信息安全作业 1

190110429-何为

1. 密码体制五要素是什么？

答:

明文空间 M：可能明文的有限集;

密文空间 C：是可能密文的有限集;

密钥空间 K：是一切可能密钥构成的有限集;

加密算法 E：对于任一密钥，都能够有效地计算;

解密算法 D：对于任一密钥，都能够有效地计算。

2. 俄语共有 32 个字母，设计一个乘数密码来加密俄语信息，并计算一下潜在的加密密钥有多少个，并列举。

答:

要满足$\gcd(k,32)=1$ 且 $0<k<32$ 的条件，枚举出潜在的密钥 k 的可能取值有：3、5、7、9、11、13、15、17、19、21、23、25、27、29、31 共 15 个。

3. 乘数密码中，当 gcd(k, q)=1 时，加密变换才是一一映射的。试证明之。

答:

设加密后的密文为c，明文为m，则满足$c=E_k(m)=(k\cdot m)\ mod\ q$。

于是

$$(k\cdot m-c)\ mod\ q=0$$
$$k\cdot m-c=q\cdot p$$
$$k\cdot m-q\cdot p=c$$

反证：若$n=\gcd(k,q)>1$，即 k, q 两数不互质，有最大公因数n，那么有$k=k'n,\ q=q'n$。

则上式两边同除n得:

$$k'm+q'p=\frac{c}{n}$$

其中左式必为整数，但右式当$c=1$时，不为整数。即密文c在加密变换中无原像，不符合一一映射。故乘数密码中，当 gcd(k, q)=1 时，加密变换才是一一映射的。

4. 乘数密码中，如何计算 k^{-1}？此处 k^{-1} 为 k 在模 q 下的乘法逆元？请给出算法伪代码。

答:

若$k\cdot k^{-1}\equiv 1(\mathrm{mod}\ q)$，且$k$与$q$互质，我们称$k^{-1}$为$k$的逆元。此时可以利用扩展欧几里得算法求解线性同余方程$a\cdot x\equiv c\ (mod\ b)$中$c=1$的情况，转化为求$a\cdot x+b\cdot y=1$这个方程。

首先求解一般情况:

$$
\begin{aligned}
ax+by &= \gcd(a,b) \\
&= \gcd(b, a \bmod b) \\
&\Rightarrow bx+(a \bmod b)y \\
&= bx+\left(a-\left\lfloor \frac{a}{b} \right\rfloor b\right)y \\
&= ay+b\left(x-\left\lfloor \frac{a}{b} \right\rfloor y\right)
\end{aligned}
$$

不难发现此时x变成了y，y变成了$x-\left\lfloor \frac{a}{b} \right\rfloor y$，利用这个性质，可以递归地求解$x$和$y$。当

互质时，边界条件当$b=0$时，$a=1, ax+by=1$即$x=1, y=0$。于是可以得到代码如下:

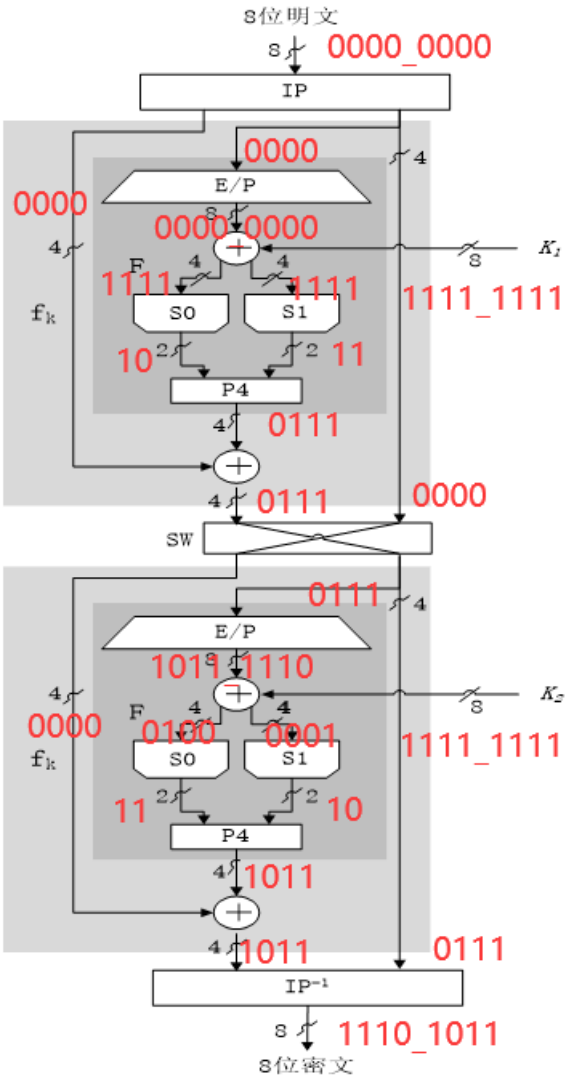
```
void Exgcd(ll a, ll b, ll &x, ll &y) {
    if (!b) x = 1, y = 0; //边界条件

    else Exgcd(b, a % b, y, x), y -= a / b * x; //递归
}

int main() {
    longlong x, y;
    Exgcd (a, p, x, y);
    x = (x % p + p) % p; //负数补成正数
    printf ("%lld\n", x);
}
```

5. 给定密钥“11 1111 1111”，明文“00000000”，计算 S-DES 的密文。请按给出主要计算过程。

答:

第一步，求子密钥：原密钥全为 1，经过置换和移位后也都为 1，所以两个子密钥 $K_1=K_2=(1,1,1,1,1,1,1,1)$。

第二步，加密变换:



S-DES的加密过程

所以最后的密文为 1110_1011。