A3/A8 Security Algorithms in GSM

Nikhil Kumar

Information Technology, SRH University,
Heidelberg
nikhil.kumar@stud.hochschule-heidelberg.de

Abstract— **The A3A8 algorithm is a cryptographic algorithm used in GSM (Global System for Mobile Communications) networks to authenticate and secure communication between mobile devices and the network. The A3 algorithm is responsible for generating the authentication key (Ki) based on the user's SIM card information and a secret key stored in the mobile device. This authentication key is then used by the A8 algorithm to produce a session key (Kc), which is employed for encrypting and decrypting user data during communication with the network.**

General Terms* — *Security, Algorithm, Authentication, GSM, Response, Service, Mobile station

Keywords* — *GSM, Security, A3 algorithm, SRES, Kc, Ki.

Software Used* — *MATLAB and Simulink

I. Introduction

Mobile network is the shared media and any user of the media can intercept the network. When the media are shared, anyone can listen to or transmit on the media. Thus communication is no longer private. When media are shared, privacy and authentication are lost unless some method is established to regain it. Cryptography provides the mean to regain control over privacy and authentication. A variety of security algorithms are used to provide authentication, cipher key generation, integrity and radio link privacy to users on mobile networks. The GSM Security Model is based on a shared secret between the subscriber's home network's HLR and the subscriber's SIM. The shared secret, called Ki, is a 128-bit key used to generate a 32-bit signed response, called SRES, to a Random Challenge, called RAND, made by the MSC, and a 64- bit session key, called Kc, used for the encryption of the over-the-air channel. GSM uses three different security algorithms called A3, A5, and A8. Algorithm A3 is used for authentication, A5 is used for encryption, and A8 is used for the generation of a cipher key. In practice, A3 and A8 are generally implemented together (known as A3/A8). An A3/A8 algorithm is implemented in Subscriber Identity Module (SIM) cards and in GSM network Authentication Centres. A3 and A8 are derivation functions implemented as part of the COMP128 algorithm.

II. Block Diagram

A3 Algorithm:

The A3 is the authentication algorithm in the GSM security model. Its function is to generate the SRES response to the MSC's random challenge, RAND, which the MSC has received from the HLR. The A3 algorithm gets the RAND from the MSC and the secret key Ki from the SIM as input and generates a 32-bit output, which is the SRES response. Both the RAND and the Ki secret are 128 bits long. (Figure 1)

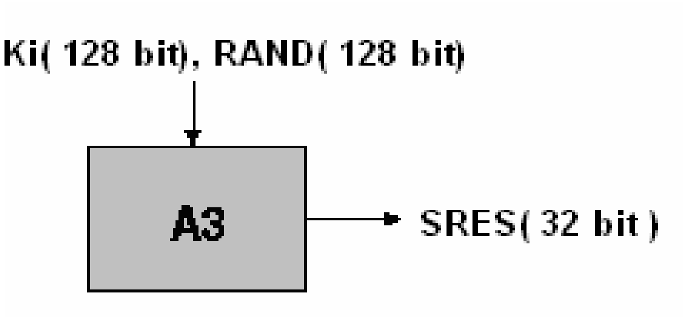


Fig. 1 Signed response (SRES) calculation

A8 Algorithm:

The A8 algorithm is the key generation algorithm in the GSM security model. The A8 generates the session key, **Kc**, from the random challenge, RAND, received from the MSC and from the secret key Ki. The A8 algorithm takes the two 128-bit inputs and generates a 64-bit output from them. This output is the 64-bit session key Kc.(See Figure 2). The BTS received the same Kc from the MSC. HLR was able to generate the Kc, because the HLR knows both the RAND and the secret key Ki, which it holds for all the GSM subscribers of this networkoperator. One session key, Kc, is used until the MSC decides to authenticate the MS again. This might take days.

