密码学基础

文档作者：LoanCold/SocialistDalao/李程浩

Thursday, December 10, 2020 10:24 PM

图片来自课件

1. 密码学攻击方法
    a. 穷举攻击（增大密钥以对抗）
    b. 统计分析攻击（减少明文与密文的统计相关性）
    c. 解密变化攻击（算法复杂化）
2. 密码攻击环境
    a. 唯密文攻击（COA）：仅仅知道一些密文
    b. 已知明文攻击（KPA）：仅仅知道一些明文和对应的密文
    c. 选择明文攻击（CPA）：选择一些明文，并且得到对应的密文
    d. 选择密文攻击（CCA）：选择一些密文，并且得到对应的明文
3. 密码学四大性质
    a. 机密性：保密信息不会透露（加密算法保证）
    b. 完整性：篡改能被检测（“指纹”校验，MAC）
    c. 认证性：身份（来源和消息本身）确认（利用密钥和认证函数相结合）
    d. 不可否认性：无法否认信息生成、签名、接收行为（数字签名）
    e. 可用性（信息安全关注）：信息资源随时可以提供服务的能力特性
4. 古典密码学
    a. 代换密码
        i. 单字母单表密码
            1) Caesar
                a) $C_i = (M_i + k) \bmod 26$
                b) $M_i = (C_i - k) \bmod 26$
            2) Affine cipher
                a) $Ci = (aM_i + b) \bmod 26$
                b) $M_i = a^{-1}(C_i - b) \bmod 26$
            3) Mixed alphabetic cipher
                a) 给定每个字母之间的映射，按照该映射关系进行加密
            4) 安全性：无法抵御统计攻击
        ii. 单字母多表密码
            1) Vigenere
                a) $C_i = (M_i + k_{i \bmod l}) \bmod 26$
                b) $M_i = (C_i - k_{i \bmod l}) \bmod 26$
            2) Rotor machine轮转密码机
                a) 有限个周期重复的固定代换表
            3) One-time pad（OTP）一次一密
                a) 密钥和明文一样长，且不能重复使用
        iii. 多字母密码

1) Playfair
   a) 挑选一个单词作为密钥
   b) 字母填入5X5矩阵
   c) 将明文分为两个字符一组
   d) 按照两个字母在矩阵中的关系进行加密
2) Hill（矩阵加密）
   a) $\mathbf{C} = \mathbf{KM} \bmod 26$
   b) $\mathbf{M} = \mathbf{K}^{-1}\mathbf{C} \bmod 26$

iv. 安全性分析
1) 都无法避免统计规律

b. 置换密码
i. 栅栏密码
1)

ext: meet me after the toga party
itext out as:
m e m a t r h t g p r y
e t e f e t e o a a t
: MEMATRHTGPRYETEFETEOAAT

ii. 列移位密码
1) 按固定列数排列
2) 按列移动（根据密钥）
3) 按列读出
4)

ext: attack postponed until two am

4	3	1	2	5	6	7
a	t	t	a	c	k	p
o	s	t	p	o	n	e
d	u	n	t	i	l	t
w	o	a	m	x	y	z

TTNAAPTMTSUOAODWCOIXKNLYPETZ

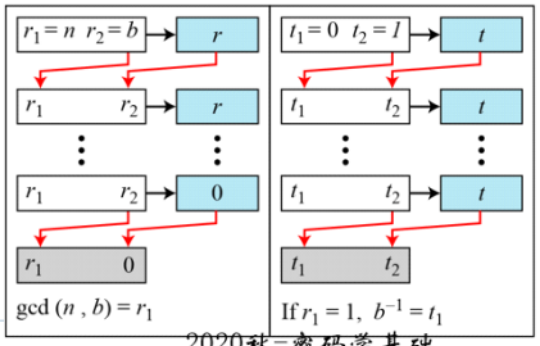
c. 总结
i. 单表代换：明文密文一对一
ii. 多表代换和多字母代换：不是一对一
iii. 替换密码：打乱明文顺序

数学原理

Thursday, December 10, 2020 11:16 PM

1. 模运算
   a. Extend Euclidean algorithm
      i. 求解乘法逆元

a. Process



b. Algorithm

```
r1 ← n;     r2 ← b;
t1 ← 0;     t2 ← 1;
while (r2 > 0)
{
  q ← r1 / r2;
  r ← r1 − q × r2;
  r1 ← r2;     r2 ← r;
  t ← t1 − q × t2;
  t1 ← t2;     t2 ← t;
}
if (r1 = 1) then b^-1 ← t1
```

      ii. ***Extended Euclidean algorithm***

a. Process b. Algorithm

   b. Chinese remainder theorem CRT
      - $a_1 \equiv A \bmod m_1$
      - $a_2 \equiv A \bmod m_2$
      - ...
      i. - $a_k \equiv A \bmod m_k$

The set of the congruences has a unique solution A modulo M

      ii. 解:

$$x = \left(\sum_{i=1}^{n} a_i t_i M_i \right) mod M$$

$$M_i = M/m_i,$$

$$t_i = M_i^{-1}$$

$$M_i t_i \equiv 1 \pmod{m_i},$$

2. 群环域
   a. Z_n

Figure ***Some Z_n and Z_n^* sets***

加法群

$\mathbf{Z}_6 = \{0, 1, 2, 3, 4, 5\}$

$\mathbf{Z}_7 = \{0, 1, 2, 3, 4, 5, 6\}$

$\mathbf{Z}_{10} = \{0, 1, 2, 3, 4, 5, 6, 7, 8, 9\}$

乘法群

$\mathbf{Z}_6^* = \{1, 5\}$

$\mathbf{Z}_7^* = \{1, 2, 3, 4, 5, 6\}$

$\mathbf{Z}_{10}^* = \{1, 3, 7, 9\}$

b. 伽罗瓦域 Galois Field GF(p)

$$\forall\ a \in Z_p,\ \gcd(a,\ p) = 1,\ \exists\ a^{-1} \in Z_p \text{ s.t. } a \times a^{-1} = 1$$

3. 多项式运算
   a. GF(2)上的多项式
   b. 质多项式

$GF(2^3)$	0	1	x	$x+1$	x^2	x^2+1	x^2+x	x^2+x+1
	000	001	010	011	100	101	110	111
Z_8	0	1	2	3	4	5	6	7

   c. 快速运算

For example, if B_2 is 10000011, we can write

$$\begin{aligned} & B_1 \times 10000011 \\ = & B_1 \times (00000001 + 00000010 + 10000000) \\ = & (B_1 \times 00000001) + (B_1 \times 00000010) + (B_1 \times 10000000) \\ = & (B_1 \times 00000001) \oplus (B_1 \times 00000010) \oplus (B_1 \times 10000000) \end{aligned}$$

76

4. 素数Prime
   a. 素数判定
   b. 欧拉函数
      i. $\phi(1) = 0$
      ii. $\phi(p) = p - 1$ if p is prime
      iii. $\phi(mn) = \phi(m)\phi(n)$if m, n is prime
      iv. $\phi(p^e) = p^e - p^{e-1}$ if p is prime
      v. $n = p_1^{e_1} \times p_2^{e_2} \times \ldots \times p_k^{e_k}$

$$\phi(n) = (p_1^{e_1} - p_1^{e_1-1}) \times (p_2^{e_2} - p_2^{e_2-1}) \times \cdots \times (p_k^{e_k} - p_k^{e_k-1})$$

5. 素数性质
   a. 费马小定理 Fermat's little theorem
      i. $a^{p-1} = 1 \bmod p$
      ii. $a^p = a \bmod p$
      iii. $a^{-1} \bmod p = a^{p-2} \bmod p$
   b. 欧拉定理 Euler's theorem
      i. $a^{\phi(n)} \bmod n = 1$
      ii. $a^{\phi(n)+1} \bmod n = a$
      iii. $a^{-1} \bmod n = a^{\phi(n)-1}$
6. 素数生成
   a. 费马检测

