Mobile Communication Security using Encryption and Decryption

Uzmasaman Aejaz Chanderki

Trainee Engineer, Prasar Bharti, All India Radio, Mumbai.

Abstract - *We live in a world where there are many secret agencies, one of them are secret organization which taps our telephonic calls. Over a million mobile phones of different service provider are under the surveillance of a central organization in India. Our private and important conversation over phones is recorded. This privacy can be secured by a security system. The proposed system is a security solution which will retain and if necessary the conversation can be made accessible to the Government using Authentication protocol and Cryptography.*

Keywords- Mobile Communication, Base Station, RF signal, Transmitter, Receiver, Antenna, Cryptography, Encryption, decryption, AES, CHAP, Authentication protocols.

1. INTRODUCTION

Privacy of our data is a major concern nowadays. But private conversations are no private anymore. Over more than 6000 mobile phones are tapped in New Delhi. The information obtained through this can be misused against anyone. We never know what are the intention of the hackers are. According to a law under the general provision of section 5 of the India Telegraph Act. Due to this provision it mobile tampering is held at large extends.

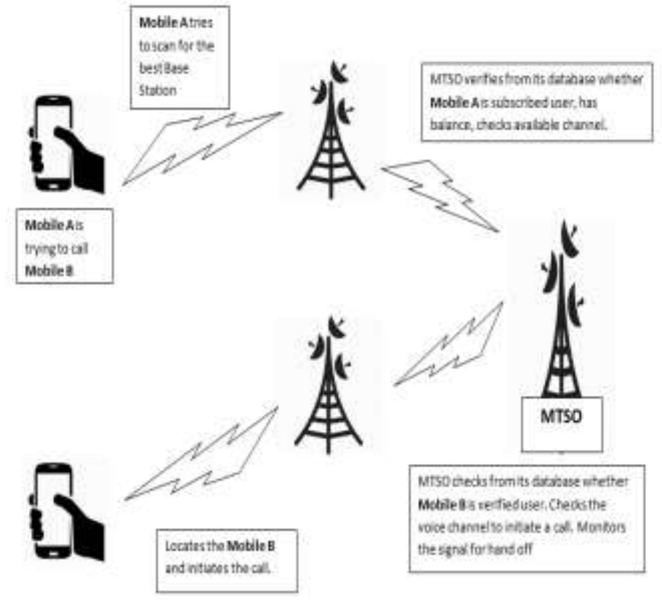

Mobile A tries to scan for the best Base Station
MTSO verifies from its database whether Mobile A is subscribed user, has balance, checks available channel.
Mobile A is trying to call Mobile B
MTSO
MTSO checks from its database whether Mobile B is verified user. Checks the voice channel to initiate a call. Monitors the signal for hand off
Locates the Mobile B and initiates the call.

Fig: 1.1 Ordinary Mobile Communications.

An ordinary mobile communication working starts with Mobile A calling Mobile B. the both can be anywhere in this world. When **A** starts calling it scans for the best cell. The base station further informs MTSO. MTSO verifies the SIM card number, balance available, checks available channel. If channel capacity is full then call drops or the call is initiated. MTSO also checks the same factors of B as it checked for **A**. If everything is clear it troughs the voice channel between these two mobiles and rings the Mobile B. Here the voice transmitted is not encrypted and secured. It can be tampered, misused or manipulated by the hacker.

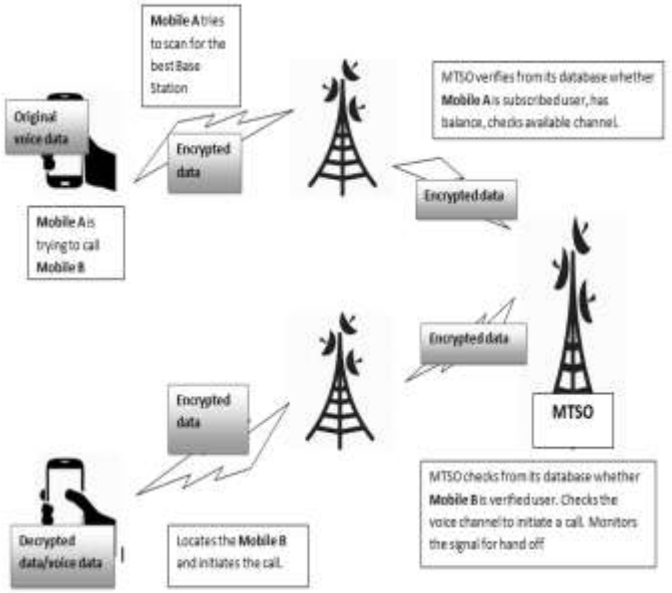

Mobile A tries to scan for the best Base Station
Original voice data
Encrypted data
MTSO verifies from its database whether Mobile A is subscribed user, has balance, checks available channel.
Encrypted data
Mobile A is trying to call Mobile B
Encrypted data
Encrypted data
MTSO
MTSO checks from its database whether Mobile B is verified user. Checks the voice channel to initiate a call. Monitors the signal for hand off
Decrypted data/voice data
Locates the Mobile B and initiates the call.

Fig: 1.2 Required Mobile Communications.

The required system should be designed in such a way that the original voice data should only be with the people who are communicating. Rest of the data transmission should in encrypted form so that even if a hacker breaks in he won't be able to understand or decode the data. Such strong encryption is done by Advance Encryption Standard. Even though the data is encrypted the voice data will still can be accessed by Government only through strong authentication protocol known as CHAP.

2. EXISTING MOBILE COMMUNICATION PROCESS

This block diagram is a general transmitter. The speech signal is given to microphone. The audio signal which is the output of microphone is given to the Preamplifier which boosts the level of the modulating signal. The local oscillator generates carrier signal which is modulated with the modulating signal in a Modulator. The power amplifier increases the power of signal makes it powerful enough to be transmitted.

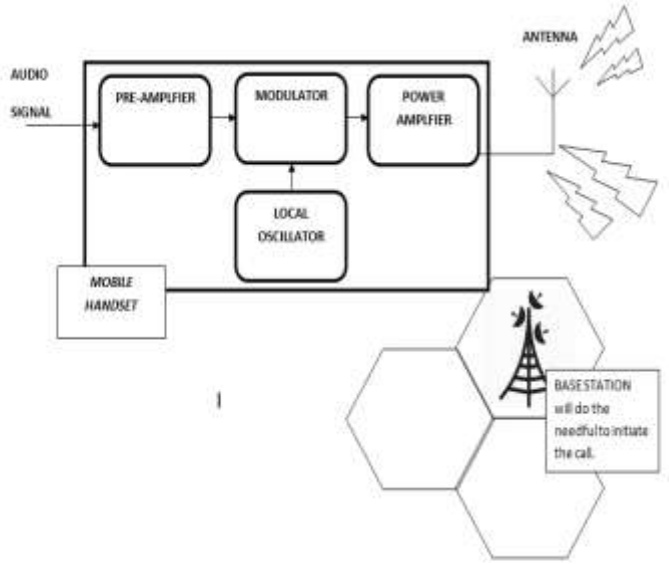


Fig 2.1 General block diagram of a transmitter.

The RF signal is then given to the antenna. This system has no security. The data flow is as it is easy for hackers to break in.

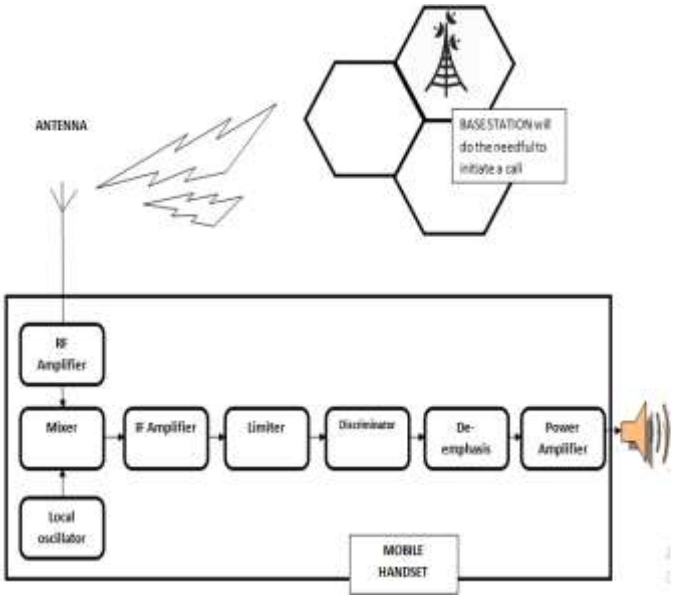


Fig: 2.2 General block diagram of a receiver

RF signal received will be amplified in an RF amplifier. Mixer is a nonlinear circuit which will mix the amplified RF signal and local frequency to produce intermediate frequencies. The signal is then limited and demodulated send to the speaker after power boosting. Hence in the entire process we didn't see any cryptography and the data is out there without any security.

3. PROPOSED SYSTEM.

The working of the new transmitter and receiver will be same but 2 new blocks will be added to increase the security.

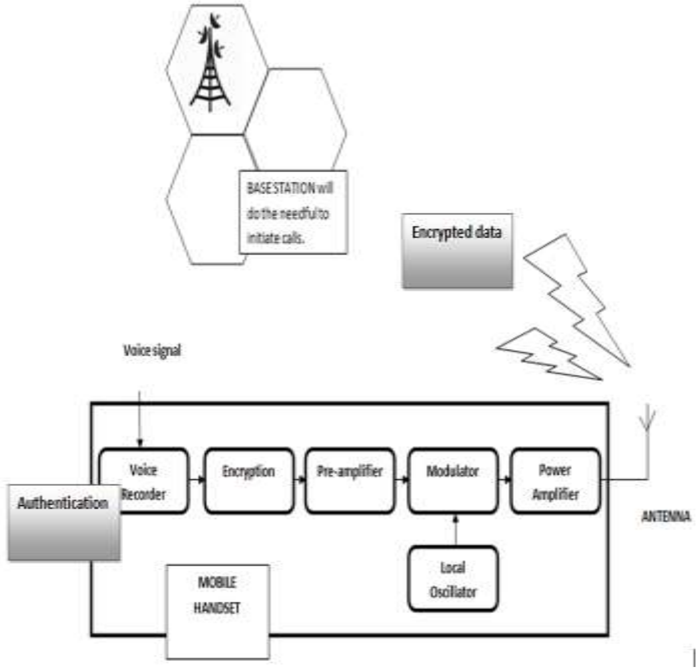


Fig: 2.3 Secured transmitter using Encryption

Voice recorder block is kept for legal purposes. Only Government official will have the correct authentication to access the voice recorder as and when it is needed. So that the data's originality is preserved even though it is encrypted. Authentication protocol which will be used is CHAP. Challenge Handshake Authentication Protocol is a more secure procedure for connecting to a system. The output of the voice recorder will be given to encryption which will use AES.

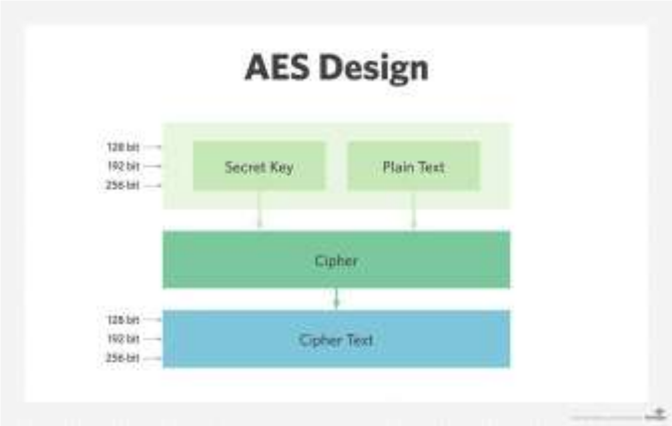


Fig: 2.4 AES Design

256-bit encryption is a data or file encryption technique that makes use of a 256-bit key to encrypt and decrypt data or files. It is one of the most secure and strongest encryption methods after 128- and 192-bit encryption, and is used in most modern encryption algorithms, protocols and technologies including AES and SSL. It can encrypt folder, file, mp3, audio even a single sentence. After encryption the operation will be same as previous process. An encrypted RF waves will be sent on air which will be protected from hackers.

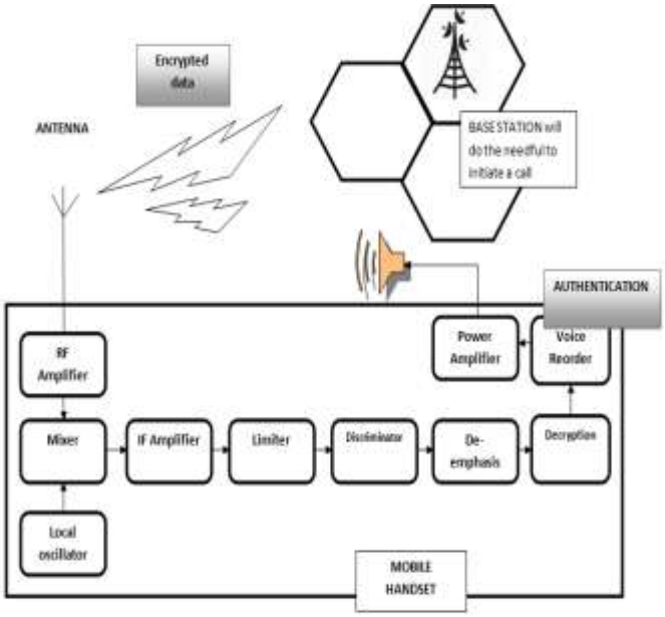
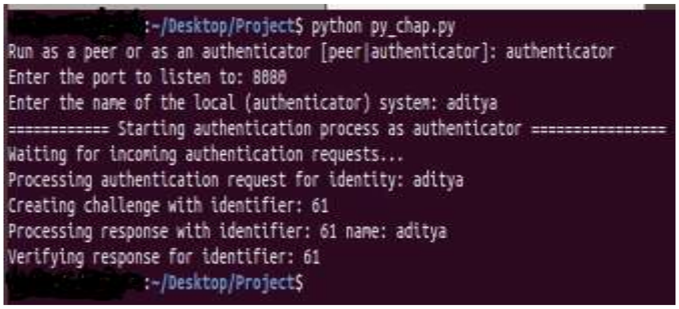


Fig: 2.4 Secured Receivers.

In receiver when encrypted signal is process in reversed way of transmitter we get the same result signal we had at the starting point of transmitter after encryption. This same signal is decrypted again recorded. It is then given to speaker of the receiver handset.

4. RESULT

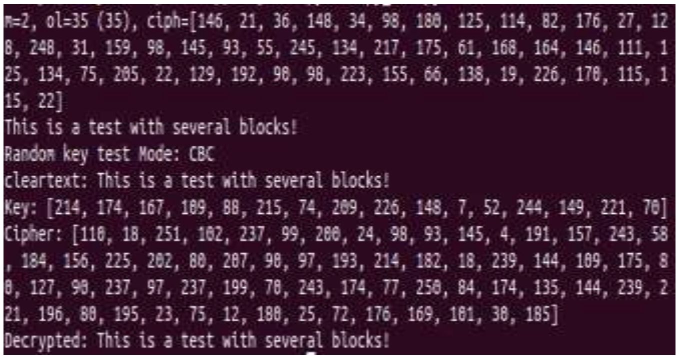
CHAP Authentication protocol which will protect the authenticity of voice recorded and its access.



```
[redacted]:~/Desktop/Project$ python py_chap.py
Run as a peer or as an authenticator [peer|authenticator]: authenticator
Enter the port to listen to: 8080
Enter the name of the local (authenticator) system: aditya
=========== Starting authentication process as authenticator ===============
Waiting for incoming authentication requests...
Processing authentication request for identity: aditya
Creating challenge with identifier: 61
Processing response with identifier: 61 name: aditya
Verifying response for identifier: 61
[redacted]:~/Desktop/Project$
```

Fig: 4.1 CHAP Authentication. (prototype)

AES encryption and decryption which are used in transmitter and receiver.



```
m=2, ol=35 (35), ciph=[146, 21, 36, 148, 34, 98, 180, 125, 114, 82, 176, 27, 12
8, 248, 31, 159, 98, 145, 93, 55, 245, 134, 217, 175, 61, 168, 164, 146, 111, 1
25, 134, 75, 205, 22, 129, 192, 90, 98, 223, 155, 66, 138, 19, 226, 170, 115, 1
15, 22]
This is a test with several blocks!
Random key test Mode: CBC
cleartext: This is a test with several blocks!
Key: [214, 174, 167, 109, 88, 215, 74, 209, 226, 148, 7, 52, 244, 149, 221, 70]
Cipher: [110, 18, 251, 102, 237, 99, 200, 24, 98, 93, 145, 4, 191, 157, 243, 58
, 184, 156, 225, 202, 80, 207, 90, 97, 193, 214, 182, 18, 239, 144, 109, 175, 8
0, 127, 90, 237, 97, 237, 199, 70, 243, 174, 77, 250, 84, 174, 135, 144, 239, 2
21, 196, 80, 195, 23, 75, 12, 180, 25, 72, 176, 169, 101, 30, 185]
Decrypted: This is a test with several blocks!
```

Fig: 4.2 AES Encryption & Decryption (prototype)

5. CONCLUSION

This proposal is simple, practical yet cost effective. Hardware changes are minimal and affordable by every service provider, mobile handset manufacturer. This system can be made even more secured by adding stronger protocol. Such systems are needed when highly confidential conversation will take place like VVIP person, military and so on. This can be implemented in telephone, data call, voice calls.

REFERENCES

[1] P. Carroll, B. Fortz, M. Labbe, and S. McGarraghy, "Improved Formulations for the Ring Spur Assignment ´ Problem," in INOC 2011, Hamburg, Germany, pp. 24–36, 2011.

[2] A. Merwaday and I. Guvenc, "UAV assisted heterogeneous networks for public safety communications," in IEEE Wireless Communications

and Networking Conference Workshops, pp. 329–334, 2015.

[3] Understanding GPS: Principles and Applications (Artech House Telecommunications Library), Elliott D. Kaplan (Editor) / Hardcover / (1996)

[4] Alex Fares,”GSM systems engineering and network management,” 2003.

[5] O. Fagbohun, "Comparative studies on 3G, 4G and 5G wireless technology," IOSR Journal of Electronics and Communication Engineering, vol. 9, pp. 88-94, 2014

[6] J. M. Keenan, A. J. Motley, Personal communication radio coverage in buildings at 900 MHz and 1700 MHz, ElectronicsLetters, 24(12), 1988, 763 – 764.

[7] D. C. Cox, 910 MHz urban mobile radio propagation: Multipath characteristics in New York City, IEEE Transactions on VehicularTechnology, 22(4), 1973, 104-110.

[8] T. S. Rappaport, S. Y. Seidel, Path loss prediction in multi floored buildings at 914MHz. ElectronicsLetters, 27(15), 1991, 1384-1387.

[9] V. Duan, Electrocardiographicartifactdueto a mobile phone mimicking ventricular tachycardia. Journal of Electrocardiology, 47 (3), 2014, 33–34.

[10] M. Periyasamy, andR. Dhanasekaran, Evaluation of electromagnetic interference between critical medical devices and new generation cellular phones. Journal of MicrowavePowerEnergy, 49 (3), 2015, 160–70.