CPSC370: Introduction to Computer Cryptology

Program 1: Caesar Cipher

Due Wednesday, September 14, 2016 11:59PM

In this programming assignment, you are asked to write C/C++/Java codes to implement encryption/decryption functions for Caesar Cipher, and brute force attack function for cipher texts.

1 Details of the program

You need to do the following tasks:

1. Implement encryption/decryption functions that take a key (as an integer in 0, 1, 2, ..., 25) and a string. The function should only operate on the characters 'a', 'b', ..., 'z' (both upper and lower case), and it should leave any other characters, unchanged.

2. Implement a function that performs a brute force attack on a ciphertext, it should print a list of the keys and associated decryptions. It should also take an optional parameter that takes a substring and only prints out potential plaintexts that contain that decryption.

3. Show the **output** of your encrypt function on the following (key, plaintext) pairs:

   - k = 6, plaintext = "Get me a vanilla ice cream, make it a double."
   - k = 15, plaintext = "I don't much care for Leonard Cohen."
   - k = 16, plaintext = "I like root beer floats."

4. Show the **output** of your decrypt function on the following (key, ciphertext) pairs:

   - k = 12, ciphertext = "NDUZS FTQ BUZQ OAZQE.'
   - k = 3, ciphertext = "FDHVDU QHHGV WR ORVH ZHLJKW."
   - k = 20, ciphertext = "UFGIHXM ULY NUMNYS."

5. Show the **output** of your attack function on the following ciphertexts, if an optional keyword is specified, pass that to your attack function:

   - ciphertext = "GRYY GURZ GB TB GB NZOEBFR PUNCRY." keyword = "chapel"
   - ciphertext = "WZIV KYV JYFK NYVE KYV TPDSRCJ TIRJY." keyword = "cymbal"
   - ciphertext = "BAEEQ KLWOSJL OSK S ESF OZG CFWO LGG EMUZ." no keyword

2 Submission

1. **Electronic submission** (Due by Wednesday, September 14, 2016 11:59PM)

   (a) Make sure that your program is compilable

   (b) Zip both the source codes and output screenshots into a file. The file format is as follows: `FirstNameLastName_Program1.zip` (e.g., `DongshengChe_Program1.zip`)

   (c) Upload the zip file onto D2L Dropbox

2. **Hardcopy submission** (Due by Thursday, September 15, 2016 in class)

   Your hardcopy should include:

   - Grading sheet (top)
   - Source code (middle)
   - Output screenshots (bottom)