Experiment No 3: GSM Security

# PART A

**(PART A: TO BE REFFERED BY STUDENTS)**

* 1. **Aim: To implement GSM security algorithms (A3/A5/A8)**
  2. **Objectives:** To understand the security algorithms in mobile networks
  3. **Outcomes:** Student will be able to implement security algorithms for mobile communication network. (LO-4)
  4. **Tools Used/programming language:** Java, Python etc

# Theory:

* + - Authentication verifies identity and validity of SIM card to the network and ensures that subscriber has access to the network.
    - Term used
      * Ki= **individual subscriber authentication key**, it is 32 bit number and present only in SIM card and stored in authentication center.
      * RAND= **random 128 bit number generated by AUC** (authentication center) when network request to authenticate the subscribers.
      * SRES (signed responses) = 32 bit crypto variable used in authentication process.
      * Kc = 64 bit cipher key.
    - MS is challenged by given RAND by the network.

# Security in GSM

* + **Three algorithms** have been specified to provide security services in GSM. **Algorithm A3** is used for **authentication**, **A5** for **encryption**, and **A8** for the **generation of a cipher key**.
  + In the GSM standard **only algorithm A5 was publicly available, whereas A3 and A8 were secret**, but standardized with open interfaces.
  + **Network providers can use stronger algorithms for authentication**– or users can apply stronger end-to-end encryption.
  + Algorithms A3 and A8 (or their replacements) are located on the SIM and in the AUC and can be proprietary.
  + Only A5 which is implemented in the devices has to be identical for all providers.

 **Subscriber Authentication**

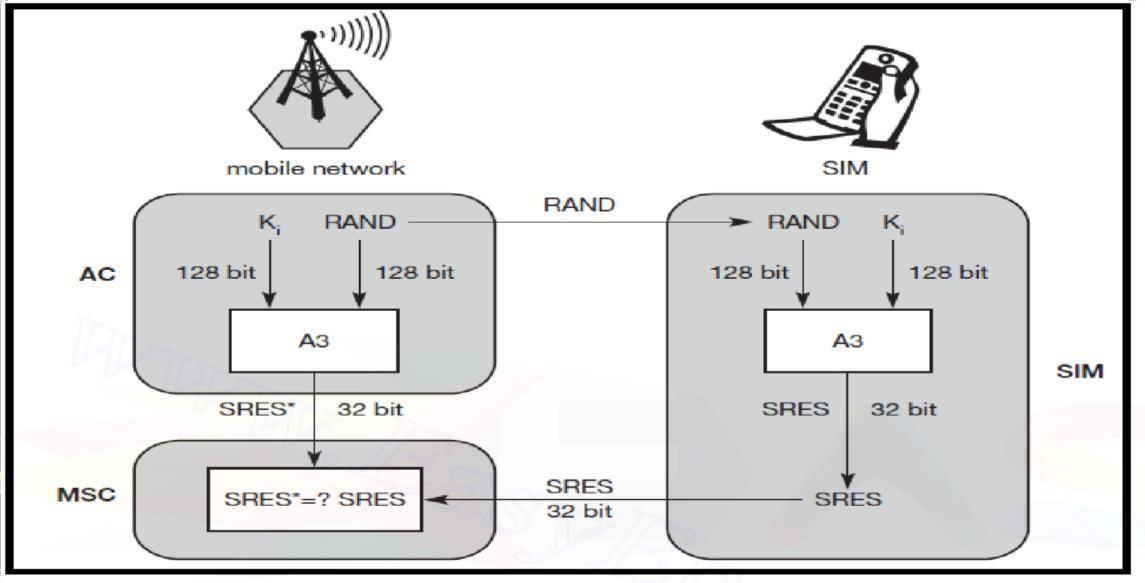
For subscriber authentication algorithm used is A3

1. A3 algorithm is inbuilt inside SIM and AUC, Input for A3 is Ki and RAND
2. Ki=Stored inside SIM(kiis encrypted inside SIM card) and not share on network and also present in AUC of MSC.
3. Before a subscriber can use any service from the GSM network, he or she must be authenticated. Authentication is based on the SIM, which stores the individual **authentication key Ki**, the **user identification IMSI**, and the algorithm used for

authentication **A3**.

