d. 计算 $A=E(R_0)\oplus K_1$

$E(R_0)$：011110 100001 010101 010101 011110 100001 010101 010101

K_1：000010 110000 001001 100111 100010 110100 100110 100101

A：011100 010001 011100 110010 111000 010101 110011 110000

十六进制：711732E15CF0

e. 把 (d) 的48位结果分成6位(数据)的集合并求对应S盒代换的值

$S_1^{00}(11)=S_1^1(14)=0_{10}=0000_2=0_{16}$

$S_2^{01}(1000)=S_2^1(8)=12_{10}=1100_2=C_{16}$

$S_3^{00}(1110)=S_3^0(14)=2_{10}=0010_2=2_{16}$

$S_4^{10}(1001)=S_4^2(9)=1_{10}=0001_2=1_{16}$

$S_5^{10}(1100)=S_5^2(12)=6_{10}=0110_2=6_{16}$

$S_6^{01}(1010)=S_6^1(10)=13_{10}=1101_2=D_{16}$

$S_7^{11}(1001)=S_7^3(9)=5_{10}=0101_2=5_{16}$

$S_8^{10}(1000)=S_8^2(8)=0_{10}=0000_2=0_{16}$

f. 利用(e)的结论来求32位的结果B.

B=0000 1100 0010 0001 0110 1101 0101 0000

十六进制：0C216D50

g. 利用置换求P(B)

P(B)=1001 0010 0001 1100 0010 0000 1001 1100

十六进制：92IC209C

h. 计算 $R_1=P(B)\oplus L_0$

R_1=0101 1110 0001 1100 1110 1100 0110 0011

十六进制：5E1CEC63

1. 这个问题给出了用一轮DES加密的具体数字的例子。假设明文和密钥K有相同的位模式，即

用十六进制表示：0 1 2 3 4 5 6 7 8 9 A B C D E F

用二进制表：0000 0001 0010 0011 0100 0101 0110 0111

1000 1001 1010 1011 1100 1101 1110 1111

a. 推导出第一轮的子密钥 K_1

解：64位初始密钥经过置换选择1分为2个28位数据 C_0 和 D_0

C_0：1111 0000 1100 1100 1010 1010 0000

D_0：1010 1010 1100 1100 1111 0000 0000

循环左移1位

C_1'：1010 0001 1001 1001 0101 0100 0001

D_1'：0101 0101 1001 1001 1110 0000 0001

再经过置换选择2，得到48位密钥 K_1

K_1：0000 1011 0000 0010 0110 0111 1001 1011 0100 1001 1010 0101

用十六进制表示：0B02679B49A5

b. 推导 L_0、R_0.

对64位明文进行初始置换(IP)，前32位为 L_0，后32位为 R_0.

L_0：1100 1100 0000 0000 1100 1100 1111 1111

R_0：1111 0000 1010 1010 1111 0000 1010 1010

用十六进制表示：L_0：CC00CCFF R_0：F0AAF0AA

C. 扩展 R_0 求 $E(R_0)$

利用扩展置换E将 R_0 扩展成48位

$E(R_0)$=011110 100001 010101 010101 011110 100001 010101 010101

十六进制：7A1555 7A1555

i. 写出密文

$L_1=R_0$，连接 L_1 和 R_1 得到密文.

十六进制表示为：F0AA F0AA 5E1C EC63 $C=IP^{-1}(R_1,L_1)$

2. 用扩展欧几里得算法求下列的乘法逆元.

(a) 1234 mod 4321 (b) 24140 mod 40902 (c) 550 mod 1769

解：(a) $\gcd(1234,4321)=1$，设 $a=1234$，$b=4321$，则 $1234x+4321y=1$

a	b	x	y
1234	4321	-1082	309
4321	1234	619	-1082
1234	619	-155	309
619	615	154	-155
615	4	-1	154
4	3	1	-1
3	1	0	1
1	0	1	0

∴ $1234\times(-1082)+4321\times309=1$，$-1082+4321=3239$

∴ 1234 mod 4321 的乘法逆元为3239.

