密码学小记

工具

ctrl+点击 跳转

CyberChef

古典密码

凯撒密码

单表替代密码 ——凯撒(Caesar)密码，又叫循环移位密码。它的加密方法就是将明文中的每个字母用字母表中该字母后的第R个字母来替换，达到加密的目的。

Atbash密码

阿特巴希密码将字母表整个扭转：第一个字母与最后一个相替换，第二个与倒数第二个相替换，如此类推。

摩斯密码

摩尔斯电码只使用零和一两种状态的二进制代码，它的代码包括五种：短促的点信号“·”，保持一定时间的长信号“—”，表示点和划之间的停顿、每个词之间中等的停顿，以及句子之间长的停顿。

摩尔斯电码表

字符	电码符号	字符	电码符号	字符	电码符号
A	· —	N	— ·	1	· ————
B	— · · ·	O	———	2	· · ———
C	— · — ·	P	· ——·	3	· · · ——
D	— · ·	Q	——· —	4	· · · · —
E	·	R	· — ·	5	· · · · ·
F	· · — ·	S	· · ·	6	— · · · ·
G	——·	T	—	7	——· · ·
H	· · · ·	U	· · —	8	———· ·
I	· ·	V	· · · —	9	————·
J	· ———	W	· ———	0	—————
K	— · —	X	— · · —	?	· · ——· ·
L	· — · ·	Y	— · · ——	/	— · · — ·
M	——	Z	——· ·	( )	— · ——· —

昵享网 www.nipic.cn ID:23631609 NO:20170113094207961000

仿射密码

仿射密码是一种单表代换的**对称**密码。明文中所有字母对应成数值，经过加密函数加密成新的数值，再对应到相应的字母，组成密文， 密文和明文一样经过解密函数恢复成明文。

维吉尼亚密码

维吉尼亚密码（又译维热纳尔密码）是使用一系列凯撒密码组成密码字母表的加密算法，属于多表密码的一种简单形式。根据密钥来决定使用哪一行的密文进行替换，以此防止词频分析攻击。

将明文与密钥对齐，密钥不够就往后循环，按照图片中的规则（明文为行，密文为列）去找相对应的密文

自动密钥密码

自动密钥密码（Autokey Cipher）也是一种多表替换加密，和维吉尼亚密码类似，但使用的是不同的方法生成密钥。

自动密钥密码吗分为两种：关键词自动密钥密码和原文自动密钥密码。

秘钥=关键字+明文

取第一个明文字符作为横标，取第一个秘钥（上一步构成的秘钥）字符作为纵标，查找对应字符，在去第二个明文字符作为横标，取第二个秘钥字符作为纵标，查找对应字符，....。最后将所有字符合在一起就构成了密文

栅栏密码

栅栏密码（Rail-Fence Cipher）：栅栏密码的加密变换规则是首先将明文分成n个字符一栏，一栏为一行构成一个行列式；然后行列式行列转置后按列上下排列字符生成密文。 将n=2的栅栏密码称为2栏栅栏密码，要求明文去除空格后长度为偶数。

现代密码学

非对称加密体系

即双密钥，公钥与私钥，公钥用于加密，私钥用于解密，公钥和私钥都来自于加密算法，即使攻击者知道了公钥和加密算法，也很难从中导出私钥或者明文。

RSA算法

一种广泛使用的公钥加密算法，核心思想是利用一对密钥（公钥和私钥）进行加密和解密操作。公钥可以公开分发给任何人，用于加密信息，而私钥则必须保密，用于解密信息。这种加密方式保证了只有私钥的持有者才能解密出原始信息，从而确保了信息传输的安全性。

互质：两个正整数只有一个公因数1时，则称其为互质。

乘法逆元：

在加法中，我们有a+(−a)=0 ，我们称其互为相反数。
在乘法中，我们有a·(1/a)=1，我们称其互为倒数。
在矩阵中，我们有M*M^(-1)=E, 我们称其为逆矩阵。

生成公钥私钥

> 1.准备两个非常大的素数p 和 q（转换成二进制后 个二进制位或者更多，位数越多越难破解）；
>
> 2.利用字符串模拟计算大素数 p和q的乘积n=pq
>
> 3.同样方法m=(p-1)(q-1),m为n的欧拉函数
>
> 4.找到一个数额（1<e<m），满足gcd(m,e)=1(即e,m互素)
>
> 5.计算e在模m域上的逆元d(即满足ed mod m=1)
>
> 6.即公钥（n,e），私钥（n,d)

RSA加密

$$y = x^e \ mod \ n$$

明文x,公钥（n.e)

RSA解密

$$x = y^d \ mod \ n$$

密文y,私钥（n,d)