      $a^{n-1} \bmod n = 1$ if n is prime
   b. Miller-Rabin 检测n是否为素数
      i. 分解: $n - 1 = m * 2^k$
      ii. 随机选择一个底a，k次费马检测

$$a^{n-1} = a^{m \times 2^k} = [a^m]^{2^k} = [a^m]^{2^{2^{\cdot^{\cdot^{\cdot^{2}}}}}} \quad k \text{ times}$$

Algorithm 9.2 *Pseudocode for Miller-Rabin test*

```
Miller_Rabin_Test (n, a)                    // n is the number; a is the base.
{
    Find m and k such that n − 1 = m × 2^k
    T ← a^m mod n
    if (T = ± 1)  return "a prime"
    for (i ← 1 to k − 1)                    // k − 1 is the maximum number of steps.
    {
        T ← T^2 mod n
        if (T = +1) return "a composite"
        if (T = −1) return "a prime"
    }
    return "a composite"
}
```

7. 因式分解
   a. 性质：
      i. $n = p_1^{e_1} * p_2^{e_2} * \cdots * p_k^{e_k}$
      ii. $\mathrm{lcm}(a,b) * \gcd(a,b) = a * b$
   b. 暴力分解：从1到√n一直找因子
   c. 费马分解
      i. 原理: $n = x^2 - y^2, a = x - y, b = x + y$
      ii. 算法：

Algorithm 9.4 *Pseudocode for Fermat factorization*

```
Feramat_Factorization (n)                   // n is the number to be factored
{
    x ← √n                                  // smallest integer greater than √n
    while (x < n)
    {
    w ← x^2 − n
    if (w is perfect square)  y ← √w;  a ← x+y;  b ← x−y;  return a and b
    x ← x + 1
    }
}
```

8. 二次同余 Quadtratic Congruence
   a. 定义
      i. $x^2 = a \pmod n$
      ii. a is called quadratic residue if the equation have two solutions
      iii. a is called quadratic nonresidue if the equation has one solution
   b. 欧拉定理
      i. $a^{(p-1)/2} = 1 \ mod \ p$ -> a quadratic residue
      ii. $a^{(p-1)/2} = -1 \ mod \ p$ -> a quadratic nonresidue
      iii. others for no solution
9. 指数对数 Exponentiation and Logarithm
   a. 快速指数运算

Algorithm 9.7 *Pseudocode for square-and-multiply algorithm*

```
Square_and_Multiply (a, x, n)
{
    y ← 1
    for (i ← 0 to n_b − 1)                    // n_b is the number of bits in x
    {
        if (x_i = 1)    y ← a × y  mod n       // multiply only if the bit is 1

        a ← a^2 mod n                          // squaring is not needed in the last iteration
    }
    return y
}
```

表 9.4 计算 $a^b \bmod n$ 的快速模幂算法，其中 a=7, b=560=1000110000, n=561

i	9	8	7	6	5	4	3	2	1	0
b_i	1	0	0	0	1	1	0	0	0	0
c	1	2	4	8	17	35	70	140	280	560
d	7	49	157	526	160	241	298	166	67	1

b. 暴力对数运算

Algorithm 9.8 *Exhaustive search for modular logarithm*

```
Modular_Logarithm (a, y, n)
{
    for (x = 1 to n −1)                       // k is the number of bits in x
    {
        if (y ≡ a^x mod n) return x
    }
    return failure
}
```

c. 本原根 primitive root

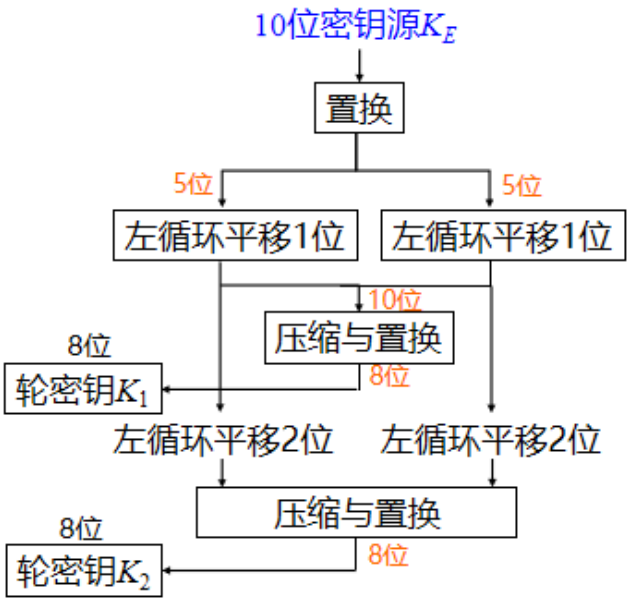
i. Z_n^* has primitive roots only if n is $2, 4, p^t, 2p^t$

ii. the number of primitive roots is $\phi(\phi(n))$

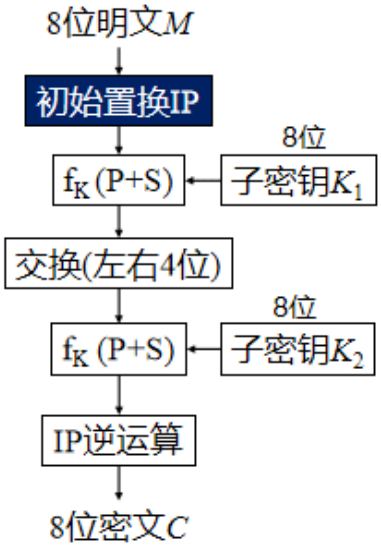
DES与AES

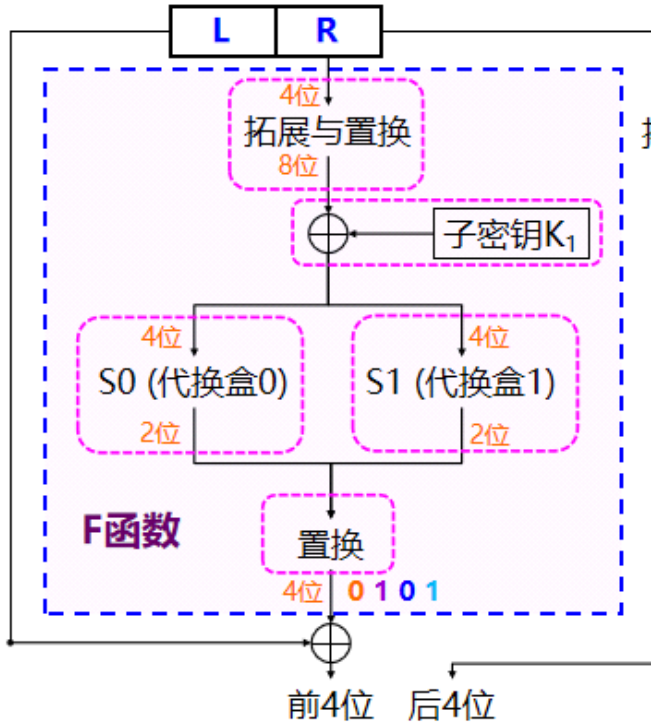
Sunday, December 13, 2020 10:20 AM

1. 对称加密
    a. 分组密码/块密码
    b. 序列密码/流密码：内部有记忆元件
2. 分组密码设计准则
    a. 混淆Confusion：密文与密钥之间的统计关系复杂
        i. 一般只用来序列加密
        ii. 操作：代换
    b. 扩散DIffusion：明文统计特性散布到密文中
        i. 序列加密和分组加密都可以使用
        ii. 操作：置换
3. 分组密码设计方法
    a. 乘积Product
        i. 顺序执行多个代换和置换
    b. 迭代Round
        i. 每轮使用S盒和P盒及其他方法，执行多轮
4. DES
    a. 简化DES原理
        i. 两部分：加密和密钥生成
        ii. 密钥生成