(b) $\gcd(24140,40902)=34$，∴ 24140 mod 40902 没有乘法逆元

(c) $\gcd(550,1769)=1$，设 $a=550$，$b=1769$，即 $550x+1769y=1$

a	b	x	y
550	1769	550	-171
1769	550	-171	550
550	119	37	-171
119	74	-23	37
74	45	14	-23
45	29	-9	14
29	16	5	-9
16	13	-4	5
13	3	1	-4
3	1	0	1
1	0	1	0

∴ $550\times550+(1769)\times(-171)=1$

∴ 550 mod 1769 的乘法逆元为550

3. 计算模26的逆

(a) $\begin{bmatrix}2&3\\1&22\end{bmatrix}$ (b) $\begin{bmatrix}6&24&1\\13&16&10\\20&17&15\end{bmatrix}$

解：(a) $A=\begin{bmatrix}2&3\\1&22\end{bmatrix}$

$\det(A)=\begin{vmatrix}2&3\\1&22\end{vmatrix}=44-3=41$，$41 \bmod 26=15$

$\begin{bmatrix}2&3&1&0\\1&22&0&1\end{bmatrix}=\begin{bmatrix}1&22&0&1\\2&3&1&0\end{bmatrix}=\begin{bmatrix}1&22&0&1\\0&11&1&-2\end{bmatrix}$

∴ $(11)^{-1} \bmod 26=-7$

∴ A的逆矩阵乘以-7

$= \begin{bmatrix} 1 & 22 & 0 & 1 \\ 0 & 1 & -7 & 14 \end{bmatrix} = \begin{bmatrix} 1 & 0 & 154 & -307 \\ 0 & 1 & -7 & 14 \end{bmatrix} = \begin{bmatrix} 1 & 0 & 24 & 5 \\ 0 & 1 & 19 & 14 \end{bmatrix}$

∴ A模26的逆为 $\begin{bmatrix} 24 & 5 \\ 19 & 14 \end{bmatrix}$

(b) $A = \begin{bmatrix} 6 & 24 & 1 \\ 13 & 16 & 10 \\ 20 & 17 & 15 \end{bmatrix}$

$\begin{bmatrix} 6 & 24 & 1 & 1 & 0 & 0 \\ 13 & 16 & 10 & 0 & 1 & 0 \\ 20 & 17 & 15 & 0 & 0 & 1 \end{bmatrix} \Rightarrow \begin{bmatrix} 1 & 24 & 6 & 0 & 0 & 1 \\ 10 & 16 & 13 & 0 & 1 & 0 \\ 15 & 17 & 20 & 1 & 0 & 0 \end{bmatrix}$

$\Rightarrow \begin{bmatrix} 1 & 24 & 6 & 0 & 0 & 1 \\ 0 & 10 & 5 & 0 & 1 & 16 \\ 0 & 21 & 8 & 1 & 0 & 11 \end{bmatrix} \Rightarrow \begin{bmatrix} 1 & 6 & 24 & 0 & 1 & 0 \\ 0 & 5 & 10 & 0 & 16 & 1 \\ 0 & 8 & 21 & 1 & 11 & 0 \end{bmatrix}$ ∵ $(5)^{-1} \bmod 26 = -5$

$\therefore \Rightarrow \begin{bmatrix} 1 & 6 & 24 & 0 & 1 & 0 \\ 0 & 1 & 2 & 0 & 24 & 21 \\ 0 & 0 & 5 & 1 & 1 & 14 \end{bmatrix} \Rightarrow \begin{bmatrix} 1 & 6 & 24 & 0 & 1 & 0 \\ 0 & 1 & 2 & 0 & 24 & 21 \\ 0 & 0 & 1 & 21 & 21 & 8 \end{bmatrix}$

$\Rightarrow \begin{bmatrix} 1 & 6 & 0 & 16 & 17 & 16 \\ 0 & 1 & 0 & 10 & 8 & 5 \\ 0 & 0 & 1 & 21 & 21 & 8 \end{bmatrix} \Rightarrow \begin{bmatrix} 1 & 0 & 0 & 8 & 21 & 12 \\ 0 & 1 & 0 & 10 & 8 & 5 \\ 0 & 0 & 1 & 21 & 21 & 8 \end{bmatrix}$

∴ A模26的逆为 $\begin{bmatrix} 8 & 21 & 12 \\ 10 & 8 & 5 \\ 21 & 21 & 8 \end{bmatrix}$

4. 若明文{0001 0203 0405 0607 0809 0A0B0 C0D0 E0F}，密钥是{0101 0101 0101 0101 0101 0101 0101 0101}

(a) 用4X4矩阵来描述状态的最初内容。

(b) 给出第一轮代替后状态的值。

(c) 给出第一轮代替后状态的值。

(d) 给出行移位后状态的值。

解：(a) 00 04 08 0C
01 05 09 0D
02 06 0A 0E
03 07 0B 0F

(b) 01 05 09 0D
00 04 08 0C
03 07 0B 0F
02 06 0A 0E

(c) 7C 6B 01 07
63 F2 30 FE
7B C5 2B 76
77 6F 67 AB

(d)

