现代密码学

第一章 古典密码学

密码分析的方法：唯密文攻击，已知明文攻击，选择明文攻击，选择密文攻击，自适应选择密文攻击

古典密码的类型：代换密码和置换密码

仿射密码

维吉尼亚密码

Kasiski测试法：用于测试密钥的长度

重合指数法：使用遍历的方法，把字符串分成m份，计算每个字符串的重合指数，重合指数最接近0.065，说明此时的m就是密钥的长度，然后对每一份字符串进行穷搜索，得到那份字符串的密钥，最后得到维吉尼亚密码的密钥。

例子:

希尔密码：将n个明文字母线性变换得到加密值，解密的时候直接乘上逆矩阵就可以

希尔密码可以隐藏字符的频率信息，同时密钥空间较大，惟密文攻击相对较难。

然而，线性变换的攻击性很脆弱，可以使用已知明文破译。

- 对于一个mxm的hill密码，假定有m个明文-密文对，明文和密文的长度都是m. 可以把明文和密文对记为：
  $P_j=(p_{1j}, p_{2j}, .. p_{mj})$ 和 $C_j=(C_{1j}, C_{2j}, \ldots, C_{mj})$，
  $C_j=P_jK$, $1\le j \le m$
  定义mxm的方阵 $X=(P_{ij})$　$Y=(C_{ij})$，得到 $Y=XK$，$K=X^{-1}Y$

置换密码实质上是输入分组的一个线性变换，是一种特殊的希尔密码

分组密码：对一整个明文x，分别对其明文单位x1x2进行加密，加密的时候可能涉及前后文的信息。

流密码：产生一个密钥流z1z2...，然后使用加密规则在加密x1x2。可以理解为，加密的信息不受之前信息影响，所以可以直接加密

- 同步流密码，就是生成的密钥流独立于明文流；
- 异步流密码：密钥流不仅与密钥有关，还与明文或密文相关。

对称密码的两种基本运算：代换和置换，两个基本设计原则：扩散（明文和密文之间的统计关系尽量复杂）和混乱（密文的统计特性与密钥的取值之间的关系尽量复杂）

第二章 密码的数学基础

数论部分:

- 欧几里得算法
- 梅森素数
- 费马素数
- 剩余类和完全剩余类

- 欧拉定理和费马小定理
- 原根、缩系
- 中国剩余定理和二次剩余
- 勒让德符号、jacobi符号

近世代数部分：

- 有限域

第三章 完善保密理论

安全分类：可证明安全、计算安全、无条件安全

计算安全：如果使用最好的算法攻破一个密码体制需要至少N次操作，这里的N是一个特定的非常大的数字，我们可以定义这个密码体制是计算安全的。

没有一个已知的密码被证明计算安全

无条件安全：对攻击者的计算量没有限制。即使提供了无穷的计算资源，也是无法被攻破的。惟密文攻击下无条件安全的密码体制是存在的

完善保密的定义：

定义2.3 一个密码体制具有完善保密性，如果对于任意的$x \in \mathrm{P}$和$y \in \mathrm{C}$，都有$Pr[x|y] = Pr[x]$。也就是说，给定密文y，明文x的后验概率等于明文的先验概率。

通俗地说，完善保密性就是攻击者不能通过观察密文获得明文的任何信息。

完善保密的证明例子：

定理 2.3 假设移位密码的26个密钥都是以相同的概率1/26使用的，则对于任意的明文概率分布，移位密码具有完善保密性。

证明 这里$\mathcal{P} = \mathcal{C} = \mathcal{K} = \mathbb{Z}_{26}$，对于$0 \leqslant K \leqslant 25$，加密函数$e_K$定义为$e_K(x) = (x + K) \bmod 26$ $(x \in \mathbb{Z}_{26})$。首先计算$\mathcal{C}$上的概率分布。假设$y \in \mathbb{Z}_{26}$，则

$$\begin{aligned}\mathbf{Pr}[\mathbf{y} = y] &= \sum_{K \in \mathbb{Z}_{26}} \mathbf{Pr}[\mathbf{K} = K]\mathbf{Pr}[\mathbf{x} = d_K(y)] \\ &= \sum_{K \in \mathbb{Z}_{26}} \frac{1}{26}\mathbf{Pr}[\mathbf{x} = y - K] \\ &= \frac{1}{26}\sum_{K \in \mathbb{Z}_{26}} \mathbf{Pr}[\mathbf{x} = y - K]\end{aligned}$$

