古典密码学

置换密码

古典密码的一种最基本的处理技术

改变明文中各字符的相对位置

但明文字符本身的取值不变

工作原理

将明文按一定长度m进行分组，把每组的字符按位置变换规则 H 重排位置。

对应置1，2，…，m的一个置换

密钥

就是置换H，H的规则中包含了分组长度m的信息

密钥空间m!

代换

古典密码的另一种最基本的处理技术

改变明文中各字符的取值

但明文字符的出现位置不变

单表代换密码

依赖一张代换表

凯撒密码

后移三位

移位密码

- **加密**：明文字母代换为字母表中其后第k个字母
- **解密**：密文字母代换为字母表中其前第k个字母（与加密相反）

密钥k

密钥空间:26

简单代换密码

可以是字母表上的任意替换

- **密钥空间很大**

26个字母的不同排列形成不同的密钥，共有26!≈4×10^26 个

穷举攻击在计算上是不可行的，即使1微秒试一个密钥，遍历全部密钥需要10^13年

然而并没有什么卵用

被频率分析吊打

AL-Kindi

阿拉伯小故事

因此，**密文字母与对应的明文字母的出现频率完全一样。**

简一种语言书写

简单代换密码加密

参考文章

字母频率相似

明文

字母频率相似

密文

字母频率相似

英文字母出现频率差别很大

频率分布极不均匀

命名密码

真香

1587年2月8日,苏格兰女王玛丽·斯图亚特被推上断头台

同音密码

多表代换密码

维吉尼亚密码

阿尔伯

曾经被称为不可破译的密码

真香

特点

- 用给定的m个移位代换表周期性地对明文字母加密；

- 考虑下面一个维吉尼亚密码的简单例子：

明文：ueets addit ional teetq

密钥：EXTEL EXTEL EXTEL EXTEL

密文：YTKLT EIQWS WJGEA LTHLV

- 当两个相同的明文区间相隔的字母数为d或m的整数倍时，将加密相同的密文段；

距离为15，正好是m=5的整数倍

假设密文中出现两个相同的段落，则说明明文很不一定相同，但相同的可能性很大。

把消息分成 m 个字母一组,变换时,使用 26 张代换表,根据不同的密钥字母,每个明文字母采用不同的代换表进行加解密

工作原理

密钥空间与密钥长度m有关

共有26^m个密钥，即使m很小，穷举攻击也不太现实

假设m=5，密钥空间超过1.1×10^7，已超出手工计算进行穷举攻击的能力范围。

密钥空间

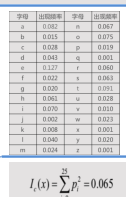
然而

19 世纪后还是被吊打了

查尔斯,巴比奇

然而,这个 b 没有开源

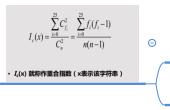
因此，这种分析方法现在被称作 **Kasiski测试法。**



字母	出现频率	字母	出现频率
a	0.082	n	0.067
b	0.015	o	0.075
c	0.028	p	0.019
d	0.043	q	0.001
e	0.127	r	0.060
f	0.022	s	0.063
g	0.020	t	0.091
h	0.061	u	0.028
i	0.070	v	0.010
j	0.002	w	0.023
k	0.008	x	0.001
l	0.040	y	0.020
m	0.024	z	0.001

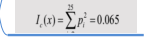
重合指数法

- $I_c(x)$ 就称作重合指数（x表示该字符串）



$$I_c(x)=\frac{\sum_{i=a}^{z} C_{n_i}^2}{C_n^2}=\frac{\sum_{i=a}^{z} f_i(f_i-1)}{n(n-1)}$$

再查表就行了



$$I_c(x)=\sum_{i=a}^{z} p_i^2=0.065$$

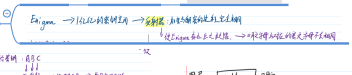
转轮机密码

Enigma,简称跑你个

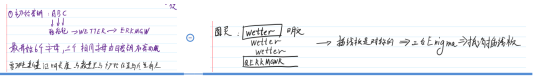
算了不考

好像有一个考点

- 反射器的作用
  - 加密与解密的过程完全相同
  - 明文字母与对应的密文字母不会相同



破解过程



课后题

1. 恺撒密码属于（ B ）

A.置换密码 B.移位密码 C.转轮机密码 D.以上都不对

2. 维吉尼亚密码属于（ D ）

A.置换密码 B.移位密码 C.转轮机密码 D.多表代换密码

3. 周期置换密码中，明文分组长度是m，密钥空间大小为 A（ ）

A. m! B. 2^m C. m D. m^2

4. 多表代换密码中，采用字母为密钥，且密钥长度是m，密钥空间大小为（ B ）

A. $(26!)^2$ B. 26^m C. m! D. m^{26}