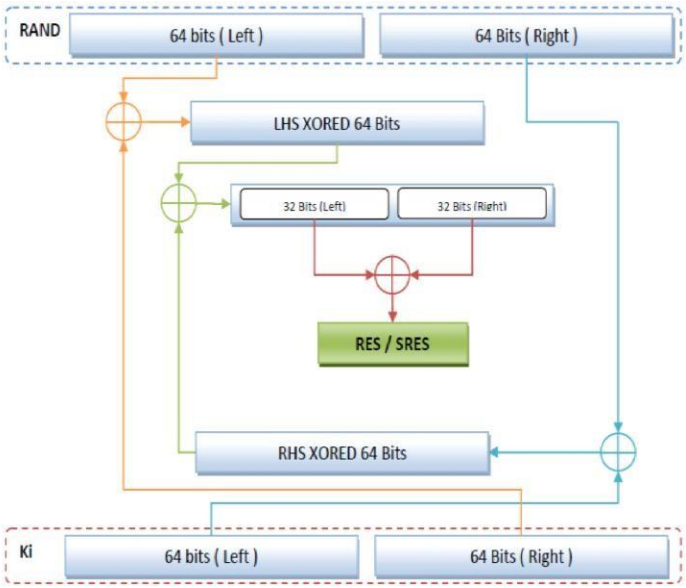
Experiment No. 08

Name-Rebecca Dias Roll No-19 BECMPN A PID-182027 Batch- 2

AIM: Implementation of GSM security algorithms (A3/A5/A8) THEORY:

Algorithm A3 is used for the authentication in the GSM cellular standard. Before a subscriber can use any service provided by the GSM network, he/she must be authenticated. This authentication is based on the SIM (Subscriber Identity Module), which stores the authentication key Ki, the user identification IMSI (International Mobile Subscriber Identity), and the algorithm used for this authentication i.e. A3. The authentication uses a challenge-response mechanism. The mobile station (MS) signs into the network. The access control (AC) generates a random number RAND as a challenge and the SIM within the MS answers with the SRES (Signed Response) as the response. The AUC (Authentication Centre) generates the random values of RAND, the signal response SRES and the cipher key Kc. This information is forwarded to the HLR (Home Location Register). The VLR (Visitor Location Register) requests the values of RAND, SRES, and Kc from the HLR. The VLR sends the RAND value generated to the SIM. On both sides, the network and the subscriber module, the same operation is performed between the 128 bit RAND and 128 bit Ki, called A3. SRES of 32 bit is generated on both sides. MS sends the SRES generated by the SIM to the VLR. Now VLR can compare both the SRES generated. If both are the same, the user or the subscriber is authenticated, otherwise rejected



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)))
```

OUTPUT:

```
128 Bit Key =
11001110010010100001011101011110110111000001000100111011110000000010010110100010100001110011100100100111111001001111111010011111101

128 Random Bits Generated =
10100001111010100011000010011110010101000011001010100000001101101111010010010001011000001101101110110101110101110100010000010010

RES/SRES = 01000101010010111101001100001101
```

CONCLUSION:

From this experiment we learnt about GSM that is global system for Mobile Communication and its security algorithms which are A3, A5, A8. We researched on A3 algorithm specifically which is used for the authentication in the GSM cellular standard and implemented it in Python to understand its significance.