现在固定y，值$(y - K) \bmod 26$构成$\mathbb{Z}_{26}$的一个置换。因此有：

$$\sum_{K \in \mathbb{Z}_{26}} \mathbf{Pr}[\mathbf{x} = y - K] = \sum_{K \in \mathbb{Z}_{26}} \mathbf{Pr}[\mathbf{x} = x] = 1$$

得到对于任意的$y \in \mathbb{Z}_{26}$，

$$\mathbf{Pr}[y] = \frac{1}{26}$$

接下来，对于任意的 x, y，我们有：

$$\mathbf{Pr}[y \mid x] = \mathbf{Pr}[\mathbf{K} = (y - x) \bmod 26] = \frac{1}{26}$$

（这是因为对于任意的 x, y，满足 $e_K(x) = y$ 的惟一的密钥 $K = (y - x) \bmod 26$。）现在应用 Bayes 定理，很容易计算出：

$$\mathbf{Pr}[x \mid y] = \frac{\mathbf{Pr}[x]\mathbf{Pr}[y \mid x]}{\mathbf{Pr}[y]} = \frac{\mathbf{Pr}[x]\frac{1}{26}}{\frac{1}{26}} = \mathbf{Pr}[x]$$

所以这个密码体制是完善保密的。

Q：第二个计算一定要用贝叶斯公式吗?

shannon定理：

假设一个密码体制（P,C,K,E,D），满足|K|=|C|=|P|，即三者的空间是一样大的，当且仅当每个密钥被使用的概率都是1/|K|，就说明该密码体制是完善保密的。

第四章 分组密码

迭代密码:

- 密钥扩展算法将输入的一个密钥K扩展为Nr个子密钥($K^1, K^2 ... K^{Nr}$)
- 每轮使用一个子密钥进行加密
- 上一轮的输入作为下一轮的输出,也就是自身迭代

