《密码学原理》作业 2 答案

1. 敌方可以向 MAC Oracle 提交一个查询 m，从而得到相应的(t_0, t_l)。显然有 $Vrfy_k$(m, t_0, t_l)=1。然后，任意选择一个 m_1’≠m_1，并且选择 t_0’使得 t_0’ ⊕ m_1’ = t_0⊕m_1 。而 m_2’,m_3’,……,m_l’都分别与 m_2,m_3,……,m_l相同，t_l’=t_l。因此，m’≠m 但 $Vrfy_k$(m’, t_0’, t_l’)= $Vrfy_k$(m, t_0, t_l)=1。
2. 对于第 i 轮，我们有 L_i=R_{i-1}， R_i=L_{i-1} 。 因此，当 r 为奇数时，L_r=R_0， R_r=L_0 ；当 r 为偶数时，L_r=L_0， R_r=R_0 。
3. 对于第 i 轮，我们有 L_i=R_{i-1}， R_i=L_{i-1}⊕R_{i-1} 。所以，L_{i+1}=R_i = L_{i-1}⊕R_{i-1}， R_{i+1}=L_i⊕R_i= R_{i-1} ⊕L_{i-1}⊕R_{i-1}= L_{i-1} 。进一步，我们得到 L_{i+2}=R_{i+1} = L_{i-1}，R_{i+2}=L_{i+1}⊕R_{i+1}= L_{i-1}⊕R_{i-1}⊕L_{i-1}= R_{i-1} 。所以，该网络每 3 轮循环一次。当 r 是 3 的倍数时，输出就等于输入。
4. 助教准备一个密钥和一个 plain.txt 文件，抽查若干名同学，核对他们加密后生成的 encrypted.txt 是否正确。
5. 敌方可以向 MAC Oracle 提交两个查询 m 和 m’，从而得到相应的(t_1, t_2,…, t_l)和 (t_1’, t_2’,…, t_l’)。显然有 $Vrfy_k$(m, t_1, t_2,…, t_l)=1 和 $Vrfy_k$(m’, t_1’, t_2’,…, t_l’)=1。取 n_2使得 n_2⊕t_1= m_2’⊕t_1’，并且令 n=(m_1,n_2,m_3’,m_4’,…m_l’), v=(t_1, t_2’, t_3’,…, t_l’)。显然 n 不等于 m 和 m’，并且不难验证 $Vrfy_k$(n, v)= 1。