CTF—古典密码（凯撒密码、维吉尼亚密码、培根密码等）

CTF—古典密码（凯撒密码、维吉尼亚密码、培根密码等）

古典密码的概念：

古典密码是密码学中的其中一个类型，其大部分加密方式都是利用【替换式密码】或【移项式密码】，有时则是两者的混合。

其于历史中经常使用，但现代已经很少使用，大部分的已经不再使用了。

一般而言，经典密码是基于一个拼音字母（像是 A-Z）、动手操作或是简单的设备。它们可能是一种简单的密码法，以致于不可信赖的地步，特别是有新技术被发展出来后。

```
【经典密码】通常很容易被破解。许多经典密码可单单经由密文而破解，
所以它们容易受到唯密文攻击法攻击（cipher text only attack）。

有些 经典密码（像是【凯撒密码】）的密钥个数有限，所以这类密码可以使用暴力破解尝试所有的密钥。

【替代式密码】有比较大的密钥数，但是容易被频率分析，因为每个密码字母各代表了一个明文字母。

【多字母替代式密码】，像是维吉尼亚密码使用多个替换防止了简单的频率分析，
然而，更先进的技术卡西斯基试验就可用来破解这类密码。
```

古典密码的起源和分类

一. 古典密码

```
密码(Cryptology)是一种用来混淆的技术它希望将正常的、可识别的信息转变为无法识别的信息。
密码学是一个即古老又新兴的学科;密码学一词源自希腊文"krypto's"及"logos"两字,直译即为"隐藏"及"讯息"之意。
```

密码学是一门拥有几千年历史的学科。

```
密码学的发展大概经历了三个阶段古典密码阶段、近代密码阶段、现代密码阶段。
古典密码阶段是指从密码的产生到发展成为近代密码之间的这段时期密码的发展历史。
```

【古典密码】是密码学中的其中一个类型，其大部分加密方式都是利用 替换式密码 或 移项式密码，有时则是两者的混合。
其于历史中经常使用，但现代已经很少使用，大部分的已经不再使用了。

古典密码通常来说要对算法和密钥保密，因为很多古典密码一旦算法泄露，就不存在秘密而言了。

二. 古典密码的分类

```
古典密码大致上可以分为【替换式密码】和【移项式密码】
```

【替换式密码】：

```
【代换密码】是通过字母（或是字母群）作原系统的替换，直到消息被替换成其它难以解读的字符串
【替换式密码】分为单字母替换和多字母替换，单字母替换又可继续划分为单表替换密码和夺标替换密码。
```

【凯撒密码】是典型的单字母替换式密码，它使用一个密码字母集。

但我们也可以使用多字母替换式密码，使用多个密码字母集。加密由两组或多组密码字母集组成，加密者可自由的选择然后用交替的密码字母集加密消息。

```
这么做将会增加解码的困难度，因为密码破解者必须找出这两组或多组密码字母集。
```

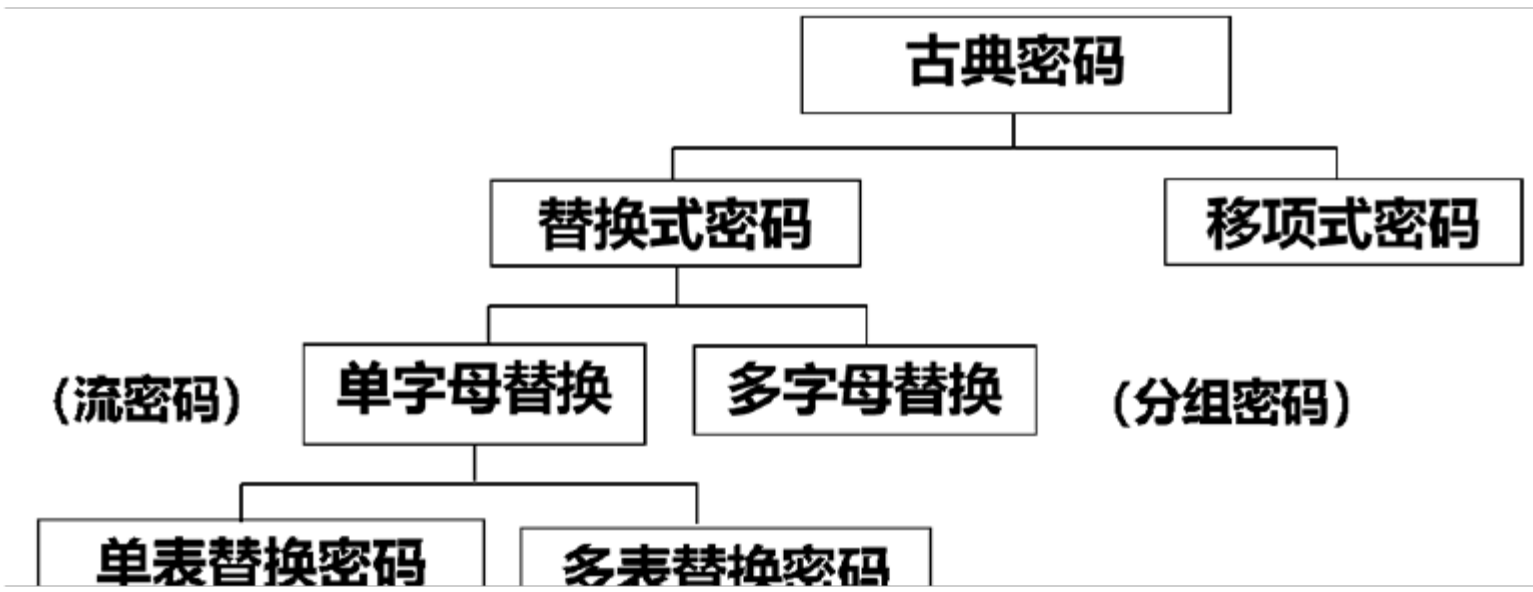
另一个著名的多字母替换式密码，称作【维吉尼亚密码】，亦作维吉尼亚方格。
这个密码更难解密，通过维吉尼亚方格，它有26组不同用来加密的密码字母集。每个密码字母集就是多移了一位的凯撒密码。