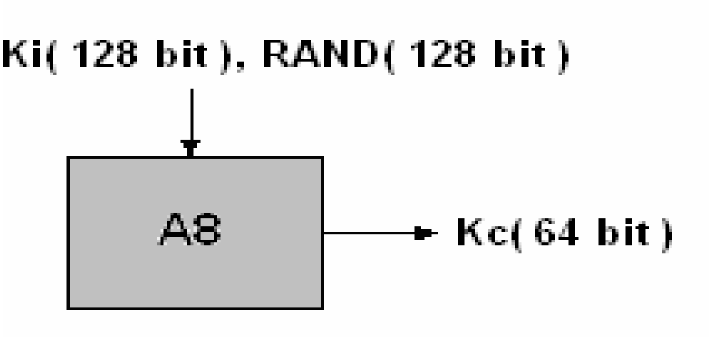


Fig.2 Session key (Kc) calculation

Nearly every GSM operator in the world uses an algorithm called COMP128 for both A3 and A8 algorithms. COMP128 is the reference algorithm for the tasks pointed out by the GSM Consortium. Other algorithms have been named as well, but almost every operator uses the COMP128 except a couple of exceptions. The COMP128 takes the RAND and the Ki as input, but it generates 128 bits of output, instead of the 32-bit SRES. The first 32 bits of the 128 bits form the SRES response.

The COMP128 is used for both the A3 and A8 algorithms in most GSM networks. The COMP128 generates both the SRES response and the session key, Kc, on one run. The last 54 bits of the COMP128 output form the session key, Kc, until the MS is authenticated again. See Figure 3. Note that the key length at this point is 54 bits instead of 64 bits, which is the length of the key given as input to the A5 algorithm.
Ten zero-bits are appended to the key generated by the COMP128 algorithm. Thus, we have a key of 64 bits with the last ten bits zeroed out. This effectively reduces the key space from 64 bits to 54 bits. This is done in all A8 implementations, including those that do not use COMP128 for key generation, and seems to be a deliberate feature of the A8 algorithm implementations .

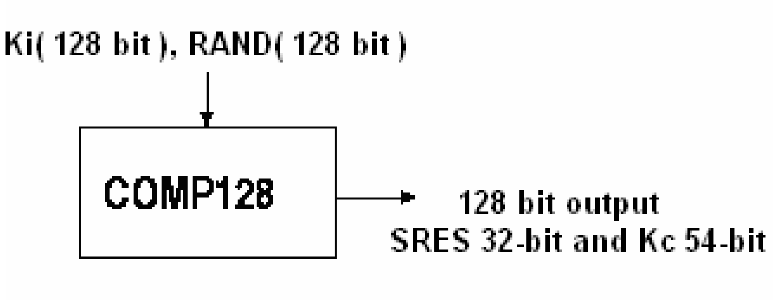


Fig.3 Comp128(Combination of A3/A8)

Both the A3 and A8 algorithms are stored in the SIM in order to prevent people from tampering with them. This means that the operator can decide, which algorithms to use independently from hardware manufacturers and other network operators. The authentication works in other countries as well, because the local network asks the HLR of the subscriber's home network for the five triples. Thus, the local network does not have to know anything about the A3 and A8 algorithms used.

III. Methodology

The proposed algorithm of security enhances the authentication of the user who is trying to communicate via the mobile device. The 128 bit RAND and the 128 bit Ki are present at both ends i.e. on the SIM as well as in the mobile network.

A3 Algorithm (Authentication Algorithm):

A. Initialization

When a mobile device attempts to access the GSM network, the network generates a random number called RAND as a challenge

B. Key Generation

The mobile device retrieves its International Mobile Subscriber Identity (IMSI) from the SIM card. Both the GSM network and the mobile device independently apply the A3 algorithm using the IMSI and a secret key (stored on the SIM card) to generate an Authentication Key (Ki).

C. Challenge Response(SRES)

The GSM network sends the RAND to the mobile device. The mobile device applies the A3 algorithm using the RAND and the Authentication Key (Ki) to generate a response called SRES.

