Department of Computer Engineering Academic Term :

Jan-Apr 2023

Class : T.E Computer Sem -VI
Subject : Mobile Computing

Practical No:	**3**
Title:	To implement GSM Security Algorithm
Date of Performance:	17/02/2025
Date of Submission:	27/04/2025
Roll No:	9913
Name of the Student:	Mark Lopes

Evaluation:

Sr. No	Rubric	Grade
1	On time Completion & Submission(2)	
2	Output(3)	
3	Code Optimization(3)	
4	Knowledge of the topic(2)	
5	Total (10)	

Signature of the Teacher :

A.1 Aim: To implement GSM security algorithms(A3/A5/A8)

A.2 Objectives: To understand the security algorithms in mobile networks

A.3 Outcomes: Student will be able to implement security algorithms for mobile communication network.(LO-4)

A.4 Tools Used/programming language: Java, Python etc

A.5 Theory:

- Authentication verifies identity and validity of SIM card to the network and ensures that subscriber has access to thenetwork.
- Termused
  - ✓ 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 cipherkey.
    - 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 cipherkey**.

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 andRAND
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**.
4. When user want to access GSM network IMSI number from SIM send to MSC then HLR then toAUC.
5. 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. 6. 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 A8arekiandRAND)calculateKcandsendtheseSRES,KcandRANDtoHLR then from HLR to MSC. These three terms SRES, Kc and RAND are called as triplet.

7. MSC now send only RAND value toMS
8. 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 toMSC
9. MSC check SRES receive from MS and Network are same or not. If both are same user is authenticated and connection is setup.

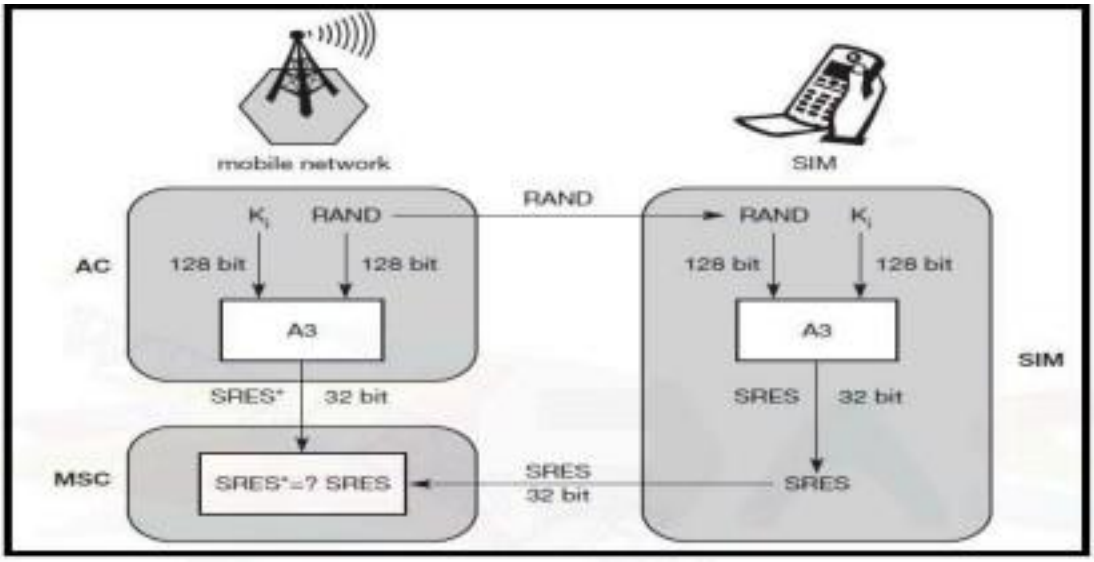

Figure: Subscriber Authentication

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 keyKc

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.**

4. MS and BTS can now encrypt and decrypt data using the algorithm A5 and the 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.

5. 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.

