校内讲义

网络安全

实验指导书

（2023 版）

编写：张海蓉

吉林大学通信工程学院

目　　录

实验一　古典密码算法实现

一、实验目的

掌握古典密码学一般原理，理解 Shannon 扩散、混淆的密码设计思想及代换、置换方法；掌握恺撒密码、维吉尼亚密码、弗纳姆密码、置换密码等典型的古典密码原理及实现。

二、实验内容

以下 4 个实验内容任选其一：

1. 编程实现单表代换密码的代表算法恺撒密码的加密解密过程。
2. 编程实现多表代换密码的代表算法维吉尼亚密码的加密解密过程。
3. 编程实现流密码初步弗纳姆密码的加密解密过程。
4. 编程实现置换密码的加密解密过程。

三、实验原理

1. 恺撒密码

恺撒(Caesar)密码是一种替换加密技术，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，简单来讲就是把原文里的字母按照 n 个单位、特定方向去替换。

恺撒密码具体原理公式：（明文 M、密文 C、替换单位 n）

加密算法：$\mathrm{C} = (M + n)\ mod\ 26$

解密算法：$\mathrm{M} = (C - n + 26)\ mod\ 26$

2. 维吉尼亚密码

维吉尼亚(Vigenere)密码是一种简单的多表代换密码（由 26 个类似的恺撒密码的代换表组成），即由一些偏移量不同的恺撒密码组成，这些代换在一起组成了密钥。

维吉尼亚坐标图如图 1-1 所示。

维吉尼亚密码具体原理公式：（明文 M、密文 C、密钥 K）

加密算法：$\mathrm{C}_i = (M_i + K_i)\ mod\ 26$

解密算法：$M_i = (C_i - K_i + 26)\ mod\ 26$

明文

密钥

	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
Z	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	Y

图 1-1 维吉尼亚坐标图（英文中 a~z，由 0~25 表示）

3. 弗纳姆密码

弗纳姆(Vernam)密码也称一次一密(One-Time-Pad)，其加密方法是：①数据以二进制数表示时，将明文和密钥按比特异或运算；②数据以英文字母表示时，将明文和密钥模 26 加。当密钥是真随机序列、密钥长度大于等于明文长度、每一密钥只使用一次时，这种密码技术是安全的。弗纳姆密码的关键在于构造和消息等长的随机密钥，实现时在通信双方由密钥序列发生器同步产生随机密钥序列。

以二进制数表示数据时，维吉尼亚密码具体原理公式：（明文 M、密文 C、密钥 K）

加密算法：$C_i = M_i \oplus K_i$

解密算法：$M_i = C_i \oplus K_i$

4. 置换密码

在纵行换位密码中，明文以固定宽度水平地写在一张图表纸上，根据密钥进行置换后，按垂直方向读出，即为密文。解密就是密文按相同的宽度垂直的写在图表纸上，根据密钥按列置换，然后按水平方向读出，即为明文。

示例，密钥：hand，明文：meet at the schoolhouse，采用置换密码加密后的密文：etsouthhhemaeooetcls。加密过程如图 1-2 所示，解密为其逆过程。

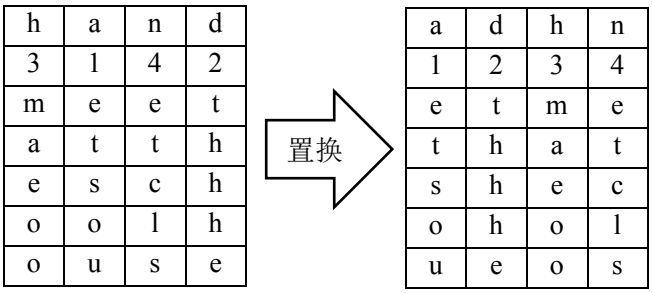

图 1-2 置换密码示例

四、实验要求

1. 程序设计语言：C 语言。

2. 完成功能：在以下四种密码算法中任选其一——恺撒密码、维吉尼亚密码、弗纳姆密码、置换密码——实现对文本/文件的加密解密过程。

五、参考学时

2 学时。

实验二　DES 单钥密码算法实现

一、实验目的

掌握单钥密码体制一般原理，重点掌握经典分组密码 DES 算法的原理及实现；理解单钥密码体制在网络安全通信中的作用。

二、实验内容

1. 编程实现 DES 算法的子密钥生成。
2. 编程实现 DES 算法的 S 盒替换。
3. 编程实现 DES 算法的 P 盒替换。

(选作)4. 编程实现 DES 算法的加密解密完整过程。

三、实验原理

DES(Data Encryption Standard)是由 BM 公司研制的一种加密算法，美国国家标准局于 1977 年公布把它作为非机要部门使用的数据加密标准，它是迄今为止在全世界范围内使用最为广泛的加密算法。