1. When user want to access GSM network IMSI number from SIM send to MSC then HLR then to AUC.
2. Now AUC check IMSI number is present or not and identify associated Ki value (Ki is fixed), in this procedure AUC generate RAND number which is different for every new user request.
3. AUC using authentication algorithm A3(input to A3 are ki and RAND) calculate SRES as output of A3 and AUC using algorithm A8 of cipher generation (input to

A8 are ki and RAND) calculate Kcand send these SRES, Kc and RAND to HLR then from HLR to MSC. These three terms SRES, Kc and RAND are called as triplet.

1. MSC now send only RAND value to MS
2. MS using algorithm A3 (input to A3 is Ki and RAND)calculate SRES and using algorithm A8 calculate Kc and send these SRES and kc to MSC
3. MSC check SRES receive from MS and Network are same or not. If both are same user is authenticated and connection is set up.

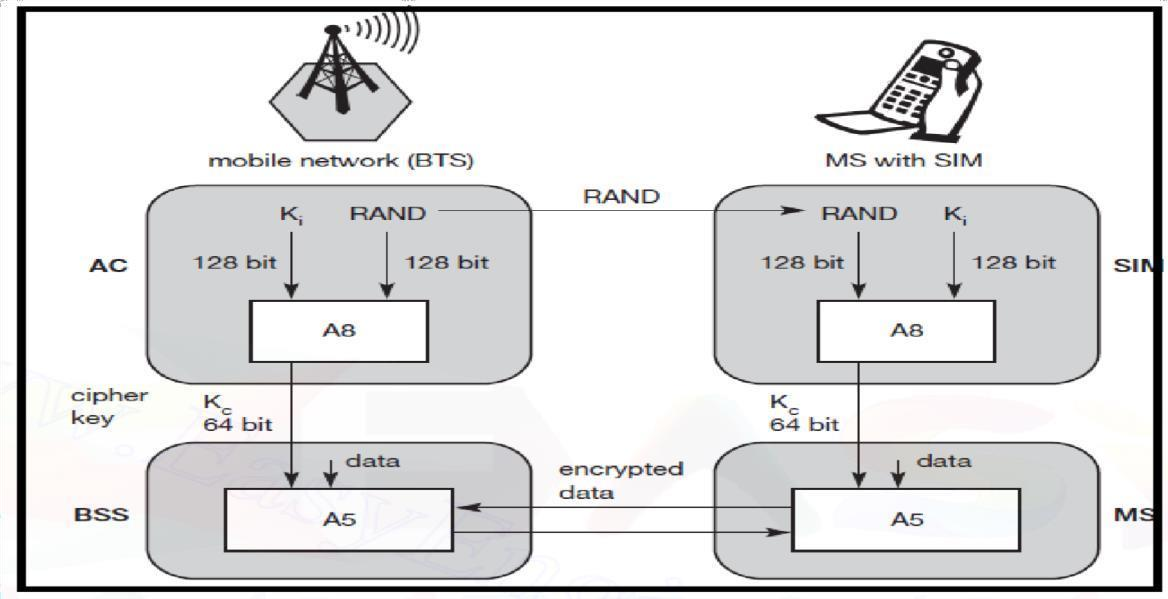
**Figure: Subscriber Authentication**

 ***Encryption***

* 1. To ensure privacy, all messages containing user-related information are encrypted in GSM over the air interface.
  2. After authentication, MS and BSS can start using encryption by applying the cipher key Kc
  3. Kc is generated using the individual key Ki and a random value by applying the algorithm A8. Note that the SIM in the MS and the network both calculate the same Kc based on the random value RAND. **The key Kc itself is not**

**transmitted over the air interface.**

* 1. MS and BTS can now encrypt and decrypt data using the algorithm A5andthe cipher key Kc. As Figure shows, Kc should be a 64 bit key – which is not very strong, but is at least a good protection against simple eavesdropping. However, the publication of A3 and A8 on the internet showed that in certain implementations 10 of the 64 bits are always set to 0, **so that the real length of the key is thus only 54 consequently**, the encryption is much weaker.
  2. Note: An **eavesdropping attack**, also known as a sniffing or snooping **attack**, is a theft of information as it is transmitted over a network by a computer, smart- phone, or another connected device. The **attack** takes advantage of unsecured network communications to access data as it is being sent or received by its user. **Eavesdropping** is the act of intercepting communications between two points.



