Program 4A: S-DES

CPSC370: Introduction to Computer Cryptology

Due Monday, November 14, 2016 11:59PM

In this programming assignment, you are asked to write C/C++/Java codes to implement encryption/decryption functions for S-DES discussed in class.

1 Details of the program

You need to do the following tasks:

1. Implement an encryption function that performs four rounds of encryption, using the S_1 and S_2 boxes, and key generation schemes discussed in class.
(Hint: http://www.cplusplus.com/reference/bitset/bitset/operators/)

2. Implement an decryption function that performs four rounds of decryption, using the S_1 and S_2 boxes, and key generation schemes discussed in class.

3. Use the following $plaintext = 100010110101$ and $K = 111000111$, print out bit strings of L_1R_1, L_2R_2, L_3R_3, and L_4R_4.

4. Decrypt your cipher text L_4R_4, and print out bit strings of L_3R_3, L_2R_2, L_1R_1, and L_0R_0.

2 Submission

1. **Electronic submission** (Due by Monday, November 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_Program4A.zip` (e.g., `DongshengChe_Program4A.zip`)

   (c) Upload the zip file onto D2L Dropbox

2. **Hardcopy submission** (Due by Tuesday, November 15, 2016 in class)

   Your hardcopy should include:

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