# Experiment No. 3

**AIM:** Write a program to show implementation of GSM security algorithms (A3/A5/A8). (Implement any one.)

**THEORY:**

The security procedures in GSM are aimed at protecting the network against unauthorized access and protecting the privacy of mobile subscriber against eavesdropping, eavesdropping on subscriber communication is prevented by ciphering the information. To protect identity and location of the subscriber the appropriate signaling 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 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 cipher key generation algorithm (A8) and the encryption algorithm (A5) are programmed into the SIM by 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 key. The IMSI and the secret authentication key (Ki) are specific to each mobile station, the authentication algorithm A3 and A8 are different for different networks and operator's encryption algorithm A5 is unique and needs to be used across all GSM network operators. The authentication center is responsible for all security aspects and its function is closely linked with HLR. The secret authentication key (Ki) is not known to mobile user and is the property of service provider, the home system of the mobile station (MS) generates the random number say Rand which is 126-bit number. This random number is sent to MS. The MS uses A3 algorithm to authenticate the user. The algorithm A3 uses Ki and Rand number to generate a signed result called s_RES. MS sends s_RES to 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 use Ki and Rand generated by home system to generate a signed result called 〖(s〗 _RES). The s_RES generated by MS and authentication center are compared. If both s_RES are identical only then the user is valid and access is granted otherwise no.

Algorithm of A3:

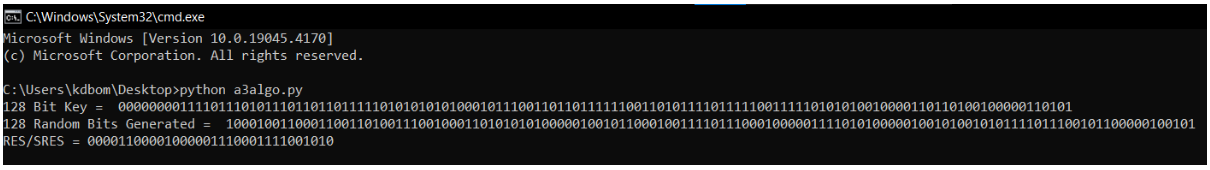
The first procedure of authentication is carried out by this algorithm. It is used to authenticate the identity of bothe the subscribers connected in the network. The keys are 128-bit and we use the RES algorithm of cryptography here to send the authentication information to each other.

## Program:

```
import random

k=random.getrandbits(128)

m=random.getrandbits(128)
```

```
kb=bin(k)[6:]

mb=bin(m)[4:]

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)))
```

**Outcome:**



```
Microsoft Windows [Version 10.0.19045.4170]
(c) Microsoft Corporation. All rights reserved.

C:\Users\kdbom\Desktop>python a3algo.py
128 Bit Key =  0000000011110111010111011011011111010101010100010111001101101111110011010111101111100111101010100100001101101001000001 10101
128 Random Bits Generated =  1000100110001100110100111001000110101010100000100101100010011110111000100000111101010000010010100101011110111001011000000100101
RES/SRES = 00001100001000001110001111001010
```

**Conclusion:**

The implemented program demonstrates the A3 authentication algorithm in GSM security. By generating random numbers and utilizing cryptographic operations, the algorithm produces a signed result (RES/SRES) used for mutual authentication between the mobile station and the home system. This experiment highlights the crucial role of A3 in verifying the identity of subscribers and ensuring secure access to GSM networks, thereby enhancing network security and protecting user privacy.