DES 是一个分组加密算法，分组长度为 64b，密钥长度也为 64b，但因为含有 8 个奇偶校验比特，所以实际密钥长度为 56b。由于计算能力的发展，DES 算法的密钥长度已经显得不够安全了，所以目前 DES 的常见应用方式是 DES EDE2，即三重 DES。

DES 算法加密流程如图 2-1 所示：

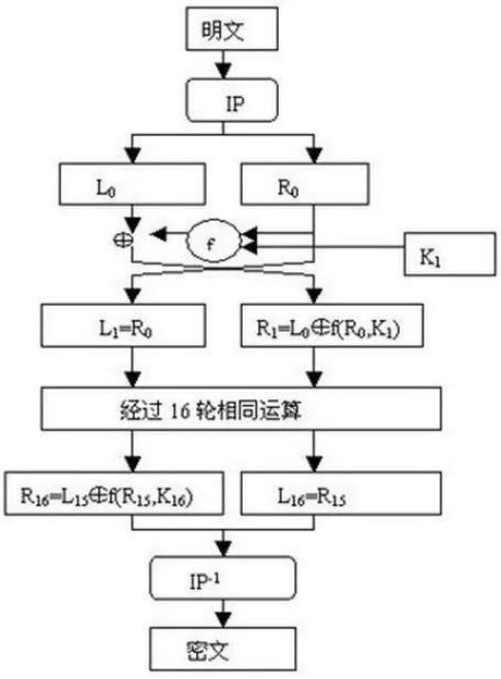

图 2-1 DES 算法加密流程

1. 子密钥生成

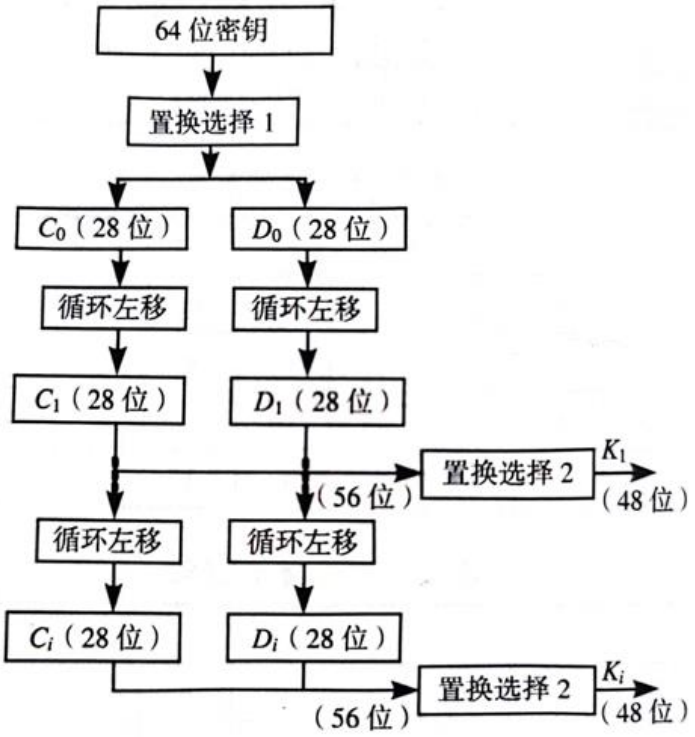

图 2-2 DES 子密钥生成流程

(1) 置换选择 1：64 位压缩为 56 位

57	49	41	33	25	17	9	1	58	50	42	34	26	18
10	2	59	51	43	35	27	19	11	3	60	52	44	36
63	55	47	39	31	23	15	7	62	54	46	38	30	22
14	6	61	53	45	37	29	21	13	5	28	20	12	4

图 2-3 压缩置换 1

(2) 循环左移：子密钥每轮左环移位数

Round	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16
Rotations	1	1	2	2	2	2	2	2	1	2	2	2	2	2	2	1

图 2-4 每轮移动的位数

(3) 置换选择 2：56 位压缩为 48 位

14	17	11	24	1	5	3	28	15	6	21	10
23	19	12	4	26	8	16	7	27	20	13	2
41	52	31	37	47	55	30	40	51	45	33	48
44	49	39	56	34	53	46	42	50	36	29	32