**Figure: Data Encryption**

# Sample Source Code:

**https://**[**www.theprogrammingcodeswarehouse.com/2020/04/implementation-**](http://www.theprogrammingcodeswarehouse.com/2020/04/implementation-) **ofa3-security.html**

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)))

# A.6 Sample Output:

128 Bit Key

=1111101110100110010000010010011000100111001111010011101011010001111000111000001

111

011101110110111010100010110101000111010001

128 Random Bits Generated

=1100000100010001011000101110010011011010110011001000110101110001001000010100101

001

0000010011110000001000011001001111111000100

RES/SRES=11110110110100000010111110001101

# PART B

**(PART B: TO BE COMPLETED BY STUDENTS)**

|  |  |
| --- | --- |
| Roll No. B42 | Name: Vivek Billa |
| Class : TE-B | Batch : B2 |
| Date of Experiment | Date of Submission |
| Grade : |  |

# Question of Curiosity:

Q.1: Source Code

(Students need to implement GSM Security Algorithm using any programming language like Java, Python, etc)

def A3(key, rand):

return key[:32]

def A8(key, rand): return key[32:96]

def A5(key, plaintext): ciphertext = ""

for i in range(len(plaintext)):

ciphertext += str(int(plaintext[i]) ^ int(key[i % len(key)])) return ciphertext

def main():

print(" GSM Secuirity Algorithm \n\t Harshal Bade\n") # Example usage

# 128-bit key (Ki)

key = "0101010101010101010101010101010101010101010101010101010101010101"

# 128-bit random challenge

rand = "1100110011001100110011001100110011001100110011001100110011001100"

# 32-bit plaintext

plaintext = "10101010101010101010101010101010"

