Solutions to Assignment 8

H1. Since N is the number of different four bit messages, $N = 2^4 = 16$.

H2. For an alphabet of size N, there are N! simple substitutions. Since N = 16, there are 16! simple substitutions.

H3.* Since we are using a 3-bit key, there are $2^3 = 8$ substitutions theoretically possible. Note that there is a 1-1 correspondence between the input and the output, so having 8 possible keys implies we could have 8 possible "outputs" for a particular input.

H4.* Since there are $2^3 \cdot 2^3 = 2^6 = 64$ possible keys, there are 64 substitutions theoretically possible.

H5.* Trying all possible keys $k_1k_2k_3$, we get the following table:

$x_1x_2x_3x_4$	$k_1k_2k_3$	$y_1y_2y_3y_4 = E(E(x_1x_2x_3x_4, k_1k_2k_3), k_1k_2k_3)$
0101	000	0101
0101	001	1110
0101	011	0011
0101	111	0101
0101	110	0010
0101	101	1101
0101	100	1000
0101	010	1011
0101	001	1110

From the above table it is clear that the correct key is 110. Following is the calculation when $k_1k_2k_3 = 110$ (see page 222 for the procedure):

$x_1x_2x_3x_4 = 0101$.

$t_1t_2 = S(x_3x_4x_3 \oplus k_1k_2k_3)$

$x_3x_4x_3 \oplus k_1k_2k_3 = 010 \oplus 110 = 100$. From the s-box, we see $S(100) = 01$.

So, $t_1t_2 = 01$.

$u_1u_2 = x_1x_2 \oplus t_1t_2 = 01 \oplus 01 = 00$.

So, $E(x_1x_2x_3x_4, k_1k_2k_3) = x_3x_4u_1u_2 = 0100$.

Now we need to find E(0100, 110):

Let $x_1'x_2'x_3'x_4' = 0100$

$t_1't_2' = S(x_3'x_4'x_3' \oplus 110) = S(000 \oplus 110) = S(110) = 11$.

$u_1'u_2' = x_1'x_2' \oplus t_1't_2' = 01 \oplus 11 = 10$.

Thus, $E(0100, 110) = x_3'x_4'u_1'u_2' = 0010$.

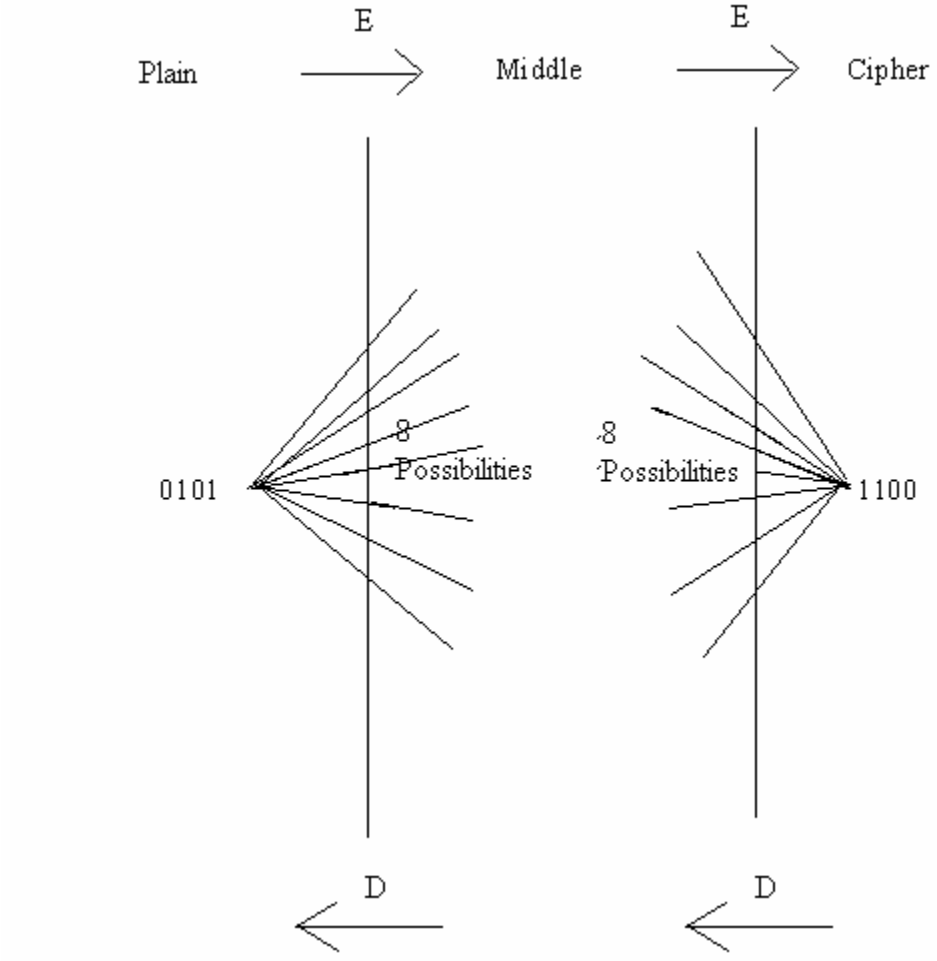
Thus, $E(E(x_1x_2x_3x_4, k_1k_2k_3), k_1k_2k_3) = E(E(0101,110),110)) = 0010 = y_1y_2y_3y_4$.

There is no better way of getting the right key other than just trying all possible keys.

H6. Since there are $2^3 \cdot 2^3 = 64$ possible keys, we would need a maximum of 64 guesses.

H7.* Since we have a 3-bit key, we would have to try $2^3 = 8$ keys for each list.

Given the plaintext $x_1x_2x_3x_4$, make the list $E(x_1x_2x_3x_4,k_1k_2k_3)$, and given the ciphertext $y_1y_2y_3y_4$ (that $x_1x_2x_3x_4$ corresponds to) make the list $D(y_1y_2y_3y_4,m_1m_2m_3)$. Compare the lists and match any 2 results that are the same. Suppose the 2nd result in the E-list corresponds to the 5th result in the D-list. Let $k_1k_2k_3$ be the key used to obtain that 2nd result, and let $m_1m_2m_3$ be the key used to obtain that 5th result. We know $k_1k_2k_3$ maps $x_1x_2x_3x_4$ to "something" and that that "something" is mapped by $m_1m_2m_3$ to $y_1y_2y_3y_4$. So $k_1k_2k_3$, $m_1m_2m_3$ could possibly be the right pair of keys. Note we could have multiple matches, so we could have multiple possible pairs of keys. This is why it is important to have more than 1 message block.



H8.* The meet-in-the-middle attack on Double DES with 2 different keys is *identical* to the procedure described in H7, except that the keys and the messages are considerably larger.

Since we are using a 56-bit key, there are $2^{56} \cdot 2^{56} = 2^{112}$ possible two-part keys for Double DES.

Using the meet-in-the-middle attack, we have to try 2^{56} keys for the E-list and 2^{56} keys for the D-list. Thus, we only need to try $2 \cdot 2^{56} = 2^{57}$ one-part keys. Note that this is considerably smaller than 2^{112}.