【移项式密码】

```
它们字母本身不变，但它们在消息中顺序是依照一个定义明确的加密算法改变。
```

许多移位式密码是基于几何设计的。
一个简单的加密（也易被破解），可以将字母向右移1位。
例如，明文"Hello my name isAlice.“将变成"olleH ym eman siecilA.”。

一个典型的移位式密码被称为栅栏密码，先选择一个关键字，把原来的消息由左而右、由上而下依照关键字长度转写成长方形。
接着把关键字的字母依照字母集顺序编号，例如A就是1、B就是2、C就是3等。依照编号大小调换位置，得到密文。



Kerckhoffs 原则

密码学上的【柯克霍夫原则】（Kerckhoffs’sprinciple）由奥古斯特·柯克霍夫在19世纪提出：即使密码系统的任何细节已为人悉知，只要密钥（key）未泄漏，它也应是安全的。

【Kerckhoffs准则】认为，一个密码系统的安全性不是取决于其算法对于攻击者来说是否保密，
而是建立在它所选择的密钥对于攻击者来说是否保密。

典型替换式密码的加解密原理

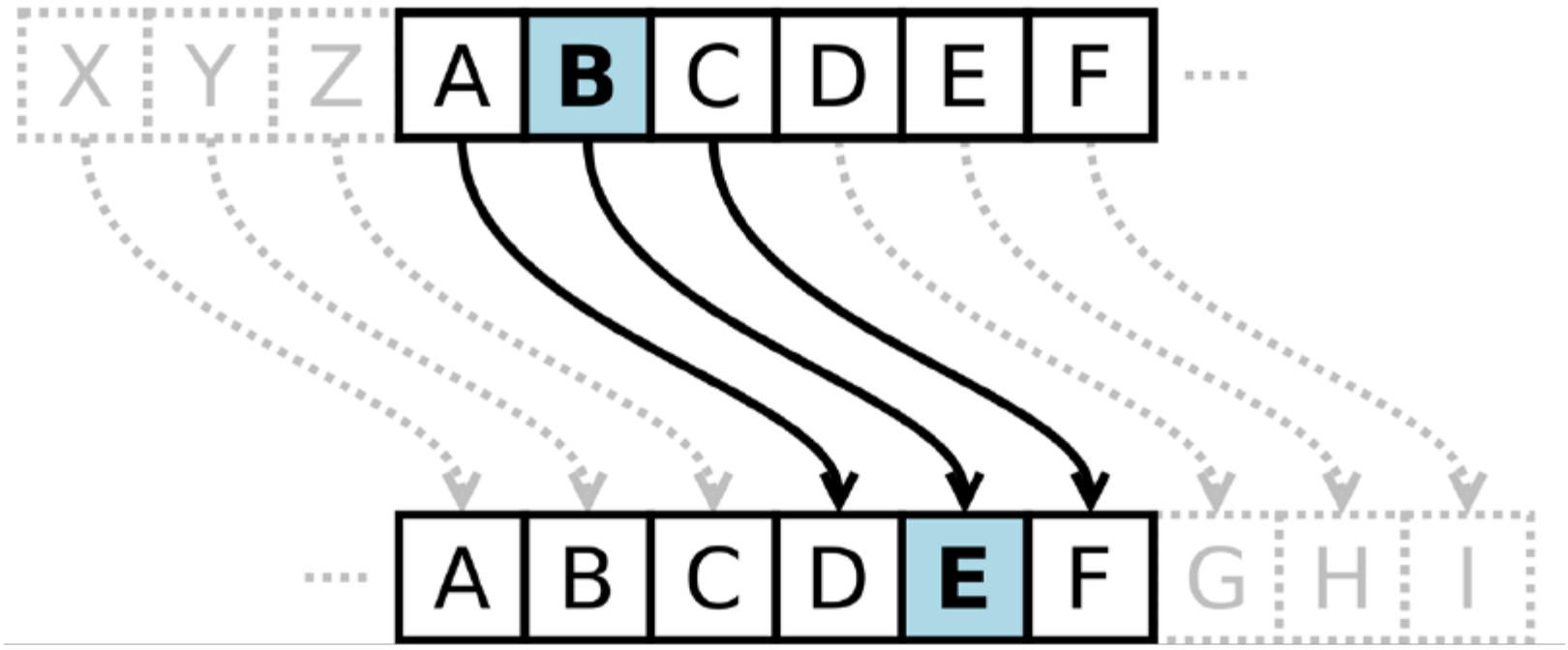
1. 凯撒密码

在密码学中，凯撒密码（英语:Caesar cipher），或称凯撒加密、凯撒变换、变换加密，是一种最简单且最广为人知的加密技术。

它是一种替换加密的技术，明文中的所有字母都在字母表上向后（或向前）按照一个固定数目进行偏移后被替换成密文。

例如，当偏移量是3的时候，所有的字母A将被替换成D，B变成E，以此类推。

这个加密方法是以罗马共和时期恺撒的名字命名的，当年恺撒曾用此方法与其将军们进行联系。



凯撒密码的替换方法

通过排列明文和密文字母表，密文字母表示通过将明文字母表向左或向右移动一个固定数目的位置。例如，当偏移量是左移3的时候（解密时的密钥就是3）：

```
明文字母表：ABCDEFGHIJKLMNOPQRSTUVWXYZ

密文字母表：DEFGHIJKLMNOPQRSTUVWXYZABC

使用时，加密者查找明文字母表中需要加密的消息中的每一个字母所在位置，并且写下密文字母表中对应的字母。
需要解密的人则根据事先已知的密钥反过来操作，得到原来的明文。例如：

明文：HEETIAN LAB

密文：KHHWLDQ ODE

凯撒密码的加密、解密方法还能够通过同余的数学方法进行计算。
```

