

# Secure Communication

The MIT exam cell wants to convey the message to their instructors and pass the messages via his LAN network. But the exam cell wants to make it private and transfer securely to the instructor. For this purpose they select message transformation techniques. In this technique, The message transformation is as follows; each character into next  $k^{\text{th}}$  character, each space character into @ , each full stop into # and rest special characters remain as it is. (for example if  $k=3$ ; A = D, a =d, B = E, b = e.....Z=C, z = c, 0 = 3, 1=4,2=5,9=3 space=@, . = #, %=%)

Now when the exam cell sends the message along with shift value  $k$  to the instructor.

At the instructor's end, if and only if the instructor types a valid value of  $k$  for the received transformed message provided by the exam cell then the instructor is able to read the original message.

Assume you are a software developer in GradsIT and your job is to design Message Transmission Software for secure message communication for the MIT College.

Design this software with the best suitable constructs of java / python taught by your instructors in the boot camp.

## **Input:**

$k$  is an integer value where  $1 < k < 20$ .

Message: Any alphanumeric sentence (may contain symbol ).

## **Output:**

Hello you send: transformed message

Receiver: if valid key then original message.

## **Example:**

### **Message Sender :**

Hello MIT CELL:

Please enter  $k$  value to shift transform message: 3

Now please type your message: Ab%c 123\*.

You send- De%f@456\*#

### **Message Receiver :**

Hello Instructor:

You got a message: De%f@456\*#

To read this in original please type  $k$  value provided by Cell:-3

Original Message: Ab%c 123\*.