实验原理

一. Caesar(恺撒)密码

Caesar密码是传统的代替加密法，当没有发生加密（即没有发生移位）之前，其置换表如5-1-1所示。

表5-1-1 Caesar置换表

a	b	c	d	e	f	g	h	i	j	k	l	m
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
N	O	P	Q	R	S	T	U	V	W	X	Y	Z

加密时每一个字母向前推移k位，例如当k=5时，置换表如5-1-2所示。

表5-1-2 Caesar置换表

a	b	c	d	e	f	g	h	i	j	k	l	m
F	G	H	I	J	K	L	M	N	O	P	Q	R
n	o	p	q	r	s	t	u	v	w	x	y	z
S	T	U	V	W	X	Y	Z	A	B	C	D	E

于是对于明文：data security has evolved rapidly

经过加密后就可以得到密文：IFYF XJHZWNYD MFX JATQAJI WFUNIQD

若令26个字母分别对应整数 0 ～ 25，如表5-1-3所示。

表5-1-3 Caesar置换表

a	b	c	d	e	f	g	h	i	j	k	l	m
0	1	2	3	4	5	6	7	8	9	10	11	12
n	o	p	q	r	s	t	u	v	w	x	y	z
13	14	15	16	17	18	19	20	21	22	23	24	25

则Caesar加密变换实际上是：

c = (m + k) mod 26

其中m是明文对应的数据，c是与明文对应的密文数据，k是加密用的参数，也称为密钥。

很容易得到相应的Caesar解密变换是：

m = D(c) = (c - k) mod 26

例如明文：data security 对应的数据序列：

3 0 19 0 18 4 2 20 17 8 19 24

当k = 5时经过加密变换得到密文序列：

8 5 24 5 23 9 7 25 22 13 24 3

对应的密文为：

I F Y F X J H Z W N Y D