图 2-5 压缩置换 2

2. DES 加密

(1) 步骤一：初始置换 IP

58	50	42	34	26	18	10	2	60	52	44	36	28	20	12	4
62	54	46	38	30	22	14	6	64	56	48	40	32	24	16	8
57	49	41	33	25	17	9	1	59	51	43	35	27	19	11	3
61	53	45	37	29	21	13	5	63	55	47	39	31	23	15	7

图 2-6 初始置换表

(2) 步骤三：第 16 轮（最后一轮）变换后结果左右互换后进行末置换（初始置换的逆运算 IP^{-1}）

40	8	48	16	56	24	64	32	39	7	47	15	55	23	63	31
38	6	46	14	54	22	62	30	37	5	45	13	53	21	61	29
36	4	44	12	52	20	60	28	35	3	43	11	51	19	59	27
34	2	42	10	50	18	58	26	33	1	41	9	49	17	57	25

图 2-7 末置换表

(3) 步骤二：DES 轮变换

1) 扩展置换：32 位扩展位 48 位

32	1	2	3	4	5	4	5	6	7	8	9
8	9	10	11	12	13	12	13	14	15	16	17
16	17	18	19	20	21	20	21	22	23	24	25
24	25	26	27	28	29	28	29	30	31	32	1

图 2-8 扩展置换表

2) S 盒替换：48 位压缩替换为 32 位

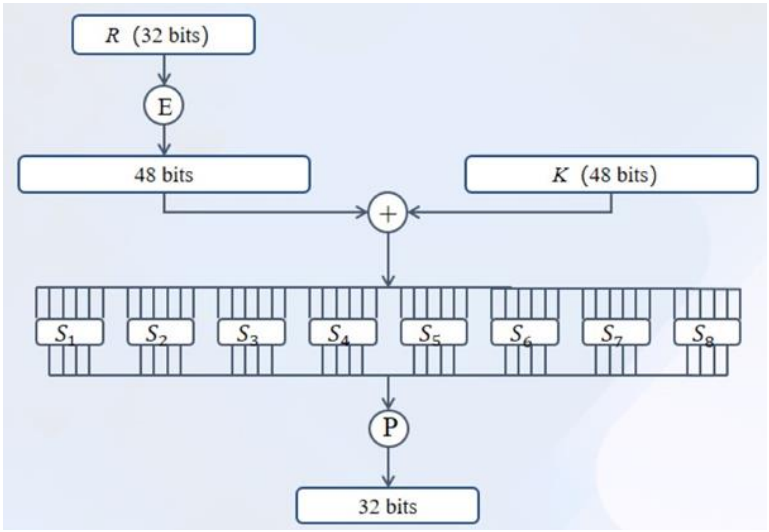

图 2-9 S 盒替换

S1															
14	4	13	1	2	15	11	8	3	10	6	12	5	9	0	7
0	15	7	4	14	2	13	1	10	6	12	11	9	5	3	8
4	1	14	8	13	6	2	11	15	12	9	7	3	10	5	0
15	12	8	2	4	9	1	7	5	11	3	14	10	0	6	13

S2															
15	1	8	14	6	11	3	4	9	7	2	13	12	0	5	10
3	13	4	7	15	2	8	14	12	0	1	10	6	9	11	5
0	14	7	11	10	4	13	1	5	8	12	6	9	3	2	15
13	8	10	1	3	15	4	2	11	6	7	12	0	5	14	9

S3															
10	0	9	14	6	3	15	5	1	13	12	7	11	4	2	8
13	7	0	9	3	4	6	10	2	8	5	14	12	11	15	1
13	6	4	9	8	15	3	0	11	1	2	12	5	10	14	7
1	10	13	0	6	9	8	7	4	15	14	3	11	5	2	12

S4															
7	13	14	3	0	6	9	10	1	2	8	5	11	12	4	15
13	8	11	5	6	15	0	3	4	7	2	12	1	10	14	9
10	6	9	0	12	11	7	13	15	1	3	14	5	2	8	4
3	15	0	6	10	1	13	8	9	4	5	11	12	7	2	14

S5															
2	12	4	1	7	10	11	6	8	5	3	15	13	0	14	9
14	11	2	12	4	7	13	1	5	0	15	10	3	9	8	6
4	2	1	11	10	13	7	8	15	9	12	5	6	3	0	14
11	8	12	7	1	14	2	13	6	15	0	9	10	4	5	3