D. Authentication

The mobile device sends its generated response 'SRES' back to the GSM Network The GSM network independently applies the A3 algorithm using the received RAND and its own copy of the Authentication Key (Ki) to generate its own SRES.
If the two SRES values match, authentication is successful, and the mobile device is granted access to the network.

A8 Algorithm (Key Generating Algorithm):

A. Initialization

After successful authentication, the A8 algorithm is used to generate a session key (Kc) for secure communication.

B. Key Generation

Both the GSM network and the mobile device independently apply the A8 algorithm using the same Authentication Key (Ki) generated by the A3 algorithm. The A8 algorithm outputs the session key (Kc).

C. Secure Communication

The generated session key (Kc) is used for encrypting and decrypting communication between the mobile device and the GSM network. This session key ensures the confidentiality and integrity of user data during the communication session.

The A3 algorithm is primarily concerned with verifying the legitimacy of the mobile device through the generation and comparison of SRES values. The A8 algorithm is focused on generating a session key (Kc) that is used for secure communication after successful authentication. The use of secret keys and random challenges ensures that only legitimate devices with valid SIM cards and associated secret keys can access the GSM network. This methodology guarantees the security and integrity of user communications within the GSM network, protecting against unauthorized access and ensuring privacy.

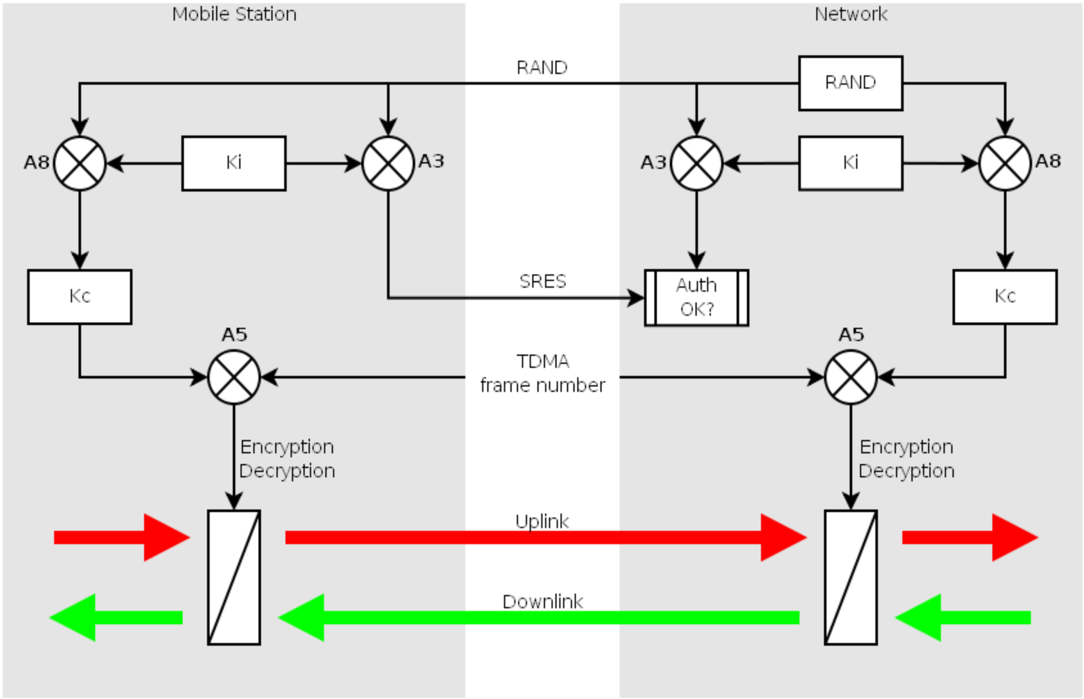
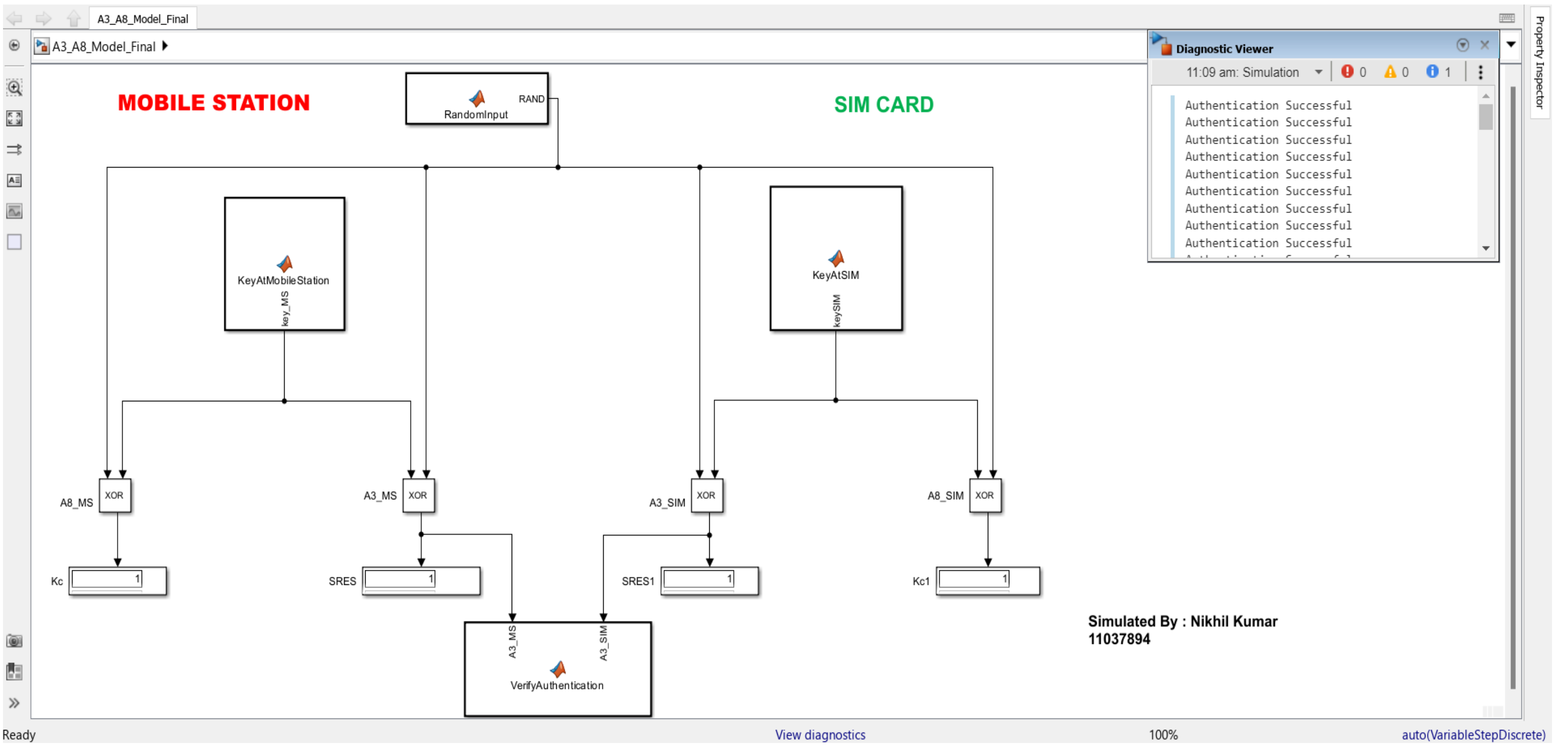


Fig.4 Architecture of A3/A8 Algorithm

IV. Simulation



```
Authentication Successful
Authentication Successful
Authentication Successful
Authentication Successful
Authentication Successful
Authentication Successful
Authentication Successful
Authentication Successful
Authentication Successful
```

Fig.4 Architecture of A3/A8 Algorithm

V. RESULTS

Result of A3 Algorithm : (A3 generates SRES for authentication)
The primary result of the A3 algorithm is the generation of a value called SRES (signed response). SRES is a 32-bit number derived from the combination of the RAND (random challenge number) and the Authentication Key (Ki).SRES is used for authentication purposes. The mobile device calculates its own SRES, and the GSM network verifies it against the expected SRES to authenticate the device.

