

1 Tutorial 3

1. Assume that you are creating a four-bit block cipher with a single-bit key. Choose a random permutation for the block cipher for each value of the key. What is the theoretical maximum key size beyond which you are guaranteed that two different keys encrypt identically. (1 mark)
2. For a hypothetical 5-DES encryption scheme with 5 independent keys used as E-E-E-D-D, what is the effective key length for a KPA (known plain-text attack), CPA (chosen plain-text attack) given that storage is not a consideration. (1.5 marks)
3. In DES, suppose that $F(R, K) = 0$, i.e., for any input the F function output 0. What function does DES compute? (1 mark)
4. In DES, how many bits in (L_1, R_1) , i.e., the 64 bits of the result of the first round, are related to bit 1 in (L_0, R_0) ? I.e., if the value of bit 1 in L_0 changes, how many bits of (L_1, R_1) may be changed? Assume key is the same in both cases. (.5 marks)
5. Suppose DES is modified so that the high order 44 key bits are set to 0 so that only the 20 low order bits are used. What is the effective key length of this system? (.5 marks)
6. Q1 on page 125 of your textbook. (1.5 marks)
7. Q4 on page 125 of your textbook. (1 mark)
8. Q5 on page 125-126 of your textbook. (1 mark)