No.

Date / /

密码.

作业2.

1. 复杂度：最好情况 $O(n)$. 最坏：$(n-1)+(n-2)+\cdots+1=\frac{n^2-n}{2}\Rightarrow O(n^2)$.

平均：$O(n^2)$.

显然是多项式时间复杂度.

2. m= 00111000 11010101 01110000 01000010 1101 0101 0011 1001 1001 0101 0111 0011.

K= 10101011 0011 0100 1000 0110 1001 0100 1101 1001 0111 1001 1100 1010 0010 1101 0011.

①密钥编排生成时，

~~a. PC1置换后得去除校验位得~~

~~10101010 0111010 1000011 1001010 1101 0000 1110 0101 0100 1111~~

a. PC1置换得

C_0: 1101 1101 1011 0000 0110 0011 1011

D_0: 1110 0101 0000 1110 0001 0001 1010.

b. 左移后得 1011 1011 0110 0000 1100 0111 0111 1100 1010 0001 1100 0010 0011 0101

c. PC2置换得知 0111 1111 0001 1001 1101 1000 1100 1011 1010 0001 0001 0010

②对m进行IP置换得 IP(m)=L0R0

= 1001 1010 0111 0111 1101 0010 1111 0010

1101 0110 1010 0101 0010 0101 1000 1000.

No.

Date / /

③ 迭代：$L_1 = R_0 =$ 1101 0110 1010 0101 0010 0101 1000 1000.

$R_1 = L_0 \oplus f(R_0, K_1)$.

a. E扩展：$E(R_0) =$ 0110 1010 1101 0101 0000 1010 1001 0000 1011 1100 0101 0001

b. 密钥加：$E(R_0) \oplus K_1 =$ 0001 0101 1100 1100 1101 0010 0101 1011 0001 1101 0100 0011

c. S盒代换得 0111 0101 1111 0010 1111 1011 0000 1111

d. P置换得 0011 1101 0110 0111 1110 1011 1011 0110

☆ 最终得 $R_1 =$ 1010 0111 0001 0000 0011 1001 0100 0100.

3. a) 删除E扩展：改变 R_0 1 bit 后，输出不变，极大影响扩散效果，急剧输出差异极小(1 bit)，因此E扩展帮助提升扩散效果.

b) 删除 S-box：使得唯一非线性变化变为线性，从而导致混淆效果大大降低，更容易被分析破解，同时也影响扩散性.

c) 删除P置换：S-box影响局限于固定部分，扩散效果减弱，密文局部依赖性增强.

4. (1) $C = E_{K_1}(E_{K_2}(E_{K_3}(m)))$；穷搜空间：$2^{168}$.

中间相遇攻击：穷举 K_1, K_2，等加密结果与(之前存储) K_3 解密进行碰撞.

时间复杂度为 $2^{112} + 2^{56}$，

空间 ~ 为 2^{112} (存加密结果)

显然 $2^{112} + 2^{56} \ll 2^{168}$.

有效降低复杂度.

No.

Date / /

(2) $C = E_{k_1}(D_{k_2}(E_{k_3}(m)))$. 搜索：$2^{112}$.

└ 中间相遇攻击：穷举 k_1 存加密结果和解密结果（~~$E_{k_1}(m)$ 与 $D_{k_2}(c)$~~）.

再穷举 (k_2, k_3) 碰撞.

时间复杂度 $2^{112} + 2^{56} \approx 2^{112}$

空间复杂度 $2^{56} \ll 2^{112}$.

对比可知，中间相遇攻击对 $C = E_{k_1}(E_{k_2}(E_{k_3}(m)))$ 更有效.