question2.m :

```
% ELEN3015 Lab 2, Question 2

clc
clear all

% keys to analyse
key1 = '1F1F1F1F0E0E0E0E';
key2 = '1FFE1FFE0EFE0EFE';
key3 = '1FFEFE1F0EFEFE0E';

% convert to binary row vectors
key_bin1 = hex2binary(key1);
key_bin2 = hex2binary(key2);
key_bin3 = hex2binary(key3);

% initial permutation
key_string1 = permuter(key_bin1, 'parity');
key_string2 = permuter(key_bin2, 'parity');
key_string3 = permuter(key_bin3, 'parity');

% DEA rounds to generate all subkeys
for round_no=1:16
    key_schedule1(round_no,:) = generateSubKey(key_string1,round_no);
    key_schedule2(round_no,:) = generateSubKey(key_string2,round_no);
    key_schedule3(round_no,:) = generateSubKey(key_string3,round_no);
end

% count and classify the subkeys
[count1, classification1] = analyseSubKeys(key_schedule1);
[count2, classification2] =  analyseSubKeys(key_schedule2);
[count3, classification3] =  analyseSubKeys(key_schedule3);

% output
disp(['Key ', key1, ' has ', num2str(count1), ' unique subkey(s). It is a ', classification1, ' key'])
disp(['Key ', key2, ' has ', num2str(count2), ' unique subkey(s). It is a ', classification2, ' key'])
disp(['Key ', key3, ' has ', num2str(count3), ' unique subkey(s). It is a ', classification3, ' key'])
```

When question2.m is run in the workspace, the following output is displayed to the command window:

```
Key 1F1F1F1F0E0E0E0E has 1 unique subkey(s). It is a weak key
Key 1FFE1FFE0EFE0EFE has 2 unique subkey(s). It is a semi weak key
Key 1FFEFE1F0EFEFE0E has 4 unique subkey(s). It is a possibly weak key
```

---

question3.m :

```
% ELEN3015 Lab 2, Question 3

clc
clear all

% inputs
plaintext_str = '0000000100100011010001010110011111000100110101011110011011101111';
key_str       = '0001001100110100010101110111100110011011101111001101111111110001';
plaintext = plaintext_str - '0';
key_64 = key_str - '0';
key_56 = permuter(key_64, 'parity');                    % discard parity bits and permute
block = permuter(plaintext,'initial');                  % initial permutation

round_no = 1;
subkey = generateSubKey(key_56,round_no);

% perform a DEA round of encryption
[ L_block, R_block ] = DES(block, round_no, subkey);

% output
disp(['Input 64-bit message: ', binary2hex(plaintext),]);
disp(['Input 64-bit key:     ', binary2hex(key_64)])
disp(['Permuted 56-bit key:    ', binary2hex(key_56)])
disp(['48-bit round (', num2str(round_no),') subkey:  ', binary2hex(subkey)])
disp(['Permuted block: ', num2string(block)])
disp(['Left: ', num2string(L_block), '   Right: ', num2string(R_block)])
```

When question3.m is run in the workspace, the following output is displayed to the command window:

```
Input 64-bit message: 0123456789ABCDEF
Input 64-bit key:     133457799BBCDFF1
Permuted 56-bit key:    F0CCAAF556678F
48-bit round (1) subkey:  1B02EFFC7072
Permuted block: 11001100000000000110011001111111111110000101010101111000010101010
Left: 11110000101010101111000010101010   Right: 11101111010010100110010101000100
```

question4.m :

```
% ELEN3015 Lab 2, Question 4

clc
clear all

% inputs
plaintext_str = '0123456789ABCDEF';                         % test block
plaintext = hex2binary(plaintext_str);                      % convert to binary row vector
key_str = '0001001100110100010101110111100110011011101111001101111111110001';
key_64 = key_str - '0';                                     % convert to binary row vector
key_56 = permuter(key_64, 'parity');                        % discard parity bits and permute

%% encryption
block = permuter(plaintext,'initial');                      % initial permutation
for round_no = 1:16                                         % 16 rounds of DES
    subkey = generateSubKey(key_56,round_no);               % subkey generation for each round
    [ L, R ] = DES(block, round_no, subkey);                % DEA (encryption)
    block = [L R];                                          % rejoin the L and R halves
end
cipherblock = permuter(block, 'final');                     % final permutation


%% decryption
out_block = permuter(cipherblock,'initial');                % initial permutation
for round_no=1:16                                           % 16 rounds of DES
    subkey = generateSubKey(key_56,17-round_no);            % subkeys generated in reverse order
    [L, R] = DES(out_block, round_no, subkey);              % DEA (decrpytion)
    out_block = [L R];                                      % rejoin block halves
end
decrypted = permuter(out_block, 'final');                   % final permutation


% output and check
decrypted_str = binary2hex(decrypted);
cipher_str = binary2hex(cipherblock);
disp(['Input 64-bit key:     ', binary2hex(key_64)])
disp(['Encryted ciphertext:  ', cipher_str])
disp(['Original input text:  ', plaintext_str]);
disp(['Decrypted plaintext:  ', decrypted_str])
disp(' ')

% check
if isequal(decrypted_str,plaintext_str)
    disp('The decrypted block matches the plaintext block');
else
    warning('The decrypted block does NOT match the plaintext block');
end
```

When question4.m is run in the workspace, the following output is displayed to the command window:

```
Input 64-bit key:     133457799BBCDFF1
Encryted ciphertext:  85E813540F0AB405
Original input text:  0123456789ABCDEF
Decrypted plaintext:  0123456789ABCDEF

The decrypted block matches the plaintext block
```