				循环左移
7C	6B	01	07	0位
F2	30	FE	63	1位
2B	76	7B	C5	2
AB	77	6F	67	3

90

1. 用RSA算法对下列数据实现加密和解密。

(a) $p=3$ $q=11$ $e=7$ $M=5$

(b) $p=5$ $q=11$ $e=3$ $M=9$

(c) $p=7$ $q=11$ $e=17$ $M=8$

(d) $p=11$ $q=13$ $e=11$ $M=7$

(e) $p=17$ $q=31$ $e=7$ $M=2$

解：(1) $n=pq=3\times11=33$，$\varphi(n)=\varphi(3)\varphi(11)=2\times10=20$

$ed\equiv1 \pmod{20}$，$d=3$，公钥对(33, 7)，私钥对(33, 3)

加密：$5^7\equiv c \pmod{33}$，$c=14$

解密：$14^3\equiv m \pmod{33}$，$m=5$

(2) $n=pq=55$，$\varphi(n)=\varphi(5)\varphi(11)=4\times10=40$

$ed\equiv1 \pmod{40}$，$d=27$，公钥对(55, 3)，私钥对(55, 27)

加密：$9^3\equiv c \pmod{55}$，$c=14$

解密：$14^{27}\equiv m \pmod{55}$，$m=9$

(3) $n=pq=77$，$\varphi(n)=\varphi(7)\varphi(11)=6\times10=60$

$ed\equiv1 \pmod{60}$，$d=53$，公钥对(77, 17)，私钥对(77, 53)

加密：$8^{17}\equiv c \pmod{77}$，$c=57$

解密：$57^{53}\equiv m \pmod{77}$，$m=8$

(4) $n=pq=143$，$\varphi(n)=\varphi(11)\varphi(13)=10\times12=120$

$ed\equiv1 \pmod{120}$，$d=11$，公钥对(143, 11)，私钥对(143, 11)

加密：$7^{11}\equiv c \pmod{143}$，$c=106$

解密：$106^{11}\equiv m \pmod{143}$，$m=7$

(5) $n=pq=527$，$\varphi(n)=\varphi(17)\varphi(31)=16\times30=480$

$ed\equiv1 \pmod{480}$，$d=343$，公钥对(527, 7)，私钥对(527, 343)

加密：$2^7\equiv c \pmod{480}$，$c=128$

解密：$128^{343}\equiv m \pmod{480}$，$m=2$

2. 在使用RSA的公钥体制中，已截获发给某用户的密文 $C=10$，该用户的公钥 $e=5$，$n=35$，那么明文 M 是多少？

解：$M^5\equiv10 \pmod{35}$

∵ $n=p\times q$，p、q 为质数

∴ p、q 分别为5和7

∴ $\varphi(n)=\varphi(5)\varphi(7)=4\times6=24$

∵ $ed\equiv1 \pmod{24}$，∴ $d=5$

∴ $C^5\equiv m \pmod{35}$ 即 $10^5\equiv m \pmod{35}$

∴ $m=5$

3. 在RSA体制中，某给定用户的公钥 $e=31$，$n=3599$，那么该用户的私钥等于多少？

解：∵ $n=3599=59\times61$

∴ $\varphi(n)=\varphi(59)\varphi(61)=58\times60=3480$

∵ $31\times d\equiv1 \pmod{3480}$

∴ $d=3031$

∴ 私钥等于3031

4. 用户A和B使用Diffie-Hellman密钥交换技术来交换密钥，设公用素数 $q=71$，本原根 $\alpha=7$，

(a) 若用户A的私钥 $X_A=5$，则A的公钥 Y_A 为多少？

(b) 若用户B的私钥 $X_B=12$，则B的公钥 Y_B 为多少？

(c) 共享的密钥为多少？

解：(a) $7^5 \bmod 71=51$，∴ $Y_A=51$

(b) $7^{12} \bmod 71=4$，∴ $Y_B=4$

(c) 共享密钥 $K=Y_B^{X_A}=4^5=Y_A^{X_B}=51^{12} \bmod 71=30$

5. 设Diffie-Hellman方法中，公用素数 $q=11$，本原根 $\alpha=2$

(a) 若用户A的公钥 $Y_A=9$，则A的私钥 X_A 为多少？

(b) 若用户B的公钥 $Y_B=3$，则A共享的密钥 K 为多少？

解：(a) $2^{X_A} \bmod 11=9$

∴ $X_A=6$

(b) $K=Y_B^{X_A} \bmod 11=3^6 \bmod 11=3$

100