首先将字母用数字代替，A=0，B=1，…，Z=25。此时偏移量为n的加密方法即为：

$$E_n(x) = (x + n) \bmod 26$$

解密方法为：

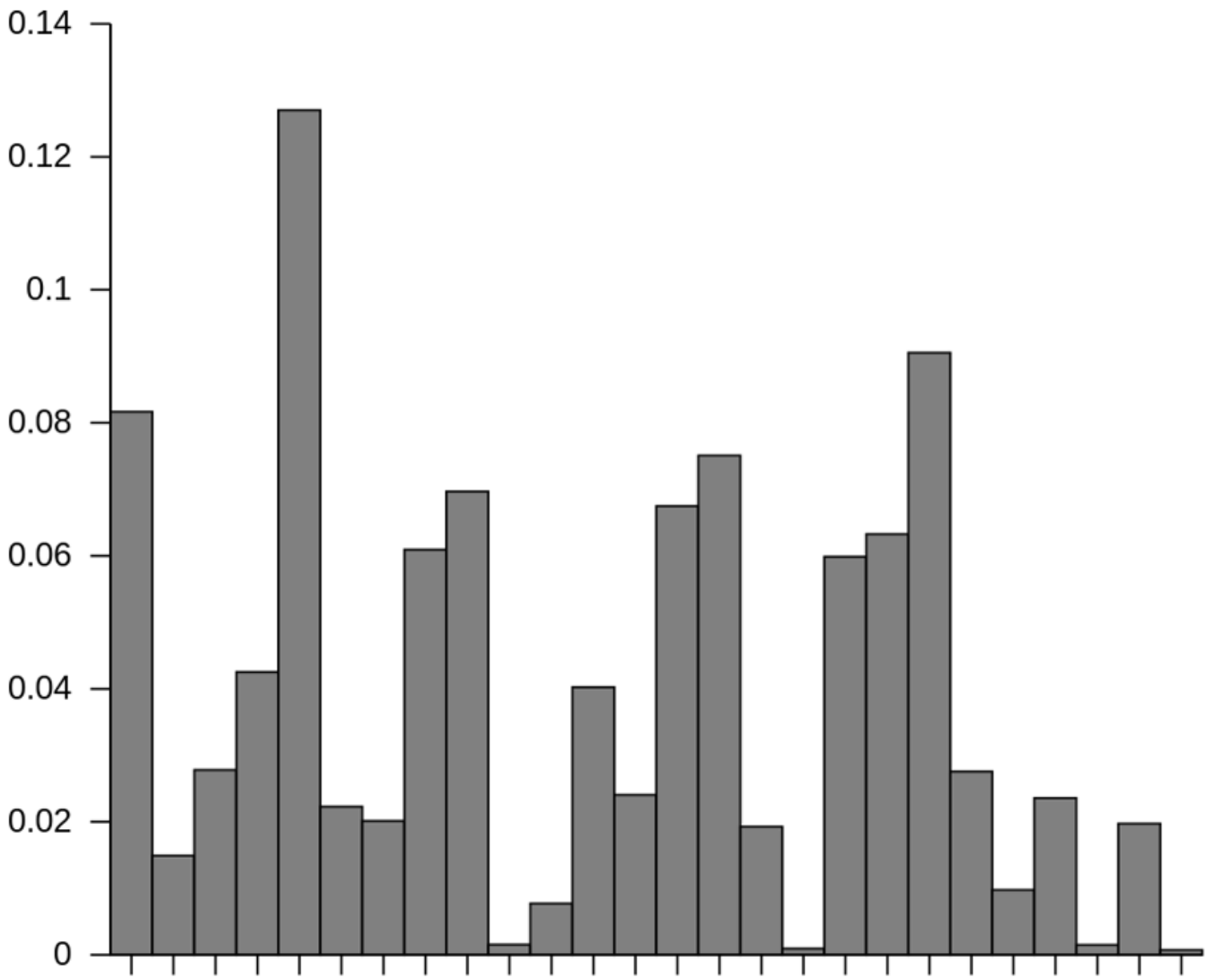
$$D_n(x) = (x - n) \bmod 26$$

2. 维吉尼亚密码

在凯撒密码中，字母表中的每一字母都会作一定的偏移。

例如当偏移量为3时，A就转换为了D、B转换为了E……因为凯撒密码中所有字母的偏移量是一样的，因此容易受到字母频率攻击分析，攻击者可以根据密文中出现字母的频率来猜测是由明文中那个字母经过偏移得到的

下图为英语语言材料中的字母频率：



而【维吉尼亚密码】则是由一些偏移量不同的恺撒密码组成。

为了生成密码，需要使用表格法。

这一表格包括了26行字母表，每一行都由前一行向左偏移一位得到。具体使用哪一行字母表进行编译是基于密钥进行的，在过程中会不断地变换。

	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z
A	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z
B	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A
C	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B
D	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C
E	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D
F	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E
G	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F
H	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G
I	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H
J	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I
K	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J
L	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K
M	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L
N	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M
