网络安全技术第三次课堂作业

> 朱浩泽 1911530 计算机科学与技术

$$
\begin{aligned}
M = WHITEHAT &= 01010111010010000100100101010100010001010100100001000001010101 00 \\
K = BLACKHAT &= 10000100100110011000001010000111100101101001000010000010101010 01 \\
IP_{KEY}(K) &= 11111111000000001000000000110101110000011001100000100010 \\
U_0 &= 11111111000000001000000000 11 \\
V_0 &= 01011100000110011000001000 10 \\
U_1 = LS_1(U_0) &= 11111110000000010000000001 11 \\
V_1 = LS_1(V_0) &= 10111000001100110000010001 00 \\
K_1 = P_{KEY}(U_1V_1) &= 00001111010000011011100100100001001010100000 1011 \\
IP(M) &= 11111111100010011001100101010101000000000000000000010011000000001 \\
L_0 &= 11111111100010011001100101010101 \\
R_0 &= 00000000000000000010011000000001 \\
EP(R_0) &= 10000000000000000000000000010000110000000000000010 \\
EP(R_0) \oplus K_1 &= 10001111010000011011100100110001111101010000001001 \\
S(EP(R_0) \oplus K_1) &= 11001100111011001011101111001010 \\
P(S(EP(R_0) \oplus K_1)) &= 00111001101110111011000111010101 \\
L_1 = R_0 &= 00000000000000000010011000000001 \\
R_1 = L_0 \oplus F(R_0, K_1) = L_0 \oplus P(S(EP(R_0) \oplus K_1)) &= 11000110001100100010100010000000
\end{aligned}
$$