第2章 古典密码

单表密码

只使用一张密码字母表，且明文字母与密文字母有固定的对应关系————频率分析法可破

- 加法密码
- 乘法密码
  - 加密算法
    $y = (x \times k)\%n$
  - 解密算法
    $x = (y \times k^{-1})\%n$
- 仿射密码
  - 加密算法
    $y = (x \times k_1 + k_2)\%n$
  - 解密算法
    $x = ((y - k_2) \times k1^{-1})\%n$

多表密码

对每个明文字母采用不同的单表代换，即同一明文字母对应多个密文字母

- Playfair
- Vigenere
- Beaufort
- Vernam
- Hill

Enigma

Tag	Walzenlage	Ringstellung	Steckerverbindungen	Kenngruppen
date	3个齿轮编号	齿轮序号	10对接线	4对明文- 对情报根据日期进行归类

- MessageKey & Ringstellung

- MessageKey
  齿轮的**外部状态**，也即可以显示的初始状态，**随着齿轮的转动会改变**
  以明文形式随机想出3个外部状态给对方->用这个外部状态加密真正的初始状态得到初始状态的密文，发送给对方->对方解密，得到真正的初始状态
- RingSetting
  齿轮的**内部状态**，不显示在外面，**在齿轮转动时不会发生变化**

> 当按下某个键时，对该键进行加密的密钥是齿轮转了一下以后的状态
> **齿轮先旋转再加密**

- Mechanism

```
反射板 3号       2号      1号 plug board 接线板
|<————|<————|<————|<-|——input A  正向查表 输入->输出
|     |     |     |  |
|————>|————>|————>|—|——>output 亮灯 逆向查表 输出->输入
|     |     |     |  |
反射板：不会转动的齿轮 里面也有一张密码表
        输入输出可逆，输入与输出成对
        (X,Y):X->Y Y->X
```

> 加密过程经过5个元件：
> plugboard,rotor Ⅰ,rotor Ⅱ,rotor Ⅲ,refelector

$$\begin{cases} Message\ key \\ Ring\ setting \end{cases} \Rightarrow \begin{cases} \Delta = Message\ key - Ring\ setting \\ input + \Delta = real\ input \\ output - \Delta = real\ output \end{cases}$$

> 不管从左到右进入还是从右到左进入，进入一定是 $+\Delta$，出来一定是 $-\Delta$

> 加密算法与解密算法相同
> 不存在输入与输出相同的情形 因为反射板中不存在任意一对相同的输入与输出

- 五个齿轮下一个齿轮发生跳转的字母
	Ⅰ	Ⅱ	Ⅲ	Ⅳ	Ⅴ
齿轮当前位置	Q	E	V	J	Z
齿轮的下一步位置	R	F	W	K	A

> **double stepping**
> 只会出现在中间的齿轮上