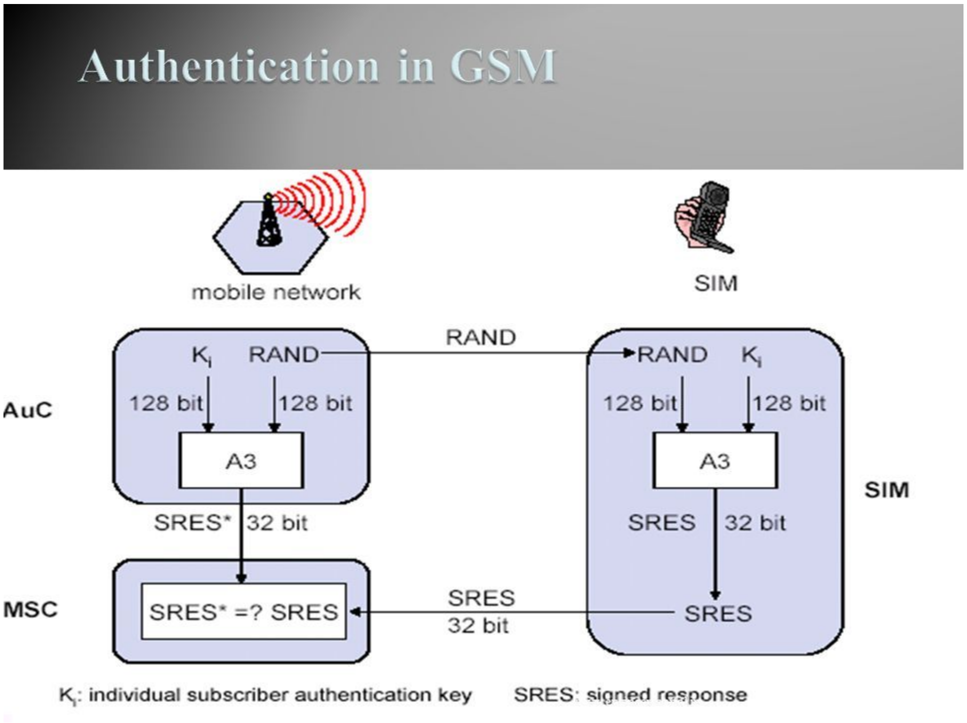
AIM: Implementation of GSM Algorithms (A3/A5/A8).

Theory:

1. The security procedures in GSM are aimed at protecting the network against unauthorized access and protecting the privacy of mobile subscriber against eavesdropping,
2. Eavesdropping on subscriber communication is prevented by ciphering the information.
3. To protect 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.
4. 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.
5. 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.
6. 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.
7. 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 operators encryption algorithm A5 is unique and needs to be used across all GSM network operators.
8. The authentication centre is responsible for all security aspects and its function is closely linked with HLR.
9. 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.
10. 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 centre are compared. If both s_RES are identical only then the user is valid and access is granted otherwise not.



Authentication in GSM

K_i: individual subscriber authentication key SRES: signed response

Fig 1. GSM Algorithms Used in Authentication.

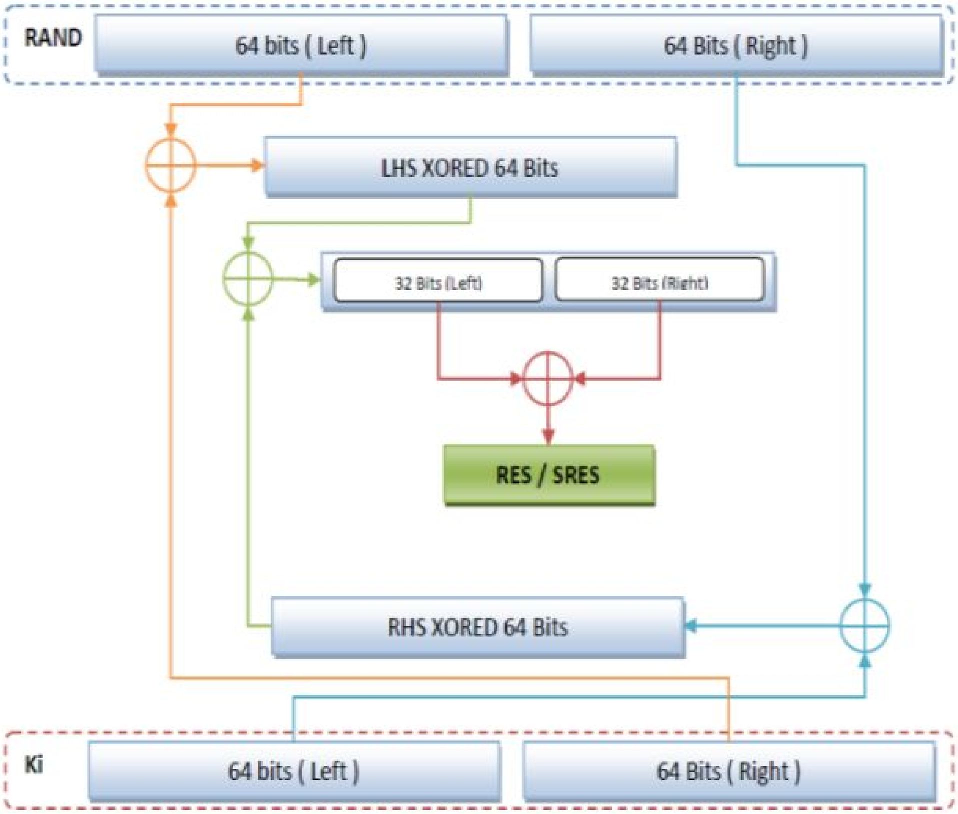


Fig 2. A3 Algorithm

CODE:

```
from functools import reduce


Fn = 1 << 22  # globally(publically) available frame number.


def split_n(num, n):
    ones = int('0b' + '1' * n, 2)
    lh = ones & num
    rh = (num - lh) >> n
    return lh, rh


def A3(rand, key):
    rand_l, rand_r = split_n(rand, 64)
    key_l, key_r = split_n(key, 64)
    l_xor = rand_l ^ key_r
    r_xor = rand_r ^ key_l

    final_xor = l_xor ^ r_xor
    res = reduce(int.__xor__, split_n(final_xor, 32))
    return res


if __name__ == '__main__':
    rand_no = 340282366920938463463374607431768211456
    key = 345282366920998463463374607431768211456
    print('Random Number:', rand_no)
    print('Key:', key)
    print('Output of A3 algorithm:', A3(rand_no, key))
```

OUTPUT :

```
Random Number: 340282366920938463463374607431768211456
Key: 345282366920998463463374607431768211456
Output of A3 algorithm: 3492679906
```