# Program 3: Stream Cipher RC4

CPSC370: Introduction to Computer Cryptology

Due Monday, October 17, 2016 11:59PM

In this programming assignment, you are asked to write C/C++/Java codes to implement the RC4 algorithm (size of vector $S = 256$).

## 1 Details of the program

1. Implement the RC4 algorithm in the following steps:

   (a) Initialize the S vector and T vector for a given seed (or initial key);

   (b) Permute the S vector;

   (c) Generate key streams;

   (d) Encrypt each byte stream of the plain text using the corresponding key byte (Hint: For byte XOR, see `http://www.cplusplus.com/forum/articles/38516/`);

   (e) Decrypt each byte stream of the cipher text using the corresponding key byte;

   When XORing two same bytes, you will generate 0. Just produce the byte itself if two bytes are same.

2. Experiment the correctness of your program by using the following plain text and seed:

   (a) plain text: cryptology seed: 1 2 3 6

   (b) plain text: RC4 seed: 5 7 8 9

   For each test of your RC4 algorithm, you need to output the following information

   (a) Plain text

   (b) Seed

   (c) The vector S after intitial permutation

   (d) Key streams used for the input plain text

   (e) Enrypted message

   (f) Decrypted message

3. Your output should look like the screenshot ouput as shown in Figure 1.

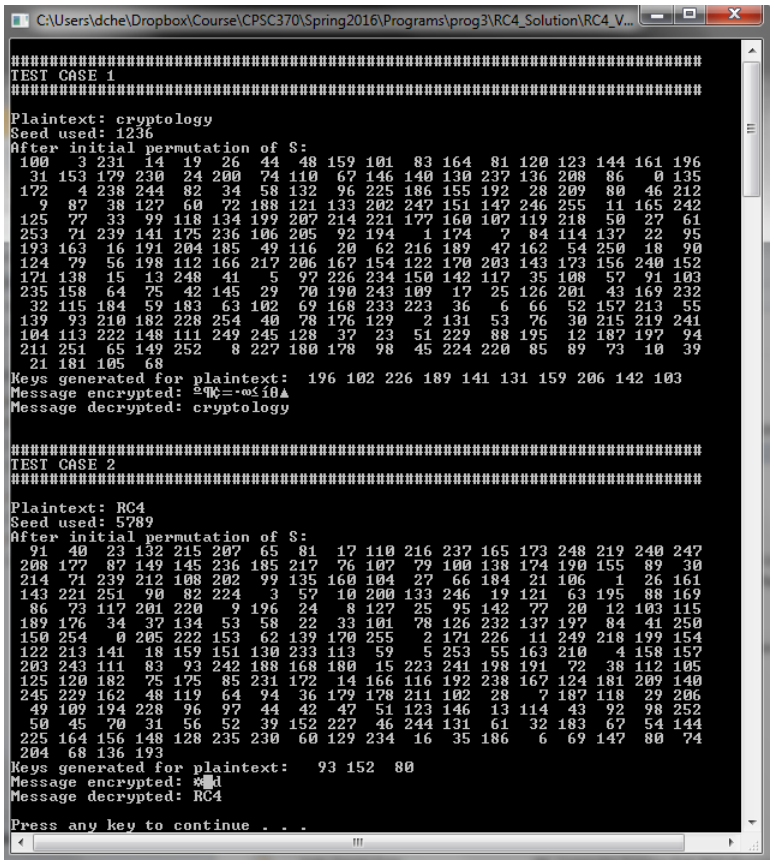


Figure 1: A screenshot of outputs

# 2 Submission

1. **Electronic submission** (Due by Monday, October 17, 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_Program3.zip` (e.g., `DongshengChe_Program3.zip`)

   (c) Upload the zip file onto D2L Dropbox

2. **Hardcopy submission** (Due by Tuesday, October 18, 2016 in class)

   Your hardcopy should include:

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