Task

Contact

📧 khagan.karimov@utah.edu

🐦 twitter.com/KhaganKarimov

Student: Khagan Khan Karimov

Course: CS 6490-001 Network Security

Instructor: Prof. Dr. Kasera

▼ Task Content:

Program a secret key encryption and decryption method based on the following:

- Your program must take an array of 8 characters as an input and output an array of 8 encrypted characters.
- Write the code necessary to create 8 unique random substitution tables, one for each character of the array.
- Your methods must use a 64-bit key (can be represented as another array of 8 characters) derived from an 8-character password.

Encryption algorithm: Take the input array and xor it with the key. Using the xored output, perform a character-by-character substitution using the different substitution tables. Perform the permutation step once after the substitution step. For the permutation step, (circular) shift the bit pattern by one to the left with the leftmost bit becoming the rightmost bit. Repeat the above steps 16 times, corresponding to 16rounds, with the output of a round serving as the input for the next round.

Decryption algorithm: Reverse the encryption algorithm. The permutation, however, should (circular) shift the bit pattern by 1 bit to the right. The substitution tables are also used for reversing the substitution.Take a sample input bit pattern (represented as an array of 8 characters) and produce the encrypted output pattern. Feed the encrypted output pattern to your decryption function to obtain the input bit pattern. Match the two patterns to ensure that your decryption indeed reverses your encryption. Do the same by changing only one bit in the input pattern.

You must include print statements in your code to print the input, per round encrypted output, and per round decrypted output in an output file for both input bit patterns.Turn in your code (in plain text) along with the output files.

While you can use any computer to work on your programs, make sure that these run on the CADE lab machines.We cannot grade any programs that do not run on the CADE lab machines.

VERY IMPORTANT: Please provide a short readme file with any instructions to run your programs on the CADE machines. We prefer that your code is written in Java but will accept Python code as well.