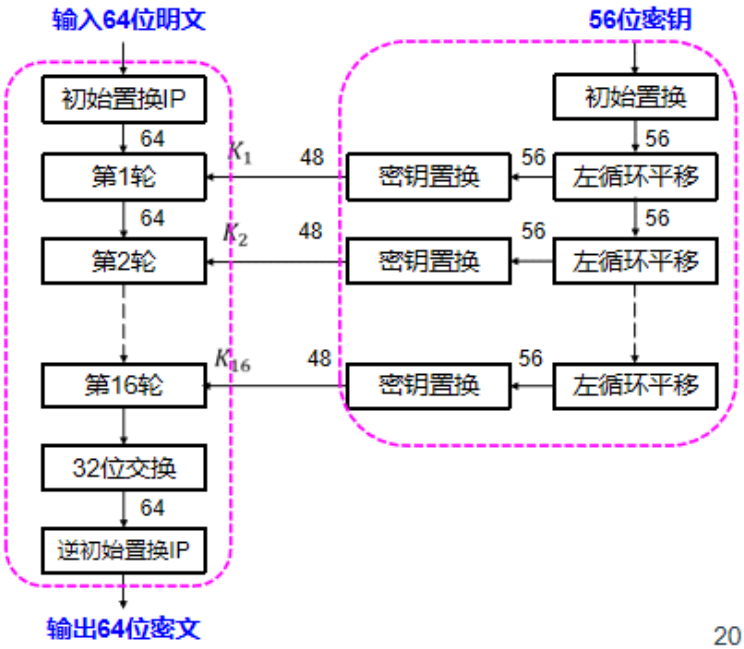
    iii. 加密



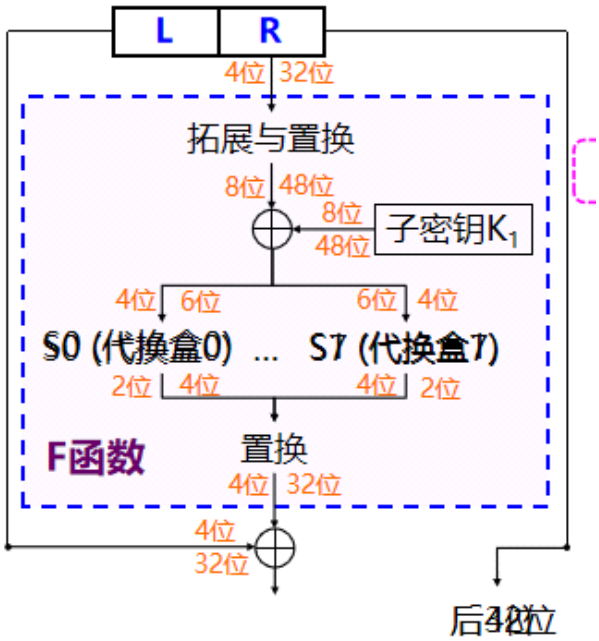


b. DES原理

- 参数
  - 密钥56比特
  - 明文/密文64比特
  - 轮数16
- 轮密钥生成
  - 初始置换
  - 16轮包括左循环平移和置换的轮密钥生成
- 加密
  - 初始置换
  - 16轮包括P盒和S盒的轮函数
  - 左右两部分交换位置
  - 初始置换的逆置换



20



c. DES安全性

i. 差分分析：CPA

ii. 线性分析：KPA

iii. 弱密钥问题

iv. 线性B盒

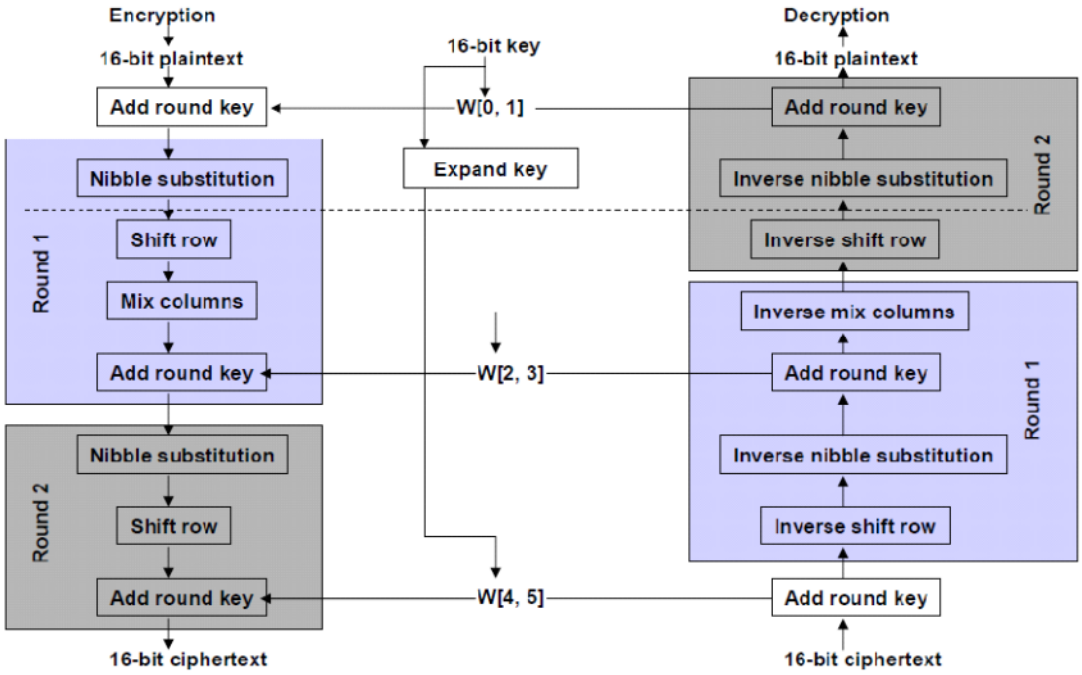
5. AES

a. 简化AES与AES参数

```
Key size = 16 bits (128/192/256 bits for AES)
Number of rounds = 2 (10/12/14 for AES)
Plaintext block = 16 bits (128 bits for AES)
Ciphertext block = 16 bits (128 bits for AES)
```