Result of A8 Algorithm : (A8 generates Kc for securing communication)
The A8 algorithm is used for generating a session key called Kc (Cipher Key).Kc is a 64-bit key used for encrypting the communication between the mobile device and the GSM network. Both the mobile device and the network independently apply the A8 algorithm using the same Authentication Key (Ki) generated by the A3 algorithm to derive the session key Kc.

Below is the Result for MATLAB Code:

```
Enter the 128 bit binary Key at Mobile Station:
111111111111111111111111111111111111111111111111111111111111111111111111111111111111111111111111111111
111111111111111111111111111111111111111111111111111111111111111111111111111111111111111111111111111111
111111111111111111111111111111
A3 Result at Mobile Station - The first 32 bit is SRES :
  Columns 1 through 41
0  0  0  1  0  0  1  0  0  1  0  0  1  1  1  0  0  1  0  0  0  0  1  1  0  1  1  1  0  1  0  1  0  0  1  0  1  0  0  1  1
  Columns 42 through 82
1  1  1  0  0  0  0  1  0  1  0  1  0  1  0  0  0  0  0  1  1  0  0  0  1  0  0  1  0  0  1  0  0  1  0  0  0  0  1  1  0
  Columns 83 through 123
0  1  1  1  1  1  0  1  1  1  1  1  1  1  1  1  1  1  1  0  1  0  1  1  1  1  1  1  1  1  1  1  0  0  0  1  1  1  0  1  1
  Columns 124 through 128
1  1  1  0  1

A8 Result at Mobile Station - The last 54 bit appended with zeros is Kc :
  Columns 1 through 41
0  0  0  1  0  0  1  0  0  1  0  0  1  1  1  0  0  1  0  0  0  0  1  1  0  1  1  1  0  1  0  1  0  0  1  0  1  0  0  1  1
  Columns 42 through 82
1  1  1  0  0  0  0  1  0  1  0  1  0  1  0  0  0  0  0  1  1  0  0  0  1  0  0  1  0  0  1  0  0  1  0  0  0  0  1  1  0
  Columns 83 through 123
0  1  1  1  1  1  0  1  1  1  1  1  1  1  1  1  1  1  1  0  1  0  1  1  1  1  1  1  1  1  1  1  0  0  0  1  1  1  0  1  1
 Columns 124 through 128
1  1  1  0  1
```

```
Enter the 128 bit binary Key at SIM :
11111111111111111111111111111111111111111111111111111111
11111111111111111111111111111111111111111111111111111111
1111111111111111
A3 Result at Subscriber End- The first 32 bit is SRES :
  Columns 1 through 41
0  0  0  1  0  0  1  0  0  1  0  0  1  1  1  0  0  1  0  0  0  0  1  1  0  1  1  1  0  1  0  1  0  0  1  0  1  0  0  1  1
Columns 42 through 82
1  1  1  0  0  0  0  1  0  1  0  1  0  1  0  0  0  0  0  1  1  0  0  0  1  0  0  1  0  0  1  0  0  1  0  0  0  0  1  1  0
Columns 83 through 123
0  1  1  1  1  1  0  1  1  1  1  1  1  1  1  1  1  1  1  0  1  0  1  1  1  1  1  1  1  1  1  1  0  0  0  1  1  1  0  1  1
Columns 124 through 128
1  1  1  0  1

A8 Result at Subscriber End - The last 54 bit appended with zeros is Kc :
  Columns 1 through 41
0  0  0  1  0  0  1  0  0  1  0  0  1  1  1  0  0  1  0  0  0  0  1  1  0  1  1  1  0  1  0  1  0  0  1  0  1  0  0  1  1
Columns 42 through 82
1  1  1  0  0  0  0  1  0  1  0  1  0  1  0  0  0  0  0  1  1  0  0  0  1  0  0  1  0  0  1  0  0  1  0  0  0  0  1  1  0
Columns 83 through 123
0  1  1  1  1  1  0  1  1  1  1  1  1  1  1  1  1  1  1  0  1  0  1  1  1  1  1  1  1  1  1  1  0  0  0  1  1  1  0  1  1
Columns 124 through 128
 1  1  1  0  1

Authentication Successful
```

