BIL 105E – Introduction to Scientific and Engineering Computing (C)

Spring 2016-2017

Homework 5
Cryptology

Assignment Date: 18.04.2017
Due Date: 25.04.2017 - 23:59
Duration 7 days

In this homework, you will implement a program that decrypts an encrypted text and prints the decrypted text to the console. A text is encrypted using two algorithms called Caesar square and Caesar cipher. In addition to these algorithms, conversion between binary numbers to decimal numbers need to be implemented to decrypt the text.

In this homework an organization wants to hold their clients' sensitive data in encrypted forms. You will be provided an encrypted text with 24 characters in which the client's name (10 characters) and its ID (9 characters) are stored. In addition, the information about how the data was encrypted is provided in the rest of the 5 characters of the encrypted text. Details of the encryption is given in the next part.

Encryption

The encrypted string has 24 characters. Here is an example encrypted string:

ozqnhfjxfw17031500501101

Encrypted string has 3 parts.

- The first 10 characters which holds Name data. These characters consists of letters from English alphabet. Only lowercase letters are used. Name can be encrypted using four different modes. Details will be given in Encryption Algorithms section.

- Next 9 characters holds Number data. These characters consists of numbers from 0 to 9. Number can be encrypted using Caesar square. Details will be given in encryption algorithms section.

- The last 5 characters hold the auxiliary data in binary form. Auxiliary data includes *the mode* and the *modifier* of the encryption. First 2 characters of the auxiliary data corresponds to the mode whereas the last 3 characters of the auxiliary data corresponds to the modifier.

Encryption Algorithms

Encrypting Name: Name can be encrypted in 4 different methods. Mode of the encryption determines which method has been used to encrypt.

- Mode 0
In this mode, name has not been changed. Modifier does not effect anything in this mode.

abcd → abcd

- Mode 1
In this mode, name has been encrypted using Caesar cipher using positive modifier. Caesar cipher is a very easy algorithm that changes the letters with respect to a modifier parameter. If we number alphabet from 1 to 26, each letter is replaced with its Mth subsequent letter in the alphabet. M is the modifier number. If overflow occurs, it continues from the other end.

If modifier 3: a->d
h->k
y->b (overflow)

- Mode 2
In this mode, name has been encrypted using Caesar cipher using negative modifier. Caesar cipher is a very easy algorithm that changes the letters with respect to a modifier parameter. If we number alphabet from 1 to 26, the letter is replaced with its Mth preceding letter in the alphabet. M is the modified number again. If overflow occurs, it continues from the other end.

If modifier 3: a->x (overflow)
h->e
y->v

- Mode 3
In this mode, name has been inverted. Modifier does not effect anything in this mode.

abcd → dcba

Encrypting Number: Number has been encrypted using Caesar square. Caesar square can only perform encryption if the number of elements is equal to square of an integer. In this homework, number has 9 digits which is the square of the 3. Caesar square creates a 3x3 square matrix from the elements and gets transpose of it, then converts it back to a single line.

$$123456789 \rightarrow \begin{bmatrix} 1 & 2 & 3 \\ 4 & 5 & 6 \\ 7 & 8 & 9 \end{bmatrix} \rightarrow \begin{bmatrix} 1 & 4 & 7 \\ 2 & 5 & 8 \\ 3 & 6 & 9 \end{bmatrix} \rightarrow 147258369$$

Encrypting Auxiliaries: Auxiliaries are stored at the end of the encrypted string in binary form. Mode has 2 binary digits and modifier has 3 binary digits.

Corruption

Size of the characters in the data is always 24 characters. There may be some corruption in data. If Name part has any other character than English alphabet or Number part has any other characters than numbers or auxiliary part has any other character than '0' or '1' then data is corrupted. You need to check if data is valid in run time.

Decrypter

You are expected to write a program that decrypts a character array storing an encrypted string, following the rules explained above. You are required to implement at least these four functions:

- decryptName
- decryptNumber
- decryptAuxiliaries
- checkCorruption

You will decide the input and output parameters of these functions.

Important :

- Do not use string library, use char array instead.
- You are not allowed to use **global variable,** use call by reference instead.
- Do not use subscripting ([]), use pointer arithmetic instead.
- Use effective address as the input of the functions if necessary.

GRADING

Compiling: Your code should be able to compiled using gcc on ssh.itu.edu.tr without any errors or warning. Your code will be compiled with the following line while grading.

gcc homework5.c -o homework5

Your code will be run as following line while grading.

./homework5

Run Time: In the run time, at first, program will ask the data to decrypt.

Enter the data to decrypt:

Then user will enter the data. As an example, following line can be entered to test your code.

ozqnhfjxfw17031500501101

Output: Program decrypts the line and gives the result as in the following format:
Decrypted ---
Name: julicaesar
Number: 130710055
Mode: 1
Modifier: 5

If data is corrupted, program should print following line then exit:
Data is corrupted

Important: Do not print anything else other than the expected text, and follow the output format.

Termination: Your code should terminate after it prints the decoded information in given format.. Successful main functions returns with 0. Do not forget to return 0 if your code worked as it should. Return 1 if an error occurred(corruption).

Example Compilation and Run:

```
airlab@mia:~/Cihan/BIL -105E/Homework5$ gcc homework5.c -o homework5
airlab@mia:~/Cihan/BIL -105E/Homework5$ ./homework5
Enter the line to decrypt:ozqnhfjxfw17031500501101
Decrypted ---
Name: julicaesar
Number: 130710055
Mode: 1
Modifier: 5
airlab@mia:~/Cihan/BIL -105E/Homework5$
```

```
airlab@mia:~/Cihan/BIL -105E/Homework5$ ./homework5
Enter the line to decrypt:3213hfjxfw17&&1500501102
Data is corrupted
airlab@mia:~/Cihan/BIL -105E/Homework5$
```

Evaluation Criterion:

- Compiling and linking with gcc
- Clear and efficient code
- decryptName, decryptNumber, decryptAuxiliaries, checkCorruption functions
- Call by reference
- Pointer arithmetic
- Clean run and correct output in requested format

All the assignments are considered individual assignments and you are expected to do it by yourself. Any form of plagiarism, even partial, will not be tolerated. It is subject to serious disciplinary actions. Note that professionals help in any form or shape is considered as an act of plagiarism.