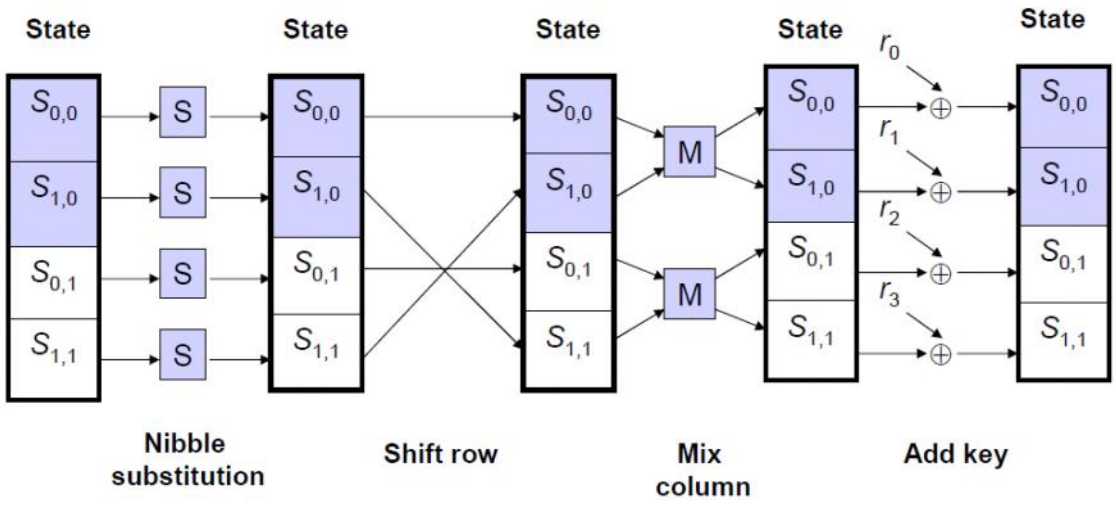
b. 简化AES

i. 总体流程

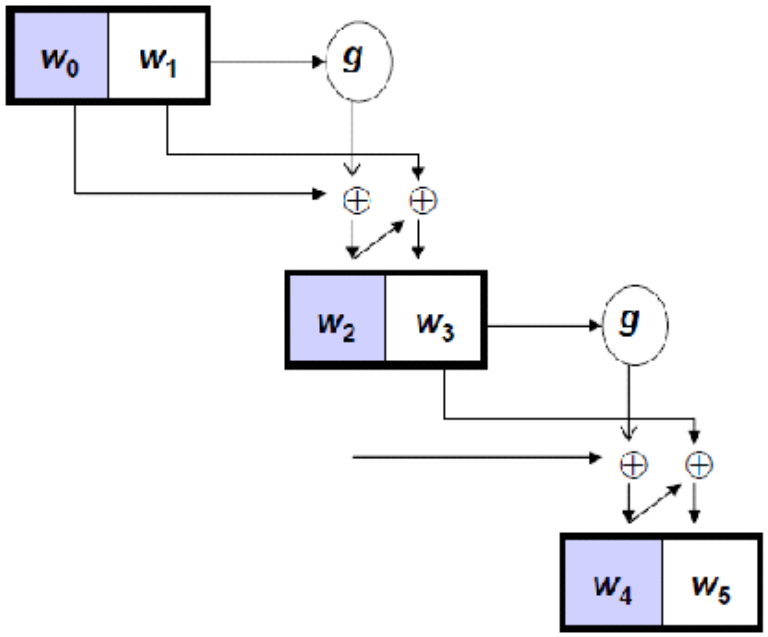


ii. 加密流程

s盒代换、行置换、列混淆、密钥轮加



iii. 密钥拓展

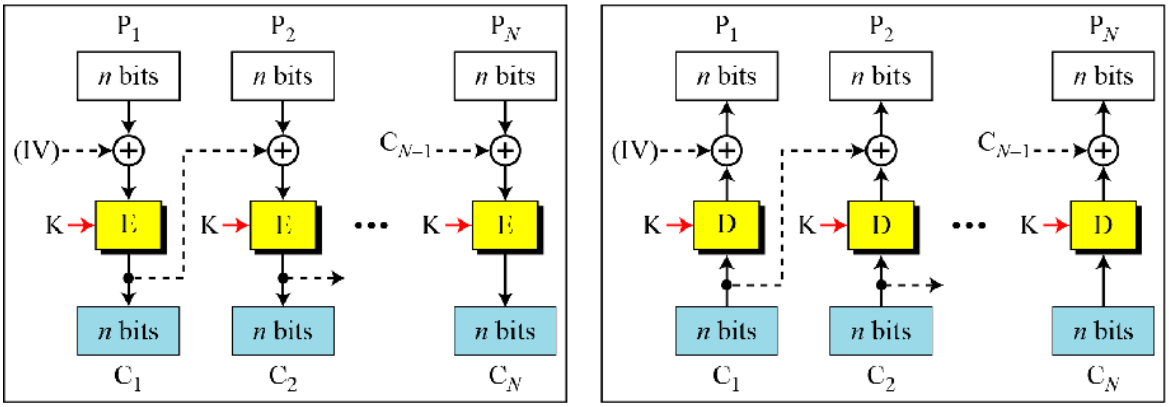


分组密码操作模式

Sunday, December 13, 2020 10:49 AM

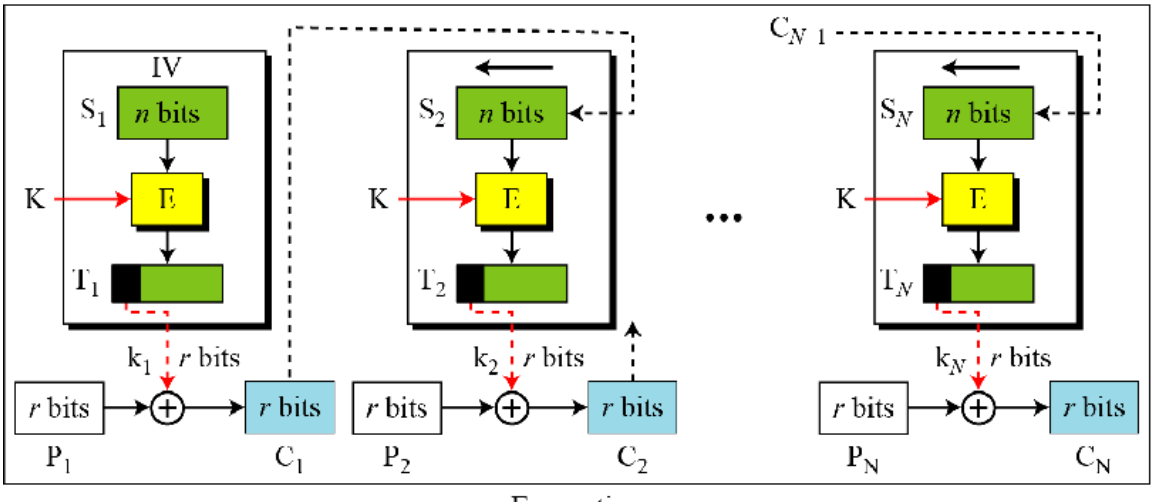
1. 电码本ECB
   a. 加密：每次加密密钥相同
   b. 适用：短消息加密
   c. 容易暴露明文数据的格式和统计特征
   d. 不会产生错误转播Error Propagation效应
2. 密码分组链接CBC
   a. 加密：输入是明文和前一次密文的异或

E: Encryption D : Decryption
P_i: Plaintext block i C_i : Ciphertext block i
K: Secret key IV: Initial vector (C_0)



   b. 会出现传播错误
   c. 能隐蔽明文的数据模式
   d. 要注意IV的使用，不能IV+1和chained IV， 他们都不能解决CPA攻击
3. 密码反馈CFB
   a. 可以进一步将DES转化为流密码
   b. 加密：输入是移位寄存器，加密的也是移位寄存器，最后与明文异或

E : Encryption D : Decryption S_i: Shift register
P_i: Plaintext block i C_i: Ciphertext block i T_i: Temporary register
K: Secret key IV: Initial vector (S_1)



