Max Gale

1) Output: pobuhfzeh

2) Output: fckdcrbq

3) a. K1 = 0x0B02679B49A5
   b. L0 = 0xCC00CCFF
      R0 = 0xF0AAF0AA
   c. E[R0] = 0x7A15557A1555
   d. E[R0] xor K1 = 0x711732E15CF0
   e. S-Box Result = 0x C416D50

4)

5) The problem with this scheme is that an attacker could use the two messages to create the key for himself.

6)