Vidya Vikas Education Trust's
Universal College of Engineering, Kaman Road,
Vasai-401212 Accredited by B+ Grade by NAAC
Experiment No.:3 GSM A3

Roll No: 80	Name: Kashyap Patel	Div: B	Batch: B1

Aim: To implement GSM A3 Security Algorithm in python.

Theory: The security procedures in GSM are aimed at protecting the network against unauthorized access and protecting the privacy of mobile subscribers against eavesdropping, eavesdropping on subscriber communication is prevented by ciphering the information. To protect the identity and location of the subscriber the appropriate signalling channels are ciphered and Temporary Subscriber Identity (TMSI) instead of IMSI is used over the radio path. At the time of initiating a service, the mobile terminal is powered on the subscriber may be required to enter a 4-8 digits Password Identification Number (PIN) to validate the ownership of the SIM. At the time of service provisioning the IMSI, the individual subscriber authentication key (Ki), the authentication algorithm (A3), the cypher key generation algorithm (A8) and the encryption algorithm (A5) are programmed into the SIM by the GSM operator. The A3 ciphering algorithm is used to authenticate each mobile by verifying the user password within the SIM with the cryptographic key at the MSC. The A5 ciphering algorithm is used for encryption. It provides scrambling for 114 coded bits sent in each TS. The A8 is used for ciphering keys. The IMSI and the secret authentication key (Ki) are specific to each mobile station, the authentication algorithms A3 and A8 are different for different networks and the operator's encryption algorithm A5 is unique and needs to be used across all GSM network operators. The authentication centre is responsible for all security aspects and its function is closely linked with HLR. The secret authentication key (Ki) is not known to mobile users and is the property of the service provider, the home system of the mobile station (MS) generates the random number say Rand which is a 126-bit number. This random number is sent to MS. The MS uses the A3 algorithm to authenticate the user. The algorithm A3 uses Ki and Rand numbers to generate a signed result called s_RES. MS sends s_RES to the home system of MS. In the home system authentication contains Ki and it also uses the same authentication algorithm A3 to authenticate the valid user. The A3 algorithm uses Ki and Rand generated by the home system to generate a signed result called 〖(s)〗_RES). The s_RES generated by MS and the authentication centre are compared. If both s_RES are identical only then the user is valid and access is granted otherwise no.

Code:

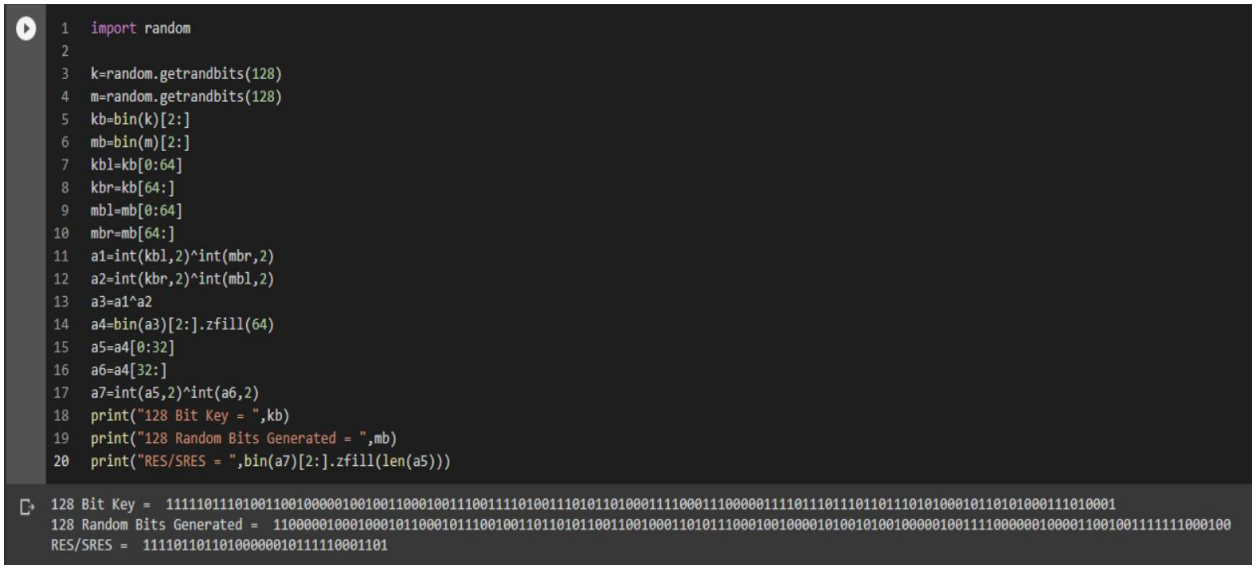
```
import random
k=random.getrandbits(128)
m=random.getrandbits(128)
kb=bin(k)[2:]
mb=bin(m)[2:]
```

kbl=kb[0:64]

```
kbr=kb[64:]
mbl=mb[0:64]
mbr=mb[64:]
a1=int(kbl,2)^int(mbr,2)
a2=int(kbr,2)^int(mbl,2)
a3=a1^a2
a4=bin(a3)[2:].zfill(64)
a5=a4[0:32]
a6=a4[32:]
a7=int(a5,2)^int(a6,2)
print("128 Bit Key = ",kb)
print("128 Random Bits Generated = ",mb)
print("RES/SRES = ",bin(a7)[2:].zfill(len(a5)))
```

GITHUB LINK: https://github.com/jayparekh1290/Mobile-Computing-Lab/blob/main/Exp%203%20(GSM%20A3).ipynb

OUTPUT:



```
import random

k=random.getrandbits(128)
m=random.getrandbits(128)
kb=bin(k)[2:]
mb=bin(m)[2:]
kbl=kb[0:64]
kbr=kb[64:]
mbl=mb[0:64]
mbr=mb[64:]
a1=int(kbl,2)^int(mbr,2)
a2=int(kbr,2)^int(mbl,2)
a3=a1^a2
a4=bin(a3)[2:].zfill(64)
a5=a4[0:32]
a6=a4[32:]
a7=int(a5,2)^int(a6,2)
print("128 Bit Key = ",kb)
print("128 Random Bits Generated = ",mb)
print("RES/SRES = ",bin(a7)[2:].zfill(len(a5)))
```

```
128 Bit Key =  11111011101001100100000100100110001001110011101001110101101000111100011100000111101110111011101101010001011010100011101000
128 Random Bits Generated =  11000001000100010110001011100100110110101100110010001101011100010010000101001010010000010011110000001000011001001111111000100
RES/SRES =  11110110110100000010111110001101
```

Conclusion: The experiment was about the GSM and it was successfully implemented using python on Google Colab it is verified and implemented successfully.