O	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N
P	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O
Q	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P
R	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q
S	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R
T	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S
U	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T
V	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U
W	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V
X	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W
Y	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X

下图是用来加解密的维吉尼亚表格：

例如，假设明文为：HEETIAN

然后选择某一关键词并重复而得到密钥，如关键词为AB时，密钥为：LABLABL

对于明文的第一个字母H，对应密钥的第一个字母L，于是使用表格中L行字母表进行加密，得到密文第一个字母S。
类似地，明文第二个字母为E，在表格中使用对应的A行进行加密，得到密文第二个字母E。以此类推，可以得到：

明文：HEETIAN

密钥：LABLABL

密文：SEFEIBY

解密的过程则与加密相反。
例如：根据密钥第一个字母L所对应的L行字母表，发现密文第一个字母S位于H列，因而明文第一个字母为H。
密钥第二个字母A对应A行字母表，而密文第二个字母E位于此行E列，因而明文第二个字母为E。以此类推便可得到明文。

[redacted]

用数字0-25代替字母A-Z，维吉尼亚密码的加密文法可以写成同余的形式：
解密方法为：

[redacted]

3. 培根密码

培根密码的本质是将字母用一串二进制数替换，但是表示的过程中，没有采取0和1的形式，而使用a和b来代替。

a	AAAAA	g	AABBA	m	ABBAA	s	BAABA	y	BBAAA
b	AAAAB	h	AABBB	n	ABBAB	t	BAABB	z	BBAAB
c	AAABA	i	ABAAA	o	ABBBA	u	BABAA		
d	AAABB	j	ABAAB	p	ABBBB	v	BABAB		
e	AABAA	k	ABABA	q	BAAAA	w	BABBA		