VI. CONCLUSIONS

The A3/A8 algorithm pair has been a fundamental component of the security infrastructure in GSM (Global System for Mobile Communications) networks for several years. The algorithms play a critical role in ensuring the security of communication between mobile devices and the network. The A3/A8 algorithm pair has been a core component of GSM security since the introduction of the GSM standard. Its long-standing implementation attests to its reliability and suitability for securing mobile communication.

FUTURE SCOPE:

A3/A8 algorithms may need to integrate seamlessly with emerging technologies such as Internet of Things (IoT) devices, artificial intelligence, and machine learning, considering the diverse and interconnected nature of modern communication systems.

REFERENCES

[1] BRUMLEY, B. (2004) A3/A8 AND COMP128, T-79.514 ,SPECIAL COURSE ON CRYPTOLOGY, PP.1–18. WWW.TCS.HUT.FI/STUDIES/T-79.514/SLIDES/S5.BRUMLEY-COMP128.PDF
[2] MUSHEER AHMAD AND IZHARUDDIN, SECURITY ENHANCEMENTS IN GSM CELLULAR STANDARD, 978-1-4244-3328-5/08/$25.00 ©2008 IEEE.
[3] JOCHEN SCHILLER, MOBILE COMMUNICATIONS SECOND EDITION, 96-122.
[4] SAXENA, NEETESH AND CHAUDHARI, NARENDRA, SECURE ALGORITHMS FOR SAKA PROTOCOL IN THE GSM NETWORK
[5] YONG LL, YIN CHEN, TIE-JUN MA, SECURITY IN GSM.
[6] JOCHEN SCHILLER, MOBILE COMMUNICATIONS SECOND EDITION, 96-122.

ANNEXURE

```
% GSM A3_A8 Algorthim
clear;
clc;
% A3 algorithm at Mobile Station

key_MS = input('Enter the 128 bit binary Key at Mobile Station: '); % 128-bit key
randNum = randi([0, 1], 1, 128);  % 128-bit random number

SRES_MS = xor(key_MS, randNum);

% Display A3 result
disp('A3 Result at Mobile Station - The first 32 bit is SRES :');
disp(SRES_MS);


% GSM A8 algorithm Mobile Station
Kc_MS = xor(key_MS, randNum);

% Display A8 result
disp('A8 Result at Mobile Station - The last 54 bit appended with zeros is Kc :');
disp(Kc_MS);

%==========================================================================
% A3 algorithm at Subscriber Identification Module (SIM)

key_Sim = input('Enter the 128 bit binary Key at SIM : '); % 128-bit key

SRES_Sim = xor(key_Sim, randNum);

% Display A3 result
disp('A3 Result at Subscriber End- The first 32 bit is SRES :');
disp(SRES_Sim);

% GSM A8 algorithm Mobile Station
Kc_Sim = xor(key_Sim, randNum);

% Display A8 result
disp('A8 Result at Subscriber End - The last 54 bit appended with zeros is Kc :');
disp(Kc_Sim);

%To check the authentication

if (SRES_MS==SRES_Sim)
    disp('Authentication Successful');
    else
    disp('Authentication Not Successful');
end
```