代换-置换网络（SPN）

P盒：存放置换规则

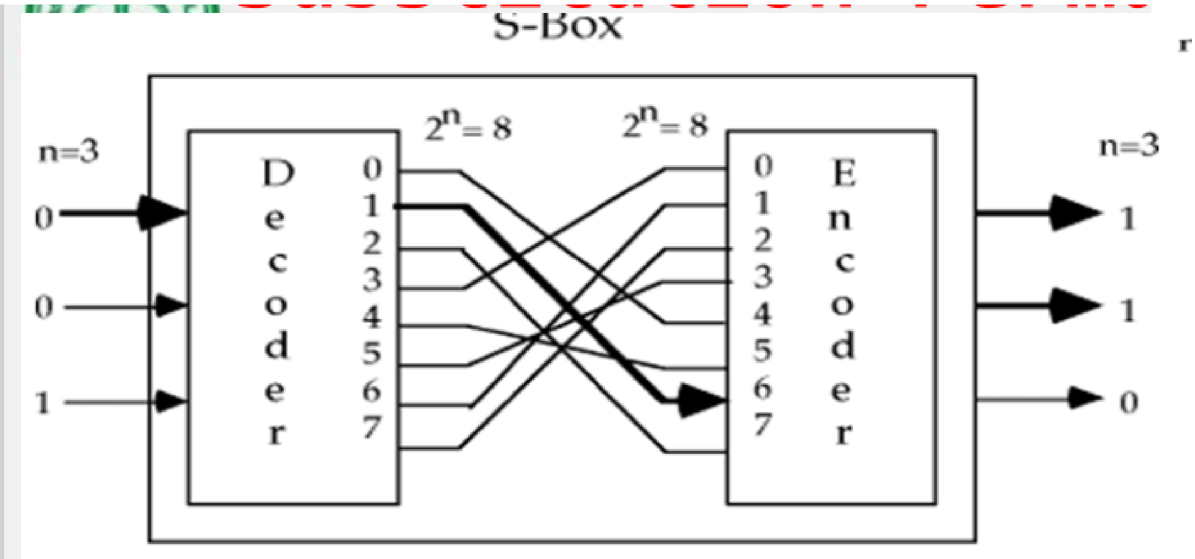
S盒：存放代换规则

在代换置换网络中，明文块和密钥块作为输入，并通过交错的若干“轮”（或“层”）代换操作和置换操作产生密文块。

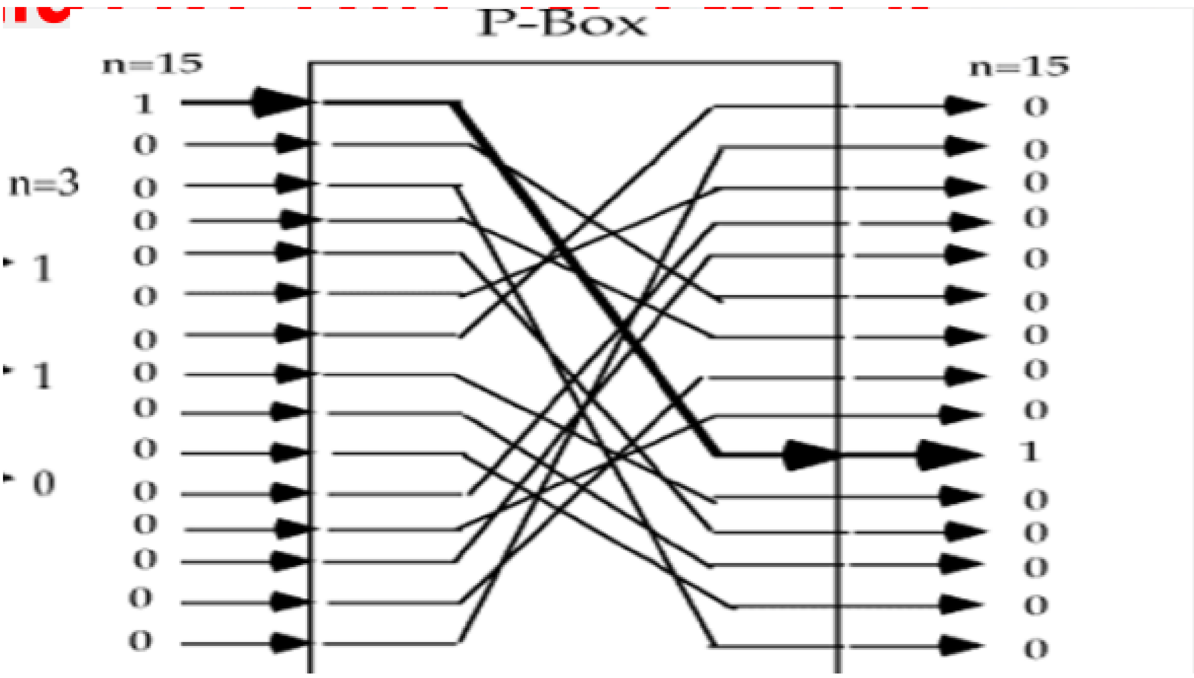
涉及到的具体名词：

白化：和子密钥异或，消除明文的统计特征（也叫轮密钥混合）

代换：将明文分成m组，明文按照一定规则进行代换，例如，长度l=4，则把5变为F（16进制，2^4次方），把1变为2...