c. 错误传播

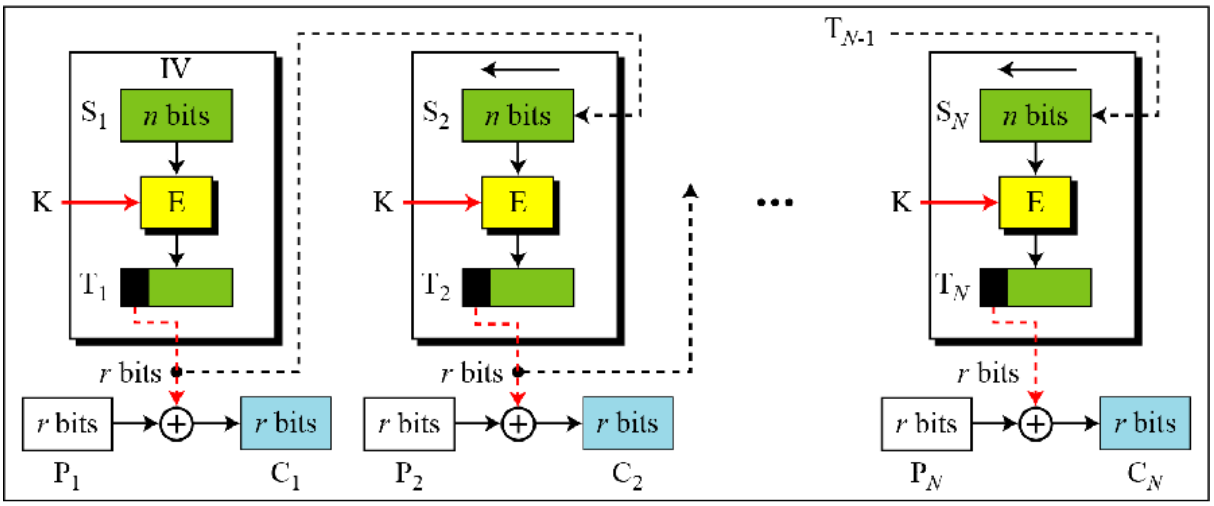
d. 能检测出篡改，还能够隐蔽明文数据图样

4. 输出反馈OFB

a. 可以进一步将DES转化为流密码

b. 加密：OFB直接将寄存器加密结构作为反馈（所以是输出反馈），而CFB是密文作为反馈（密码反馈）

E : Encryption　　D : Decryption　　S_i: Shift register
P_i: Plaintext block i　　C_i: Ciphertext block i　　T_i: Temporary register
K : Secret key　　IV: Initial vector (S_1)



Encryption

c. 克服了错误传播问题，难以检测密文篡改

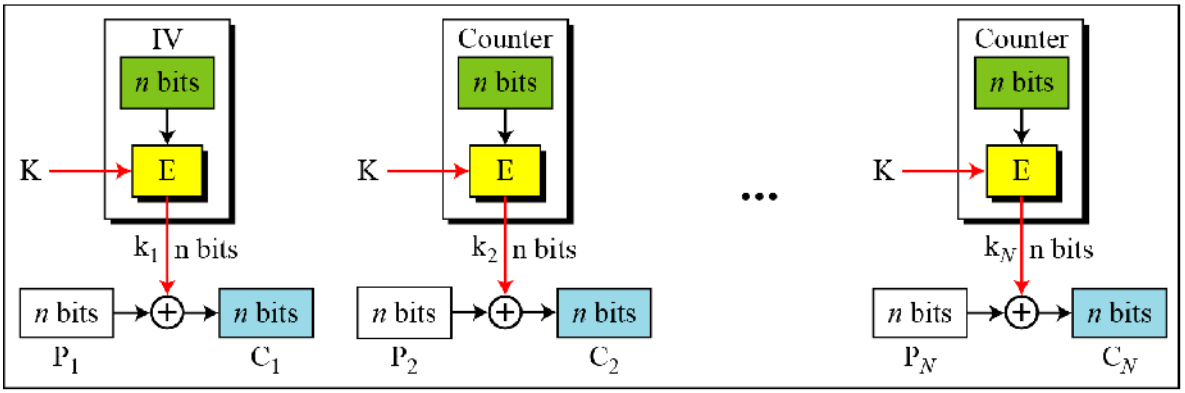
d. 不具有自同步功能，需要与系统保持严格的同步

5. 计数器CTR

a. 加密：OFB移位寄存器换成计数器

E : Encryption　　IV: Initialization vector
P_i: Plaintext block *i*　　C_i: Ciphertext block *i*
K : Secret key　　k_i : Encryption key *i*

The counter is incremented for each block.

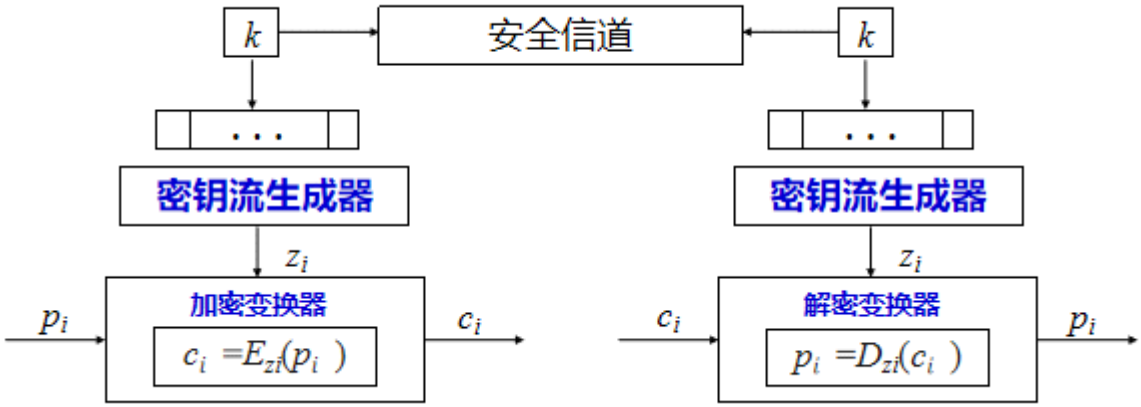


Encryption

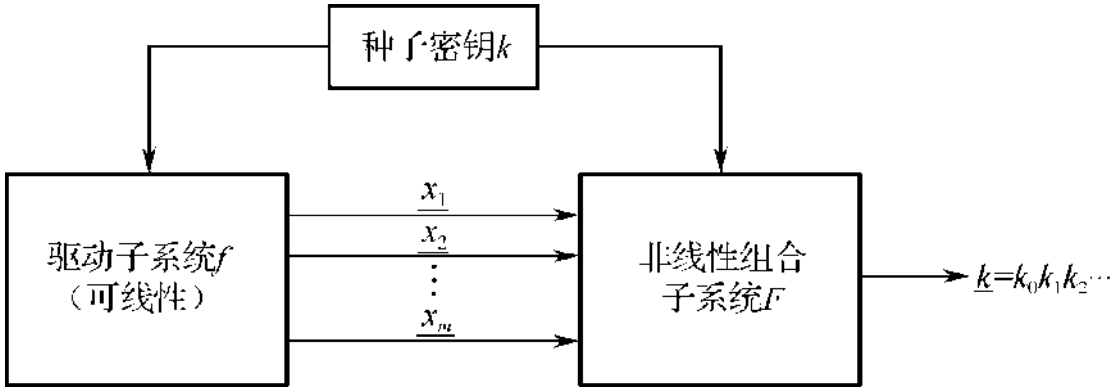
序列密码

Sunday, December 13, 2020 11:13 AM

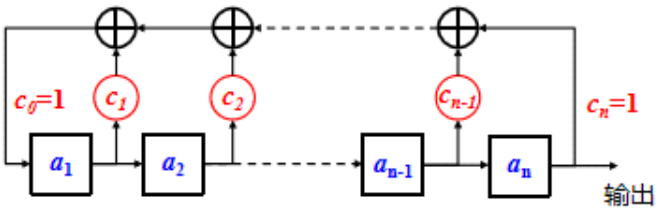
1. 概述
   a. 序列密码，也称流密码，是对称密码中的一种
   b. 序列密码的因一次一密应运而生的
   c. 思想：用短的种子密钥来获取长的密钥序列，其独立于明文消息和密文消息。
   d. 结构：



   e. 密钥流是密钥和固定大小的以往密文位的函数
2. 序列密码生成
   a. 密钥序列生成：安全性至关重要
   b. 密钥生成器一般由两部分构成：驱动子系统、非线性组合子系统

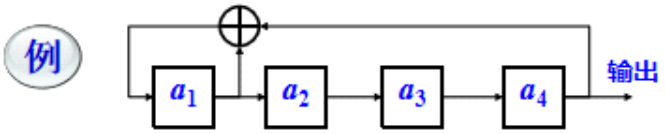


   c. 内部由有限状态自动机构成
3. 伪随机序列
   a. m序列：最大长度线性反馈移位寄存器序列的简称。k位数据最大重复周期$2^k - 1$（0不是有效数据）
   b. 线性反馈寄存器的特征多项式：以此产生m序列



$$f(x) = c_0 + c_1 x + c_2 x^2 + \ldots + c_{n-1} x^{n-1} + c_n x^n$$

注意：x^i 仅代表移位寄存器的位置，x本身的取值并无实际意义。



$f(x) = 1 + x + x^4$

$f(x) = 1 + x + x^4$

$c_0 = c_1 = c_4 = 1$

1

c. 产生m序列的充要条件：特征多项式为“本原多项式”

n	本原多项式		n	本原多项式	
	代数式	8进制表示法		代数式	8进制表示法
2	x^2+x+1	7	14	$X^{14}+x^{10}+x^6+x+1$	42103
3	x^3+x+1	13	15	$x^{15}+x+1$	100003
4	x^4+x+1	23	16	$x^{16}+x^{12}+x^3+x+1$	210013
5	x^5+x^2+1	45	17	$x^{17}+x^3+1$	400011
6	x^6+x+1	103	18	$x^{18}+x^7+1$	1000201
7	x^7+x^3+1	211	19	$x^{19}+x^5+x^2+x+1$	2000047
8	$x^8+x^4+x^3+x^2+1$	435	20	$x^{20}+x^3+1$	4000011
9	x^9+x^4+1	1021	21	$x^{21}+x^2+1$	10000005
10	$x^{10}+x^3+1$	2011	22	$x^{22}+x+1$	20000003
11	$x^{11}+x^2+1$	4005	23	$x^{23}+x^5+1$	40000041
12	$x^{12}+x^6+x^4+x+1$	10123	24	$x^{24}+x^7+x^2+x+1$	100000207
13	$x^{13}+x^4+x^3+x+1$	20033	25	$x^{25}+x^3+1$	200000011

d. 特性
   i. 均衡性
   ii. 短游程特性
   iii. 自相关特性

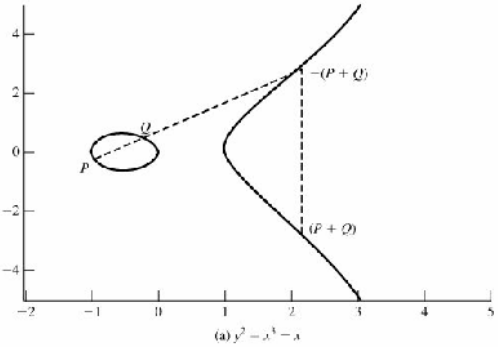
e. 应用
   i. 测试噪声源
   ii. 加密通信
   iii. 加扰以及平衡

公钥加密（RSA，DH, ElGamal 与椭圆曲线）

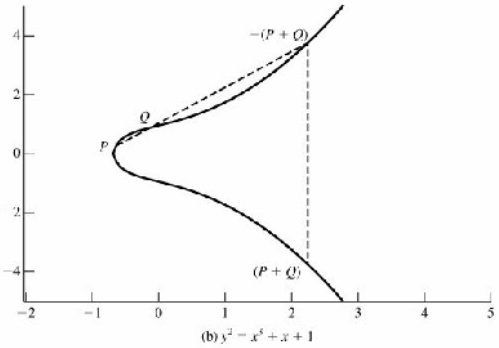
Sunday, December 13, 2020 11:15 AM

1. 公钥密码体制
    a. 非对称密码：免去密钥分发、密钥管理简单
    b. 原则
        i. 单向函数
        ii. 陷门单向函数
2. RSA
    a. 密钥生成
        i. 选择两个大素数p,q
        ii. 随机选择公钥e , sub to $1 < e < \phi(n), \gcd(e, \phi(n)) = 1$
        iii. 产生私钥d, sub to ed = 1 mod ϕ(n)
    b. 加密:$C = m^e \bmod n \ (m < n)$
    c. 解密:$m = C^d \bmod n \ (C < n)$
3. RSA安全性
    a. 共模攻击
    b. 低指数攻击
    c. CCA选择密文攻击（因为RSA是确定性加密算法）
4. DH密钥交换协议
    a. 目的：双方在网络中交换信息以生成双方共享的会话密钥
    b. 原理
        i. 本原根g，双方密钥x,y
        ii. 公开交换g^x, g^y
        iii. 公钥g^{xy}
    c. 出现中间人攻击问题
5. ElGamal加密
    a. 密钥生成
        i. 选择大素数p，本原根e_1，选择整数d
        ii. 生成$e_2 = e_1^d \bmod p$
        iii. e_2, e_1, p作为公钥，d作为私钥
    b. 公钥加密：
        i. $C_1 = e_1^r \bmod p$
        ii. $C_2 = (e_2^r * P) \bmod p$
    c. 私钥解密
        i. $P = C_2 * (C_1^p)^{-1} \bmod p$

6. 椭圆曲线加密
   a. 椭圆曲线定义：$E(a,b): y^2 = x^3 + ax + b$



(a) $y^2 = x^3 - x$



(b) $y^2 = x^3 + x + 1$

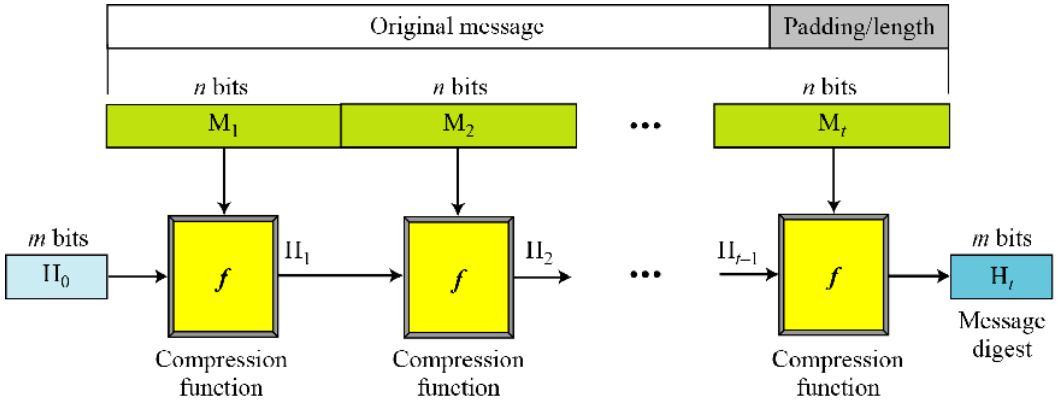
   b. 运算定义
      i. P=(x,y) -p=(x,-y)
      ii. R=P+Q
      iii. P+P=2P
      iv. P+(-P)=O
      - $P = (x_P, y_P),\ Q = (x_Q, y_Q)$
      - $R = P + Q = (x_R, y_R)$
        - $x_R = \lambda^2 + \lambda - x_P - x_Q - a$
        - $y_R = -\lambda(x_R - x_P) - x_R - y_P$

   c. 可以看到，对于P，nP非常复杂，也就是说已知nP求解出P是困难的，基于此对ElGamal做改进如下
   d. 密钥生成
      i. 选择椭圆曲线$E_p(a,b), e_1 = (x,y), d$
      ii. 生成$e_2 = de_1$
      iii. e_2,e_1作为公钥，d作为私钥
   e. 公钥加密
      i. $C_1 = re_1$
      ii. $C_2 = P + re_2$
   f. 私钥解密
      i. $P = C_2 - dC_1$

