Laboratory Session 6

1. Introduction

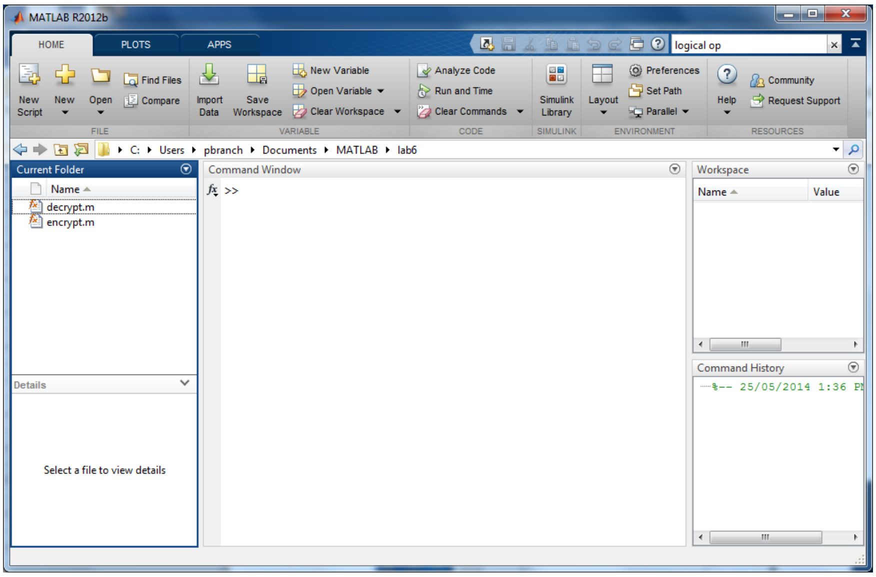
In this lab you will use MATLAB to break a symmetric key, block algorithm that uses some of the transforms used in AES. The encryption algorithm was used with cipher block chaining. The purpose of the lab is for you to determine the plaintext from a given ciphertext message encrypted with an unknown, but short key.

You will need to use MATLAB which you should have set up in the previous lab. You may wish to refer to the previous lab to revise MATLAB.

2. Method

You are to decrypt the following message c which you know was encrypted with the code in `encrypt.m` and using cipher block chaining where each block of cipher text is XOR ed with the previous block of cipher text. The routine `decrypt.m` is available to carry out decryption. The routine `encrypt.m` is included for interested students to examine, but is not required for the lab.

1. Install the routine `decrypt.m` in the work directory. This can be done by dragging the file from the desktop directly into the left-hand panel as shown below:



2. Determine the key that was used to encrypt the message. The key is greater than 0 and less than 64.

   This can be done by trying different key values on the first block of cipher text `ct1`.

3. Once the key is determined, decrypt the remaining blocks. Cipher block chaining was used to encrypt blocks 2 to 7. This means that each block of cipher text was XOR ed with the previous block of cipher text after the plain text was encrypted. For example ct2 = encrypted plain text XOR ct1.

4. ct1 is XORed with an initialisation vector. The initialisation vector in this case is all 0s.

5. To recover blocks 2 to 7 it is necessary to XOR them with the previous cipher text block before applying the decryption routine. The MATLAB routine `bitxor` will be useful.

Laboratory Session 6

3. Cipher text

The cipher text is available in the file Lab6ciphertext.txt but can also be copied from here.

```
ct1 = [11 34 57 51 39 32 21 38 51 23 35 34 34 51 41 17]
ct2 = [41 24 44 17 20 4 38 55 36 50 4 55 11 23 16 55]
ct3 = [14 33 11 53 51 17 11 4 51 30 39 4 49 2 54 34]
ct4 = [42 9 26 17 38 34 44 44 21 45 20 39 36 49 33 10]
ct5 = [59 43 62 34 4 6 4 5 54 7 59 20 12 18 26 57]
ct6 = [31 8 13 52 43 32 17 20 18 53 8 61 4 52 63 10]
ct7 = [8 29 62 45 62 55 57 54 52 6 33 40 55 7 12 57]
```

4. Assessment

No report is required for this lab. Show the lab supervisor the plain text and your code and explain how it works.