bmod p$；

4)加密明文 $C_2=m2\cdot Q_y \bmod p$；

5)最后，明文M经 ECC 加密后的结果是(C_0,C_1,C_2)。

ECC 密码

- 4．解密

对接收到的密文$(C_0, C_1, C_2) \epsilon E(\mathbb{F}_p) \times \mathbb{F}_p^* \times \mathbb{F}_p^*$，

1)利用自己的私钥d，计算$dC_0 = (R_x, R_y)$；

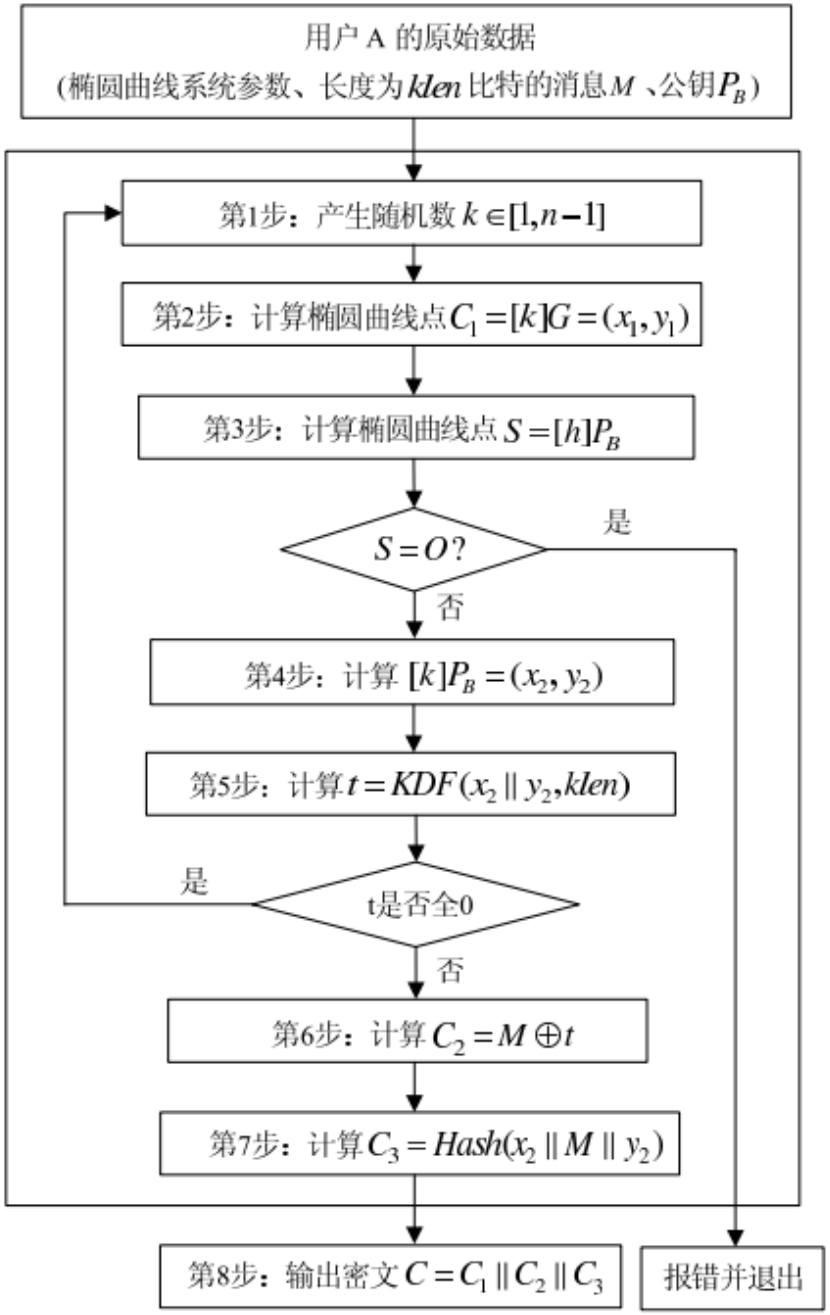
2)计算明文$m1 = C_1 \cdot R_x^{-1} mod\ p$；

3)计算明文$m2 = C_2 \cdot R_y^{-1} mod\ p$；

4)拼接$M = (m1, m2)$，解密完成。

SM2 加密算法

- 基本与 ECC 一致



MD5

- **1、数据填充：**对消息进行数据填充，使消息的长度对 512 取模得 448 ，并添加消息长度。最终消息长度就是 512 的整数倍。
- **2、数据说明：**
- 4 个常数： A = 0x67452301, B = 0x0EFCDAB89, C = 0x98BADCFE, D = 0x10325476;
- 4 个函数： F(X,Y,Z)=(X & Y) | ((~X) & Z); G(X,Y,Z)=(X & Z) | (Y & (~Z)); H(X,Y,Z)=X ^ Y ^ Z; I(X,Y,Z)=Y ^ (X | (~Z));
- 2 个预置参数： T (64) , S (64)

MD5

- 3．数据处理
- 把消息分以 512 位为一分组进行处理，每一个分组进行 4 轮变换每一轮变换分别调用， 16 次 FF(A,B,C,D,mj,s,ti) ， 16 次 GG(A,B,C,D, mj,s,ti) ， 16HH(A,B,C,D, mj,s,ti) ， 16 次 II(A,B,C,D, mj,s,ti) 。
- 最后的结果，即 MD5 值。

SM3 算法

对长度为 l(l < 264) 比特的消息 m ， SM3 杂凑算法经过填充和迭代压缩，生成杂凑值，杂凑值长度为 256 比特。

备注：填充后的消息 m′ 的比特长度为 512 的倍数

Diffie-Hellman 密钥交换

两个通信主体 Alice 和 Bob ，希望在公开信道上建立共享密钥

1.选择一个大素数 p (~ 200 digits) ，一个生成元 a

2.Alice 选择一个秘密钥 (private key) $x_A < p$ ， Bob 选择一个秘密钥 (private key) $x_B < p$

3.Alice and Bob 计算他们的公开密钥 : $y_A = a^{x_A} \bmod p$ ， $y_B = a^{x_B} \bmod p$ ， Alice , Bob 分别公开 y_A , y_B

4.计算共享密钥： $K_{AB} = a^{x_A x_B} \bmod p$ $=(y_A^{x_B})$mod p (which B can compute) $=(y_B^{x_A})$mod p (which A can compute)

5. K_{AB} 可以用于对称加密密钥

课堂讨论 - 国产商用密码路在何方？

- **题目：在我国全面使用国产商用密码的优劣？困难和出路？**

- 国际主流商用密码算法有 DES、AES、MD5、SHA1、SHA3、RSA、ECC 等，我国商用密码有 SM4，SM3，SM2 等等。现有的信息系统和产品，例如支付宝、微信支付、数字杭电统一登录系统等等目前均还是使用国际主流商用密码，那么如果要在我国全面使用国产商用密码，请结合国际形势、算法安全程度、技术实现和社会实践等几方面分析优势和劣势？困难和出路？