<u>Section 4 Lecture 25 – DES Implementation - Exercise</u>

Try to work through the following example of the operation of DES. This is a lengthy procedure, but good practice and might help you fully understand the workings!

(i) Take the 56-bit keyword

10010100011001011101010101011101111110101010101010101110
\`

Turn this into a 64-bit keyword by adding in an even parity bit after each sub-block of seven bits.

(ii) Take the 64-bit message

0010101010111101001010010011101101011000111010101010000111101110

Apply the initial permutation below to the message, where the notation means that the first bit of the output is the 58th bit of the original block, and so on.

{58, 50, 42, 34, 26, 18, 10, 2, 60, 52, 44, 36, 28, 20, 12, 4, 62, 54, 46, 38, 30, 22, 14, 6, 64, 56, 48, 40, 32, 24, 16, 8, 57, 49, 41, 33, 25, 17, 9, 1, 59, 51, 43, 35, 27, 19, 11, 3, 61, 53, 45, 37, 29, 21, 13, 5, 63, 55, 47, 39, 31, 23, 15, 7}

Now split the message into two halves of 32 bits. Perform the following steps on the first half first:

(iii) Expand the 32 bits to a 48-bit block. To do this, take each block of 4 bits in turn. For each block of 4 bits, look at the 32-bit block, and write the bit immediately to the left of the 4-bit block under consideration, followed by the 4-bit block, followed by the bit immediately to the right (for the first and last blocks, you will need to "wrap around" similarly to modular arithmetic). For example, the 4-bit block in positions 1, 2, 3, 4 would be transformed to the six bit block in positions 32, 1, 2, 3, 4, 5, the next block in positions 5, 6, 7, 8 would be transformed to the 6-bit block consisting of positions 4, 5, 6, 7, 8, 9, and so on.

(iv) Generate a 48-bit subkey from the *64-bit keyword* by doing the following permutations:

- Firstly create a 56-bit key using the permutation
{57, 49, 41, 33, 25, 17,9, 1, 58, 50, 42, 34, 26, 18, 10, 2, 59, 51, 43, 35, 27, 19, 11, 3, 60, 52, 44, 36, 63, 55, 47, 39, 31, 23, 15, 7, 62, 54, 46, 38, 30, 22, 14, 6, 61, 53, 45, 37, 29, 21, 13, 5, 28, 20, 12, 4}
- Then create a 48-bit key subkey from *this 56-bit key* using the permutation
{14, 17, 11, 24, 1, 5, 3, 28, 15, 6, 21, 10, 23, 19, 12, 4, 26, 8, 16, 7, 27, 20, 13, 2, 41, 52, 31, 37, 47, 55, 30, 40, 51, 45, 33, 48, 44, 49, 39, 56, 34, 53, 46, 42, 50, 36, 29, 32}

(If you are wondering why we don't do this all in one go, we could here, but the "middle" 56-bit keyword is used in practice to determine shifts in future rounds)

(v) XOR your 48-bit block from (iii) with your 48-bit subkey from (iv)

(vi) Split the result of (v) into eight blocks of six letters. For each block in turn, apply the appropriate S-box to each of these six blocks in turn (so S_1 on the first block, S_2 on the second block, and so on) using the lookup table provided separately. To use these tables, here a * can be either 0 or 1 – look up the cell corresponding to the appropriate row and column that matches your block. The resulting number from 0 to 15 should then be written in binary to get a 4-bit block. Put these 4-bit blocks all together to get a 32-bit block.

(vii) Apply the following permutation to your 32-bit block:

{16, 7, 20, 21, 29, 12, 28, 17, 1, 15, 23, 26, 5, 18, 31, 10, 2, 8, 24, 14, 32, 27, 3, 9, 19, 13, 30, 6, 22, 11, 4, 25}

(viii) Repeat (iii) – (vii) for the second block of 32 bits (the second half obtained when you originally split your message into two 32-bit halves)

(ix) Merge together the two 32-bit blocks obtained from this process by writing the second one followed by the first one, to get a 64-bit block.

This completes the first round. In practice, there are another 15 rounds to do with a different subkey each time, but you don't have to do these – this one round is sufficient to illustrate it!

(x) Calculate the inverse permutation of the permutation in (ii). To do this, find each number 1-64 in turn in the permutation and write down its position. For example, 1 is in position 40 of the original permutation, so the inverse permutation begins {40,…}.

(xi) Apply the inverse permutation you found in (x) to the 64-bit block you obtained in (ix).

And that completes the process – you have your DES encrypted message (apart from you only did one round rather than sixteen!)