Hash, MAC, DS

Sunday, December 13, 2020 11:14 AM

1. 哈希函数应用
   a. 消息验证
   b. 完整性
   c. 口令验证
   d. MAC（与加密配合）
   e. 数字签名（与加密配合）
2. 两个简易哈希函数
   a. 全文XOR
   b. 每块异或之后左移一位
3. 哈希函数要求（哈希函数容易收到生日攻击）
   a. 不定长明文->定长哈希
   b. 单向性（抗原像攻击）
   c. 弱抗碰撞性（抗第二原像攻击）：给定原文和哈希，寻找碰撞
   d. 强抗碰撞性：任意寻找两个碰撞原文
4. 哈希函数结构
   a. Merkle-Damgard 结构



   b. 两大流派

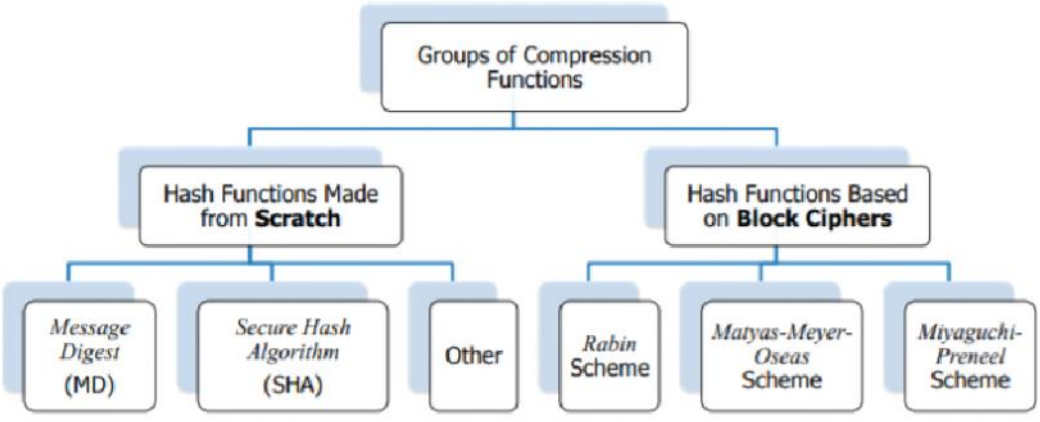


Figure12.1: Two groups of compression function in cryptographic hash function

MD2
MD4
MD5

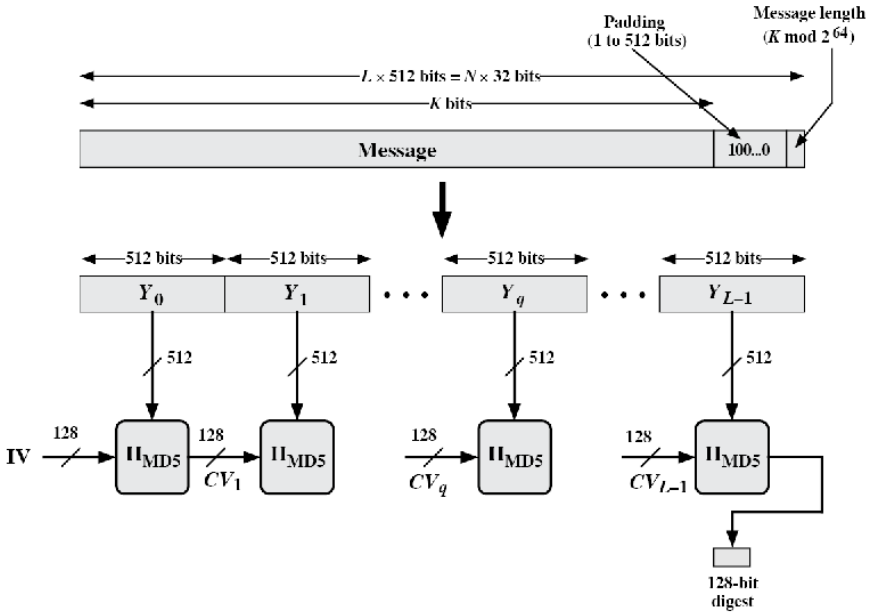
SHA-1
SHA-224
SHA-256

Whirlpool

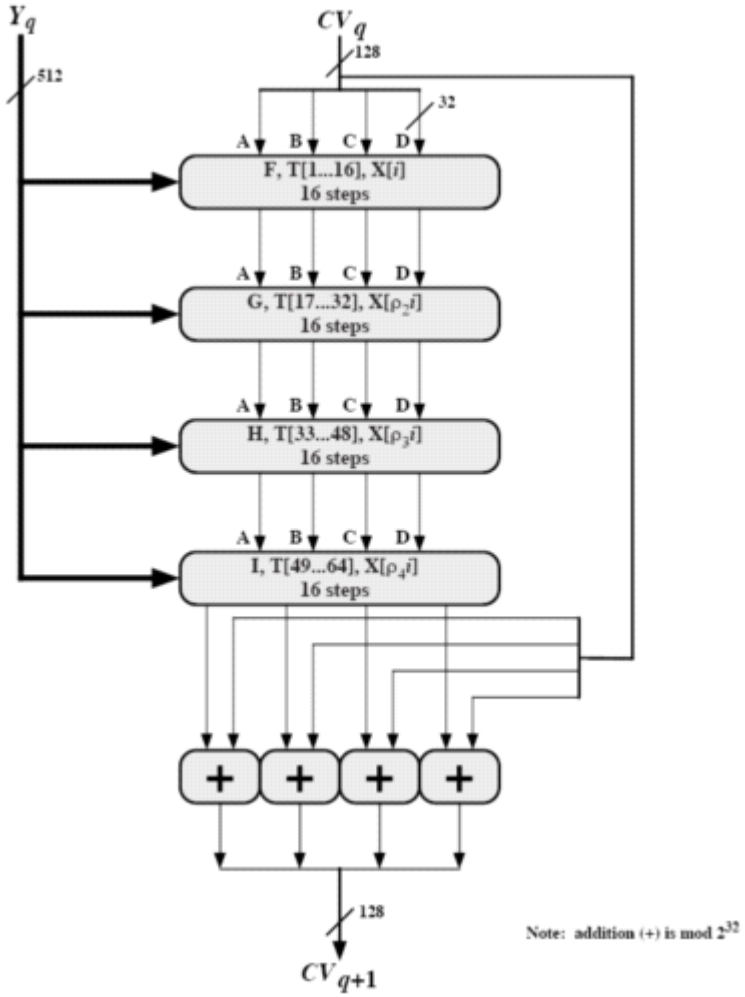
MD2 *MD4* *MD5*	*SHA-1* *SHA-224* *SHA-256* *SHA-384* *SHA-512*	*Whirlpool*

