CRYPTOGRAPHY AND NETWORK SECURITY

HOMEWORK 5

1. A transpositions block has 10 inputs and 10 outputs. What is the order of the permutaiton group? What is the key size?

2. A subsitution block has 10 inputs and 10 outputs. What is the order of the permutation group? What is the key size?

3. A message has 2000 characters. If it is supposed to be encrypted using a block cipher of 64 bits, find the size of the padding and the number of blocks.

4. A 6 × 2 S-box exclusive-ors the odd-numbered bits to get the left bit of the output and exclusiver-ors the even-numbered bits to get the right bit of the output. If the input is 110010, what is the output? If the input is 101101, what is the output?

5. A 4 × 3 S-box rotates the other three bits. If the leftmost bit is 0, the three other bits are rotated to the right one bit. If the leftmost bit is 1, the three other bits are rotated to the left one bit. If the input is 1011, what is the output? If the input is 0110, what is the output?