下面是一个常用的培根密码加密表：

加密的过程首先将要加密的内容根据加密表里的内容进行替换，
如a用AAAAA替换，b用AAAAB替换。
替换完之后，我们可以把A和B当作两个不同的特征（如大写小写，正体斜体）带入到一个无关的句子中，
这就得到了我们加密后的结果。

【培根密码】本质上是将二进制信息通过样式的区别，加在了正常书写之上。
培根密码所包含的信息可以和用于承载其的文章完全无关。

例：

（1） 加密字符串heetian

（2） 根据加密表转换aabbb aabaa aabaa baabb abaaa aaaaa abbab

（3） 任选一句话，将a当作小写，b当作大写带入

it IS BacOn cipHer'S exAMpLe and now yoU KnOwit.

典型移项式密码的加解密原理

1. 栅栏密码

栅栏密码属于古典密码中最经典的移项式密码，同之前讲到的凯撒密码等替换式密码代表了密码学中最重要的两个概念（扩散和混淆）

我们以2栏栅栏密码为例来讲解它的加密和解密过程。

加密过程：

明文：THERE_IS_A_CIPHER_

两个一组，得到：(TH) (ER) (E_) (IS) (_A) (_C) (IP) (HE) (R_)

先每组中取出第一个字母：TEEI__IHR

再从每组中取出第二个字母：HR_SACPE_

连在一起得到密文：TEEI__IHRHR_SACPE_

解密过程：

而解密的时候，我们先把密文从中间分开，变为两行：

TEEI__IHR

HR_SACPE_

再按上下上下的顺序组合起来：

THERE_IS_A_CIPHER_

那么如何将2栏密码扩展到多栏呢？在之前的明文中，CIPHER这个单词之后加了一个下划线，
目的就是为了让明文字符串的长度是2的倍数，
栅栏密码的分栏的一个前提就是分的栏数需是明文长度的因数，这样才会使得分出来的每个栏长度都一样。

对于多栏，我们还是用上面的例子来讲解。

上面的明文字符串（THERE_IS_A_CIPHER_）的长度是18

所以我们可以把它分为2，3，4，6，9栏，这里我们以6栏为例。

以每个元素相隔6个字符分割出栅栏。

第一栏：TII

第二栏：HSP

第三栏：E_H

第四栏：RAE

第五栏：E_R

第六栏：_C_

连接在一起得到密文：TIIHSPE_HRAEE_R_C_

2. 周期置换密码

周期置换密码是将明文字符串P按固定的长度m进行分组，然后对每组字符串中的字符按照某个密钥重新排位得到密文C。

其中密钥S包含分组长度信息。
解密时只需得到密钥S的逆置换，把密文重新分组，按照密钥的逆置换对密文的子字符串重新排位就可以得到明文

例：

（1）明文为Heetian Cryptography Experiments

（2）密钥为S =（3 6 2 1 4 ）

（3）将明文分为五组，每组6个字符，不足6个的用双方规定的Padding进 行填充，比如空格。

p =（Heetia ）（nCrypt）（ograph）（yExper）（iments ）

（4）对每组的字符进行加密

根据密钥S，可知将第3个字符放在第6个字符的位置，第6个字符放在第2个字符的位置，
第2个字符放在第1 个字符的位置，第1个字符放在第4个字符的位置，
第4个字符放在第3 个字符的位置，置换后得到密文：

C =（eaHie ）（Ctynpr）（ghaopr）（Erpyex）（msnite ）

（5）周期置换的解密方法就是加密的逆运算，只需求出密钥的逆置换即可。可以知道密钥

S =（3 6 2 1 4 ）的逆置换1/S =（3 4 1 2 6 ）

所以只需要将密文重新分组，通过1/S 的置换顺序就可以得出明文P 。

相关推荐

- CTF必备密码编码大全
- CTF理论考核题及答案
- CTF竞赛进阶(一)密码
- [CTF]凯撒密码
- 凯撒密码-CTF(Crypto)

猜你想看

- CTF中常见密码题解密网站总
- 古典密码学算法之(一)凯撒移位(CaeserianShift)
- CTF密码学writeup传统知识+古典密码
- CTF——常见密码
- CTF常见密码及工具

相关好店

大隐隐于市blog
「其它」

文档新时代
「其它」

风住尘散了

「教育」

云梦合同

「互联网」

在行创意

「互联网」

伊呀

「互联网」

工具

收藏

领福利

下载文档