置换：把明文分成m组，明文按照一定的规则进行代换，代换会改变数字的位置，但不会改变其他内容（例如：输入4，4位二进制下是0010，其可以置换成1000、0100、0001，但不会变为其他内容）



线性密码分析:

S盒的线性逼近

差分分析

[(IMC小记)差分密码分析与线性密码分析 - 知乎 (zhihu.com)]

第五章 DES

加密整体过程：

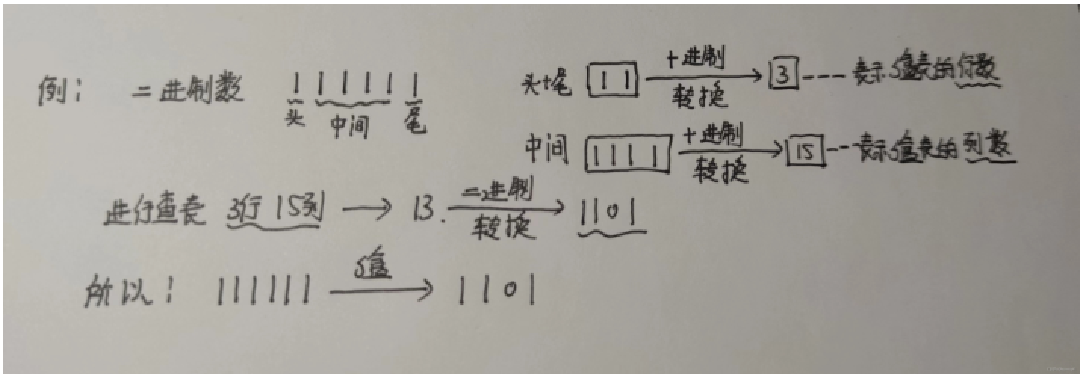
- 对64bit的明文进行置换，分成左右两个分支，左边是L0，右边R0，各32bit
- 生成L1和R1，其中L1=R0，R1=L0异或f(R0,K1)，其中f表示运算函数，K1表示第1轮的密钥
- 重复上面的过程15次，一共进行16论操作，产出R0~R16，L0~L16.
- 对R16和L16进行IP逆置换，最后得到64bit密文。

f函数包括：

- IP置换
- E扩展：将32位的R扩展为48bit，拓展运算的方法如下所示：即在每一行的左边和右边，加上对应位置的值，例如第一行左边是32，所以左边拓展为32位置的数字，右边是05，所以拓展为05位置的数字
-

32	|	01	02	03	04	|	05
04	|	05	06	07	08	|	09
08	|	09	10	11	12	|	13
12	|	13	14	15	16	|	17
16	|	17	18	19	20	|	21
20	|	21	22	23	24	|	25
24	|	25	26	27	28	|	29
28	|	29	30	31	32	|	01

- 异或：将48bit的R和48bit的K进行异或（也称密钥加密运算）
- 压缩：将得到的异或结果进行压缩，变为32bit
- （4）**S盒压缩处理：大盒子里有8块6bit 的小盒子，刚好容纳48bit的二进制数，盒子的特点是6进4出，出了盒子就变成了32bit的二进制数**，举例：



教材上的说法：右边的段要经过**选择扩展运算E 、密钥加密运算、选择压缩运算S、置换运算P和左右混合运算**

密钥形成过程：

- 密钥有64bit，去除8位校验位，剩余56位参与运算。
- 将56bit进行置换并分组，得到28bit的C和D。
- 置换规则：

- PC-1

57	49	41	33	25	17	9
1	58	50	42	34	26	18
10	2	59	51	43	35	27
19	11	3	60	52	44	36
63	55	47	39	31	23	15
7	62	54	46	38	30	22
14	6	61	53	45	37	29
21	13	5	28	20	12	4

- 对C和D进行循环左移
- 将其组成新的56bit，然后再进行置换，最后得到一轮的子密钥Ki（48位）
- 置换规则：
- PC-2

14	17	11	24	1	5
3	28	15	6	21	10
23	19	12	4	26	8
16	7	27	20	13	2
41	52	31	37	47	55
30	40	51	45	33	48
44	49	39	56	34	53
46	42	50	36	29	32

DES安全性：其密钥量为2^{56}

第六章 AES

第七章 Hash函数

哈希函数的安全性:

- 原像
- 第二原像

- 碰撞

原像:

只要找到h(x)，就可以找到x

第二原像:

问题4.2(第二原像)

实例：Hash函数$h:\mathbb{X}\to\mathbb{Y}$和$x\in\mathbb{X}$。

找出：$x'\in\mathbb{X}$使得$x\neq x'$，并且$h(x)=h(x')$。

不能解决第二原像问题的Hash函数通常称为第二原像稳固的。

碰撞:

问题4.3(碰撞)

实例：Hash函数$h:\mathbb{X}\to\mathbb{Y}$。

找出：$x,x'\in\mathbb{X}$使得$x\neq x'$，并且$h(x)=h(x')$。

不能解决碰撞问题的Hash函数通常称为碰撞稳固的。

随机喻示模型:

> **定理4.1** 假定$h\in\mathbb{F}^{\mathbb{X},\mathbb{Y}}$是随机选择的，令$\mathbb{X}_0\subseteq\mathbb{X}$。假定当且仅当$x\in\mathbb{X}_0$时，$h(x)$被确定（通过查询$h$的喻示器）。则对所有的$x\in\mathbb{X}\setminus\mathbb{X}_0$和$y\in\mathbb{Y}$，都有$Pr[h(x)=y]=1/M$。

这个定理的意思是，只有x在X_0中这个集合，或者就直接说x=x_0时，才能够确定h(x)的值，对于所有X\X_0的x，以及在Y中的y，h(x)=y的概率正好是1/M（因为只有一个x正好对应y,而X中有M个x，所以概率为1/M）

第二原像和碰撞：生日悖论

迭代哈希函数:

$(0,1)^{m+t}$变为$(0,1)^m$

预处理阶段：填充比特串

> 预处理的通常用以下方式构造串y:
>
> $$y=x||pad(x)$$
>
> 其中$pad(x)$是由填充函数对x作用后得到的。一个典型的填充函数是填入$|x|$的值，并填充一些额外的比特，使得所得到的比特串y变成t倍长。而且$x\to y$必须是1对1的，否则将不是碰撞稳固的。

哈希函数结构：MD

SHA算法：SHA1、SHA256、SHA3

第八章 RSA

公钥密码学：

解决问题：加密规则和解密规则相同导致系统的不安全。

体制：陷门单向函数（容易计算但难于求逆）

RSA的单向性：大素数分解

素性检测算法：Miller-rabin

攻击RSA方法：分解因子（Pollard ρ）

对RSA的其他攻击：

1.计算n的欧拉函数$\phi(n)$

2.计算解密指数a

3.Winenr低解密指数攻击：如果a满足3a<n^{1/4}且q<p<2q，就可以成功计算a

RSA不安全的四种情况：

- 模数n的两个素因子相差太大或太小
- 低解密指数和低加密指数
- N=pq，p-1或q-1没有大素数因子
- p-1和q-1有大公因子

模n的平方根：$y^2=a(modn)$，如果n是素数，同余方程要么0个解，要么两个解（平方剩余的定义）

假定p为一个奇素数，e为正整数，a,p互余。$y^2=a(modp^e)$在(a/p)=-1时无解，在（a/p)=1时有2解

Rabin密码体制：假设分解整数问题在计算上是不可行的，则rabin密码体制是安全的。

加密解密方案：随机选取2个大素数p、q，其满足:p=q=3 mod4

令n=q*p

加密:c=m^2 modn

解密:x^2=c mod n

解密的时候，其实就是计算一个方程组：

$$\begin{cases} \mathrm{x}^2 \equiv \mathrm{c} \mod \mathrm{p}, \\ \mathrm{x}^2 \equiv \mathrm{c} \mod \mathrm{q}, \end{cases}$$

由于p=4k+3，有一个公式可以计算

$x_1=c^{\frac{1}{4p+1}}$

$x_2=-c^{\frac{1}{4p+1}}$

由上述公式，就可以计算出2个解

第9章 DLP

离散对数问题：n阶循环群

ElGamal密码体制: