Name - Yash Lakhtariya
Enrollment number - 21162101012
Branch - CBA   Batch - 61
INS Practical 9

Aim : Consider the scenario and provide solution accordingly - An organization
has given you a task to provide authentication to each and every message which
is being transfer between employees to identify the message is transferred by
legit employee only. (Hint - Use MAC).

Code :

```python
import hashlib
import YSL_io as ysl


ysl.printMGNTA("=============================== Sender side
===========================\n")
message = ysl.inputGRN("\nEnter the message : ")
ysl.printORNG("\nMessage : ", message)


result = hashlib.sha512(message.encode())
hashval = result.hexdigest()
ysl.printORNG("\nHash value : ", hashval)


finalmessage = message + 'xx' + hashval
ysl.printORNG("\nThe final message : ", end='')
print(finalmessage)
ysl.printGRN("\n......................... SENDING THE MESSAGE
........................\n")
ysl.printMGNTA("\n=============================== Receiver side
===========================\n")
ysl.printGRN("\n......................... RECEIVING THE MESSAGE
........................\n")


rm = finalmessage
ysl.printORNG("Received message : ", end='')
print(rm)
```

```python
rm2 = rm.split('xx')
message = rm2[0]
hashval = rm2[1]

result = hashlib.sha512(message.encode())
temp = result.hexdigest()

ysl.printORNG("\nReceived message : ", end='')
print(message)
ysl.printORNG("\nHash value of received message : ", end='')
print(temp)
ysl.printORNG("\nReceived hash value : ", end='')
print(hashval)
ysl.printGRN("\n............... Checking If message is altered or not ...............\n")

if temp == hashval:
    ysl.printRED("\nThe message is not altered and Integrity achieved.")
else:
    ysl.printRED("\nThe message is altered and Integrity not achieved.")
```

Name - Yash Lakhtariya
Enrollment number - 21162101012
Branch - CBA   Batch - 61
INS Practical 9

Output :


```
yash  …/INS  ⌥ main  08:50  .venv/bin/python p9.py
=============================== Sender side ===============================

Enter the message : hare krishna

Message : hare krishna
Hash value : 8275bd6c5d6a5cd85400055699c257f1fb64ce73d9444bf909364651245a9ed2516a0e24f909b4a586ef3eaf27ed1c614b426359b7249f576e732ed0c61b576b
The final message : hare krishnaxx8275bd6c5d6a5cd85400055699c257f1fb64ce73d9444bf909364651245a9ed2516a0e24f909b4a586ef3eaf27ed1c614b426359b7249f576e732ed0c61b576b

.......................... SENDING THE MESSAGE ..........................


=============================== Receiver side ===============================

.......................... RECEIVING THE MESSAGE ..........................

Received message : hare krishnaxx8275bd6c5d6a5cd85400055699c257f1fb64ce73d9444bf909364651245a9ed2516a0e24f909b4a586ef3eaf27ed1c614b426359b7249f576e732ed0c61b576b

Received message : hare krishna

Hash value of received message : 8275bd6c5d6a5cd85400055699c257f1fb64ce73d9444bf909364651245a9ed2516a0e24f909b4a586ef3eaf27ed1c614b426359b7249f576e732ed0c61b576b

Received hash value : 8275bd6c5d6a5cd85400055699c257f1fb64ce73d9444bf909364651245a9ed2516a0e24f909b4a586ef3eaf27ed1c614b426359b7249f576e732ed0c61b576b

................ Checking If message is altered or not ................


The message is not altered and Integrity achieved.
yash  …/INS  ⌥ main  08:50
```