GOA COLLEGE OF ENGINEERING

"Bhausaheb Bandodkar Technical Education Complex"

Experiment No: 6

GSM Encryption

Aim: To write and execute a program to implement GSM authentication

Theory:

Encrypted voice and data communications between the MS and the network is accomplished by using the ciphering algorithm A5. Encrypted communication is initiated by a ciphering mode request command from the GSM network. Upon receipt of this command, the mobile station begins encryption and decryption of data using the ciphering algorithm (A5) and the ciphering key (Kc).

The GSM A5/3 algorithm produces two 114-bit keystream strings, one of which is used for uplink encryption/decryption and the other for downlink encryption/decryption.

Code:

Client Program

```
import socket
ki=181105010
port = 12345
s = socket.socket()

def A8(RAND,ki):
   return (RAND^ki)%26

def A5_encrypt(key,data):
   alphabet = [’a’, ’b’, ’c’, ’d’, ’e’, ’f’, ’g’, ’h’, ’i’, ’j’,’k’, ’l’, ’m’, ’n

      ’, ’o’, ’p’, ’q’, ’r’, ’s’, ’t’, ’u’, ’v’, ’w’, ’x’, ’y’, ’z’]
   encrypted=""

   data=data.lower()
   for char in data:

      if char.isalpha():
         idx=(alphabet.index(char)+key)%26

encrypted+=alphabet[idx]
      else:

         encrypted+=char
   return encrypted

s.connect((’127.0.0.1’, port))
```

```
RAND=int(s.recv(1024).decode())
data=input("Enter data to be sent: ")
key=A8(RAND,ki)
encrypted=A5_encrypt(key,data)
print("sending encrypted message:",encrypted)

s.send(encrypted.encode())

s.close()
```

Server Program

```
import socket
from random import randint

maxBufSize=1000
ki=181105010
def A8(RAND,ki):

   return (RAND^ki)%26

def A5_decrypt(key,data):
   alphabet = ['a', 'b', 'c', 'd', 'e', 'f', 'g', 'h', 'i', 'j','k', 'l', 'm', 'n

      ', 'o', 'p', 'q', 'r', 's', 't', 'u', 'v', 'w', 'x', 'y', 'z']
   decrypted=""

   data=data.lower()
   for char in data:

      if char.isalpha():
         idx=(alphabet.index(char)-key)%26
         decrypted+=alphabet[idx]

      else:
         decrypted+=char

   return decrypted

s = socket.socket()
print ("Socket successfully created")

port = 12345

s.bind(('', port))
print ("socket binded to %s" %(port))
```

```
s.listen(5)
print ("socket is listening")

while True:
   c, addr = s.accept()
   print ('Got connection from', addr )
   RAND=randint(1000,100000)
   print(RAND)
   c.send(str(RAND).encode())

   key=A8(RAND,ki)
   encrypted=c.recv(maxBufSize).decode()
   decrypted=A5_decrypt(key,encrypted)
   print("Recieved and decrypted message:\n",decrypted)

        c.close()
```

Output:

Server output

```
$ p server.py
Socket successfully created
socket binded to 12345
socket is listening
Got connection from ('127.0.0.1', 54940) 61323
Recieved and decrypted message:

hello world
```

Client output

```
$ p client.py
Enter data to be sent: hello world

sending encrypted message: wtaad ldgas
```

Conclusion: A program to implement and execute GSM Encryption was successfully written and executed.