S6															
12	1	10	15	9	2	6	8	0	13	3	4	14	7	5	11
10	15	4	2	7	12	9	5	6	1	13	14	0	11	3	8
9	14	15	5	2	8	12	3	7	0	4	10	1	13	11	6
4	3	2	12	9	5	15	10	11	14	1	7	6	0	8	13

S7															
4	11	2	14	15	0	8	13	3	12	9	7	5	10	6	1
13	0	11	7	4	9	1	10	14	3	5	12	2	15	8	6
1	4	11	13	12	3	7	14	10	15	6	8	0	5	9	2
6	11	13	8	1	4	10	7	9	5	0	15	14	2	3	12

S8															
13	2	8	4	6	15	11	1	10	9	3	14	5	0	12	7
1	15	13	8	10	3	7	4	12	5	6	11	0	14	9	2
7	11	4	1	9	12	14	2	0	6	10	13	15	3	5	8
2	1	14	7	4	10	8	13	15	12	9	0	3	5	6	11

图 2-10 8 个 S 盒(x_0x_5选择行$x_1x_2x_3x_4$选择列)

3) P 盒替换：

16	7	20	21	29	12	28	17	1	15	23	26	5	18	31	10
2	8	24	14	32	27	3	9	19	13	30	6	22	11	4	25

图 2-11 P 盒替换

3. DES 解密

解密步骤与加密步骤相同，解密时子密钥将加密子密钥逆序使用。

四、实验要求

1. 程序设计语言：C 语言。

2. 完成功能：采用 DES 单钥密码算法实现对文本/文件的加密解密过程中子密钥成成、S 盒替换、P 盒替换等关键步骤。

五、参考学时

3 学时。

实验三　RSA 双钥密码算法实现

一、实验目的

掌握公钥密码体制一般原理；掌握 RSA 算法的基本原理；了解素数判定、幂模、模逆等大数运算的算法；了解公钥加密体制的优缺点及其应用方式；理解双钥密码体制在网络安全通信中的作用。

二、实验内容

1. 编程实现 RSA 公钥密码算法密钥对生成。
2. 编程实现 RSA 公钥密码算法加密、解密过程。

三、实验原理

1978 年麻省理工学院的 Rivest, Shamir 和 Adleman 三人共同提出了 RSA 公钥密码体制的理论，RSA 是第一个既能用于数据加密也能用于数字签名的算法。它易于理解和操作，是最为流行的公钥加密算法之一。算法基于大数分解这个数论难题，即在计算上很容易求两个大素数的乘积，但是求出一个大整数的因子（将一个大整数分解成为两个素数的乘积）是很困难的。RSA 算法的一个缺陷是其运算速度要远慢于私钥密码算法，因此，RSA 很少直接用于加密数据，而是应用于数字签名、密钥分配等领域。

RSA 公钥密码算法算法描述：

密钥对生成：

I　随机生成两个不同的大素数p和q（保密）；

II　计算：$n = pq$（公开）；

III 计算n的欧拉函数$\varphi(n)$：$\varphi(n) = (p-1)(q-1)$（保密）；

IV 随机选择一个整数e（公开），使$1 < e < \varphi(n)$，且e与$\varphi(n)$互质；

V　计算e对于$\varphi(n)$的逆元d（保密），满足$ed \equiv 1 (\mathrm{mod} \varphi(n))$。

则公钥为：n、e，私钥为：d。

加密运算：$C = M^{e} \mod n$

解密运算：$M = C^{d} \mod n$

RSA 算法的具体实现过程如图 3-1 所示。

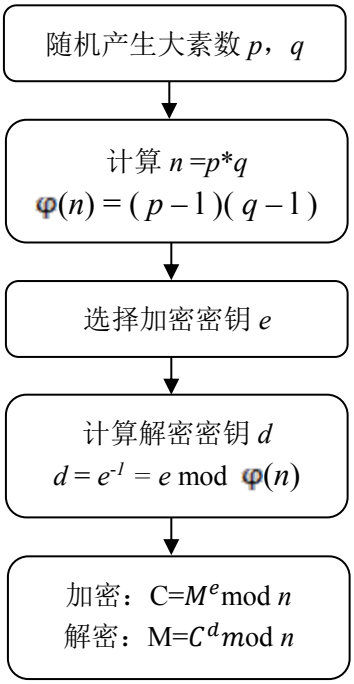

图 3-1 RSA 算法的实现过程

四、实验要求

1. 程序设计语言：C 语言。
2. 完成功能：编程实现 RSA 算法的密钥对生成、加密与解密完整过程。
3. 推荐密钥长度 1024bits，但不要求。

五、参考学时

3 学时。