

Principles of Web Development

Mini Assignment 2
Due: September 25, 2018

Create a simplified DES encryption and decryption algorithm in Java.

This is a single source file single class program called MyDES.

The program will prompt the user for:

- Three positive integer number. Each number must be strictly >9 and <100. These values as a group (tuple) is called the key. The program terminates prematurely if the user inputs an incorrect number. It shows the error message: “You did not input 3 positive integer numbers each strictly >9 and <100”. If the key is valid then the program displays: “Your key is valid.”
- A single sentence stored as a single-line string. This is called the message. The program validates the string. If the string is empty (null) or length zero, then the program terminates with the error message: “You input an empty string”. If the message is valid then the program displays: “Your message is valid.”

The basic flow of the program:

- Encrypt the input string and display the encrypted string.
- Then it will automatically decrypt the encrypted string and display the decrypted string. Note: the decrypted string should agree with the input string.
- The program then terminates
- Sample run-time output:

Welcome to myDES

Please enter your key (3 numbers): **95 25 30**

Your key is valid. ← or: the error message and then program terminates

Please enter your message: **my name is Bob**

Your message is valid. ← or: the error message and then program terminates

Encrypted message: <<encrypted message displayed as a single line>>

Decrypted message: **my name is Bob**

End of myDES

The simplified DES algorithm:

- Assumes: int key[3] and String message
- Convert String message into char array[message.length] copy each character from message into this array.
- Create a new array: char array2[message.length] and block Caesar cipher array into array2 using the key.
- Rotate the key: Cell 0 goes to cell 1, cell 1 goes to cell 2, cell 2 goes to cell 0.
- Create a new array: char array3[message.length] and block Caesar cipher array2 into array3
- Rotate key, again.
- Create a new array: char array4[message.length] and block Caesar cipher array3 into array4

- Array4 is the final encrypted message
- Print out array4.

The decryption algorithm is the inverse of the above.

WHAT TO HAND IN

Submit a run-able Java file to myCourses Mini Assignment #2 electronic drop box.
This mini assignment has two late days with -5% penalty per late day.

HOW IT WILL BE GRADED

It will be graded proportionally based on the above requirements. The program must run to be graded.

This assignment is out of 20 points.

- 2 points - Following instructions
- 4 points - Error checking
- 7 points - Encryption
- 7 points - Decryption