# Authentication using A3 sres = A3(key, rand) print("SRES:", sres)

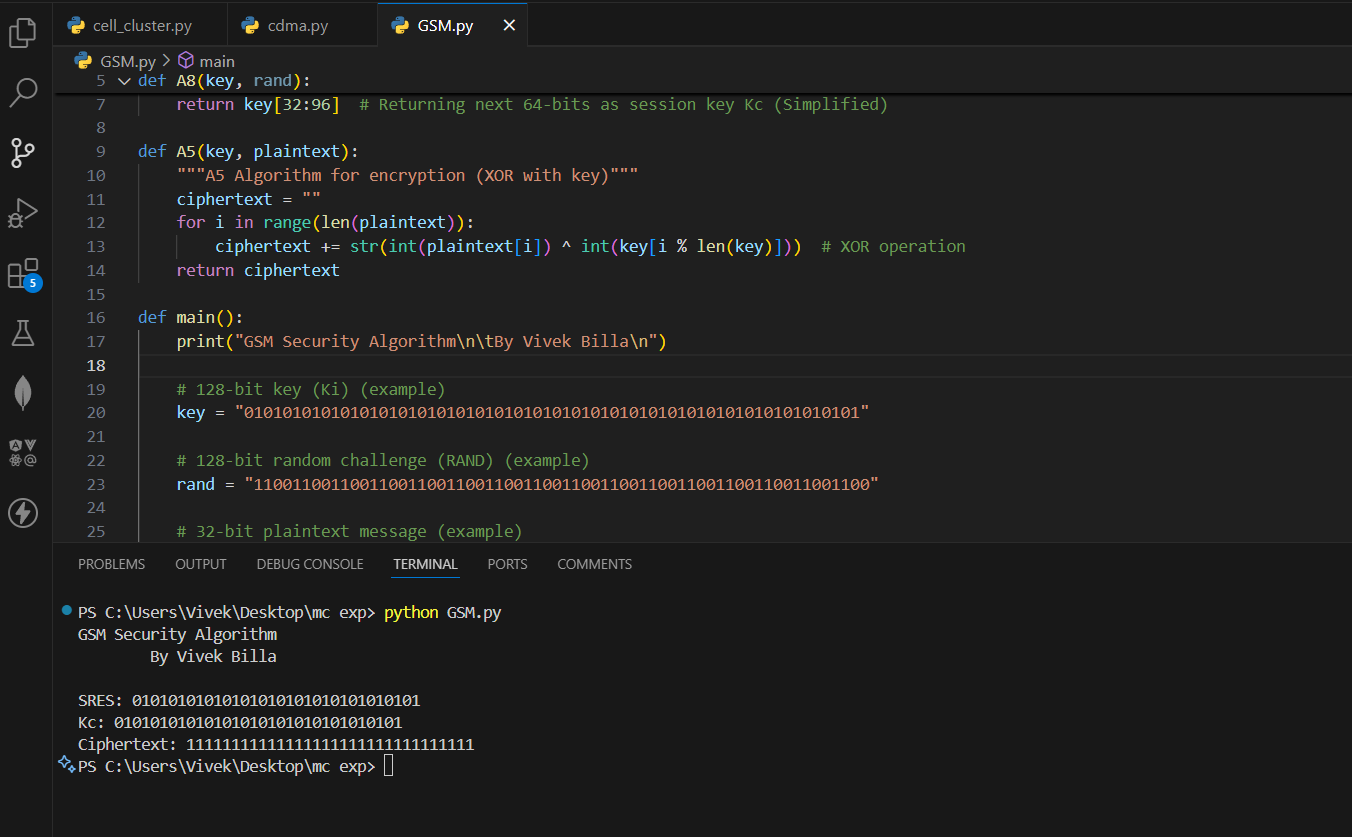
# Key generation using A8 kc = A8(key, rand)

print("Kc:", kc)

# Encryption using A5 ciphertext = A5(kc, plaintext) print("Ciphertext:", ciphertext)

if name == " main ": main()

Q.2: Output of GSM Security Algorithm



Q.3: List out various elements of GSM architecture and explain in brief function of each element**.** Ans:

GSM (Global System for Mobile Communications) architecture is a framework that defines the components and protocols used in mobile telecommunications networks. Here are the key elements of GSM architecture and their functions:

Mobile Station (MS):

* The mobile device used by subscribers to access the GSM network.
* Functions include initiating and receiving calls, sending and receiving SMS messages, and accessing data services.

Base Transceiver Station (BTS):

* Radio equipment responsible for communicating directly with the mobile station.
* Converts digital data into radio signals for transmission over the air interface.
* Manages radio frequency and power levels.

Base Station Controller (BSC):

* Controls multiple BTSs.
* Handles handovers between cells.
* Manages radio frequency resources.
* Controls power levels and handoff procedures. Mobile Switching Center (MSC):
* Central component responsible for call switching and mobility management.
* Manages connections between mobile users within the same network or between different networks.
* Handles call setup, call routing, and call termination.

Home Location Register (HLR):

* Central database that stores subscriber information and current location.
* Manages subscriber authentication, authorization, and mobility tracking.
* Provides information required for call routing and call setup.

Visitor Location Register (VLR):

* Temporary database that stores subscriber information when they roam into a different network.
* Contains information about subscribers currently within the coverage area of the serving MSC.

Gateway Mobile Switching Center (GMSC):

* Interfaces between the GSM network and other networks, such as the Public Switched Telephone Network (PSTN) or other mobile networks.
* Responsible for call routing between GSM and external networks.

Short Message Service Center (SMSC):

* Stores and forwards SMS messages.
* Manages SMS delivery and receipt.
* Interfaces with other messaging systems and networks.

# Conclusion:

We learned and successfully implemented the GSM security algorithm A3,A5,A8 using python.