1.9

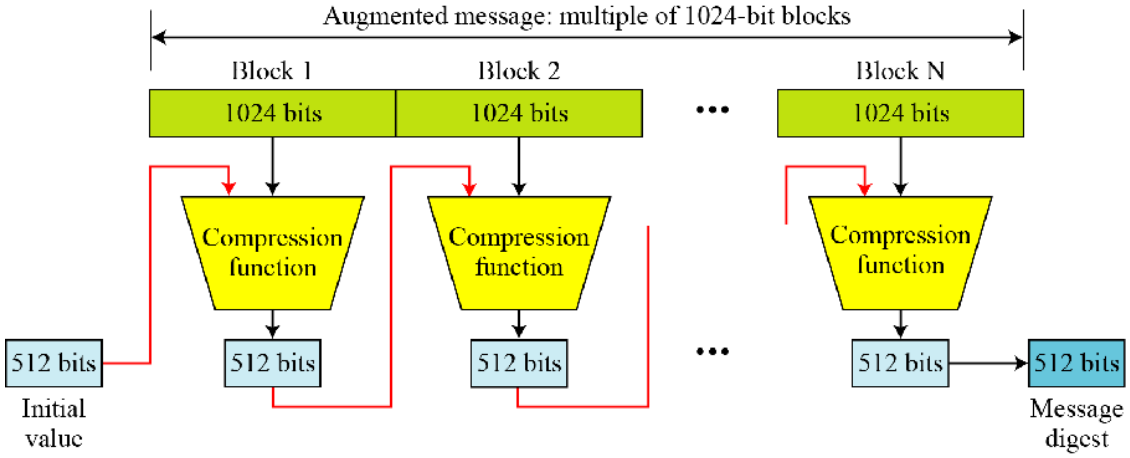
5. MD5
   a. 总结构



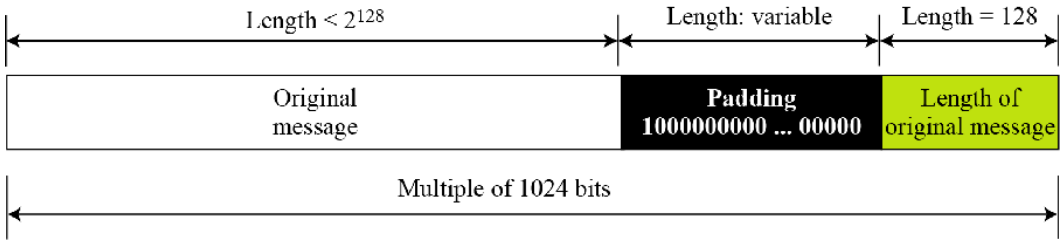
   b. MD5运算



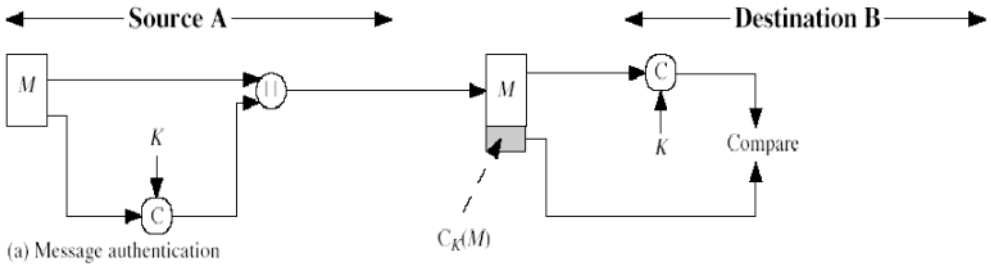
6. SHA512
   a. 总结构（与MD5基本一致）



b. 填充



7. Message Authentication Code MAC 消息验证码
   a. 目的：检测消息的改动
   b. 一种结构



   c. 本质：一种与密钥有关的哈希函数
8. Digital Signature DS 数字签名
   a. 性质
      i. 身份验证（来自公私钥加密）
      ii. 数据完整性（来自hash）
      iii. 不可否认性（来自DS）
   b. RSA签名
      i. 速度慢
      ii. 可伪造
   c. ElGamal签名
      i. 密钥生成
         1) p大素数
         2) g本原根
         3) x密钥

4) $y = g^x \bmod p$公钥

ii. 签名

1) $\text{sig}(m,k) = (r,s), k \in Z^*_{p-1}$ is random
2) $r = g^k \bmod p$
3) $s = k^{-1}(H(m) - xr) \bmod (p-1)$

iii. 验证

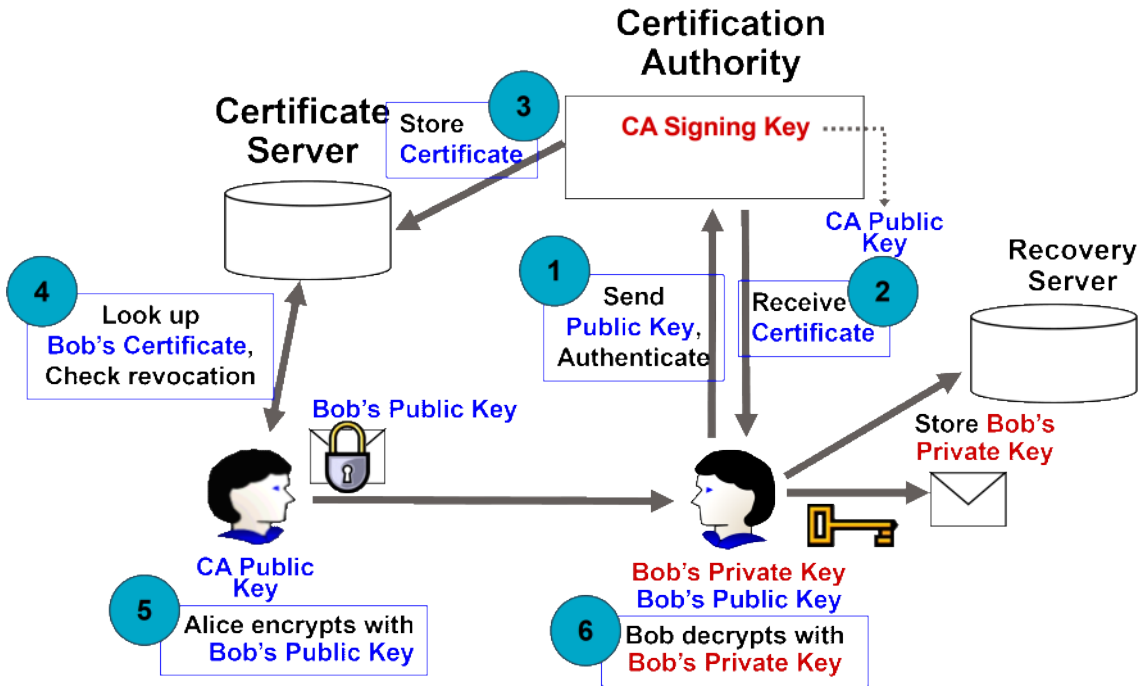
1) $y^r r^s = g^{H(m)} \bmod p$

d. Schnorr签名（略）

e. DSS（略）

9. PKI 公钥基础设施

结构如下



一些题目和参考

Monday, December 14, 2020 12:07 PM

参考网站：

- http://www.360doc.com/content/17/0618/18/41572081_664229414.shtml
- http://www.doczj.com/doc/e58056cd9e31433238689329.html
- https://wenku.baidu.com/view/fdf2e654bceb19e8b8f6baf2.html
- https://blog.csdn.net/dyw_666666/article/details/85717104

题目：

- 32、SHA-1 是数字签名标准 DSS（Digtial Signature Standard）中使用的散列算法。它所处

  理的分组长度为 512 位，输出为 160 位的散列函数值。

  33、SHA-256 所处理的分组长度为 512 位，输出为 256 位的散列函数值。

  33、SHA-384 所处理的分组长度为 1024 位，输出为 384 位的散列函数值。

  33、SHA-512 所处理的分组长度为 1024 位，输出为 512 位的散列函数值。

  7、Elgamal算法的安全性是基于（离散对数问题），它的最大特点就是在加密过程中引入了一个随机数，使得加密结果具有（不确定性），并且它的密文长度是明文长度的（两）倍。该算法的变体常用来进行数据签名。

  1、信息安全中所面临的威胁攻击是多种多样的，一般将这些攻击分为两大类（主动攻击）和被动攻击，其中被动攻击又分为（消息内容的泄露）和（进行业务流分析）。

  2、密码技术的分类有很多种，根据加密和解密所使用的密钥是否相同，可以将加密算法分为：对称密码体制和（非对称密码体制），其中对称密码体制又可分为两类，按字符逐位加密的（序列密码）和按固定数据块大小加密的（分组密码）。

  13、DES的分组长度是____64位____，密钥长度为____56位____

  14、AES的分组长度是___128位_____，密钥长度为_____128、192、256位_____

- 13．在线性反馈移位寄存器（LFSR）中，移位寄存器中存储器的个数称为移位寄存器的阶数，移位寄存器中存储的数据称为移位寄存器的状态。

- # DSA和RSA的区别

  2017-06-18 野崎君noZ... 阅 1976 转 1 分享 全屏 转藏

  DSA算法好在加/解速度快,密钥量短,采用对称加密

  RSA算法好在网络容易实现密钥管理,便进行数字签名,算法复杂,加/解速度慢,采用非对称加密