Universal College of Engineering, Kaman
Department of Computer Engineering
Subject: Mobile Computing

Experiment No: 5

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

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 algorithms (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 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 a mobile station (MS) generates a random number, say Rand which is a 126-bit number.This a 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 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.

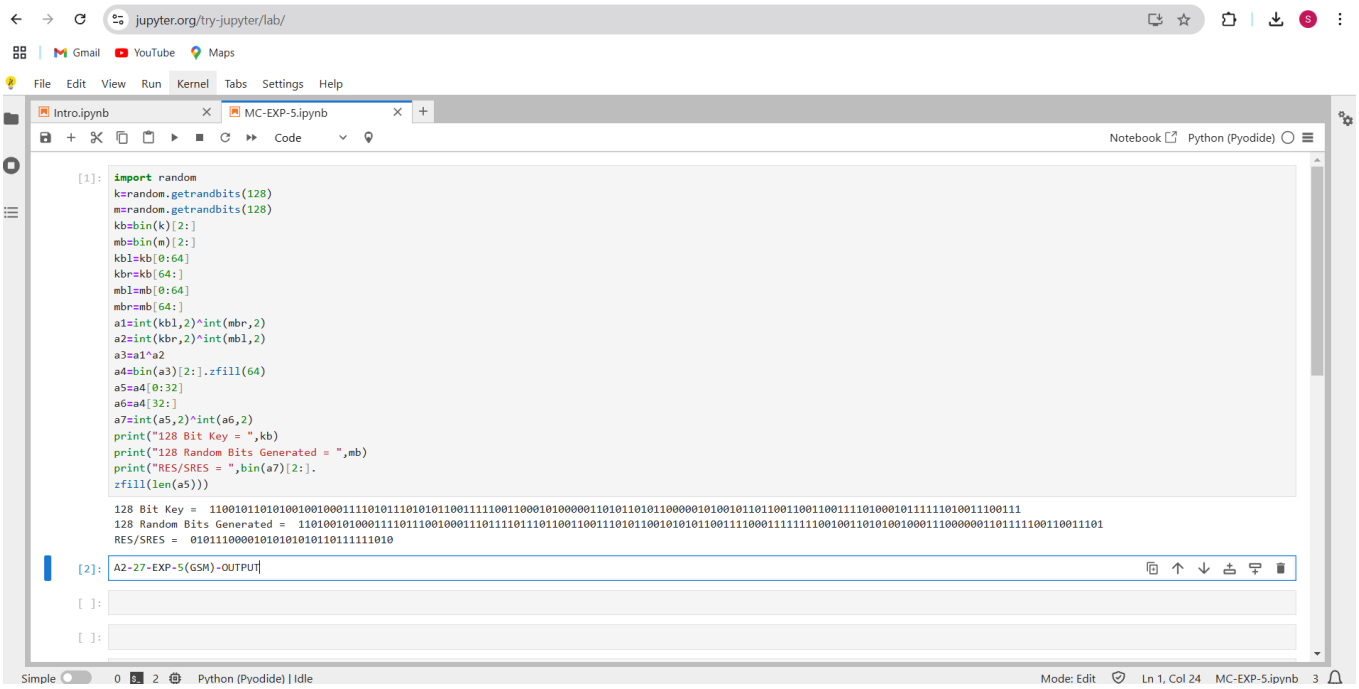
The A3 algorithm use Ki and Rand generated by home system to generate a signed result called 〖(s)〗 _RES). The s_RES generated by MS and authentication center are compared. If both s_RES are identical only then the user is valid and access is granted otherwise no.

Universal College of Engineering, Kaman
Department of Computer Engineering
Subject: Mobile Computing

Github Link :

https://github.com/sachinskill/MC-EXPERIMENTS/tree/main/EXP-5%20GSM

Screenshots of the Output:



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