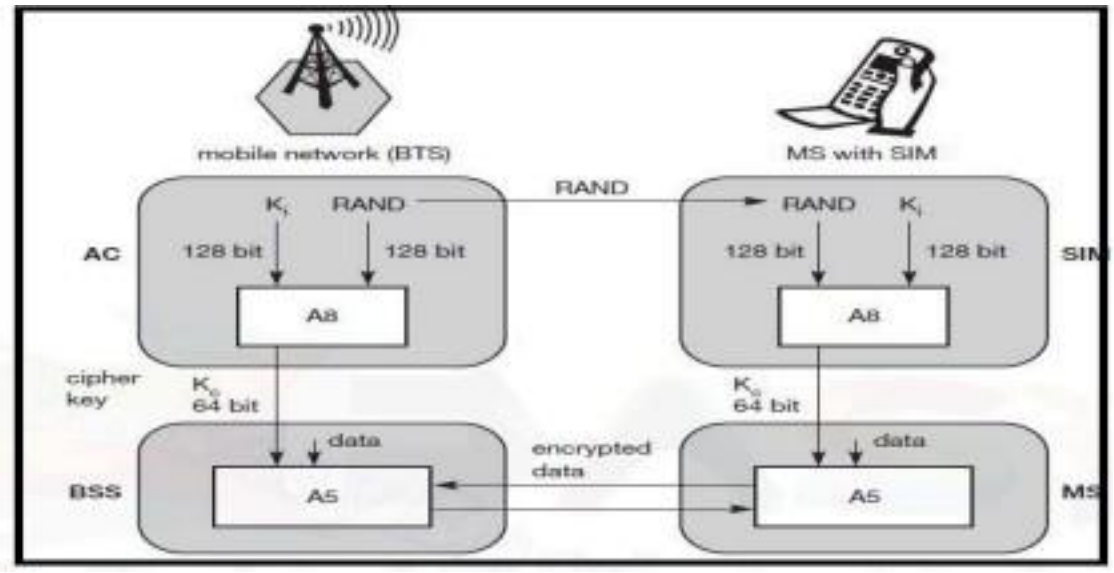

Figure: Data Encryption

A.6 Sample SourceCode:

https://www.theprogrammingcodeswarehouse.com/2020/04/implementation-of-a3-security.html

A.6 Sample Output:

A3 Algorithm

```
128-Bit Key (Ki): 11111011101001100100000100100110001001110011111010011101011010001111000111000001111011011
1101101110101000101101010001110100 01
128-Bit Random Bits (RAND): 11000001000100010111000101110010011011010110011001000110101110001001000010100101
1001000000100111100000100001100100111111100010
32-Bit Signed Response (SRES): 11010111100101001010010111010111
```

A5 Algorithm:

```
64-Bit Session Key (Kc): 1101011100101001011011100101101001010110010101011010101010101010
22-Bit Frame Number (FN): 1010101010101010101010
Plaintext: 1100110011001100110011001100
Keystream: 0000000000000000000000000000000000
Ciphertext: 1100110011001100110011001100
```

A8 Algorithm:

```
128-Bit Subscriber Key (Ki): 1111101110100110010000010010011000100111001111010011101011010001111000111000001
01111011101110111011010100010110101000111010001
128-Bit Random Challenge (RAND): 1100000100010001011000101110010011011010110011001000110101110001001000010
10010100100000010011110000010000110010011111110001000
64-Bit Session Key (Kc): 1101011110010100101001011101011101001100110100010111111000001001
```

POSTLAB:

17/02/25

MC Postlab lab 3

Observation for A3, A5, A8 algorithm.

1) A3 algorithm: (Authentication):-
Used to authorise a mobile to GSM network.
Involves sim card (containing unique authkey) and random no (RAND) generated by authentication centre.

2) A5 algorithm :- (Encryption):-
Responsible for encryption of data between mobile device and the base station to ensure confidentiality.

3) A8 algorithm :- (Key generation)
Generate a session key for ~~generating~~ encrypting voice and data during a session.