IJCSE International Journal of Computer Sciences and Engineering Open Access
Technical Paper Vol.-6, Issue-6, June 2018 E-ISSN: 2347-2693

Applications of Stream ciphers in wireless communications

Y.Nagendar[1], V. Kamakshi Prasad[2], Allam Appa Rao[3], G.Padmavathi[4*]

[1,4] CRRAO AIMSCS,HCU Campus, Hyderabad
[3]Chairman of NATIONAL INSTITUTE OF Technical TEACHERS TRAINING AND RESEARCH, Chennai
[2] Department of Computer Science, JNTUCEH, Hyderabad

*Corresponding Author:padmagvathi@gmail.com,Tel:9848271485

Available online at: www.ijcseonline.org

Accepted: 09/Jun/2018, Published: 30/Jun/2018

Abstract**—** Stream ciphers are widely used in wireless communications to transforms the data and delivers through wireless channel. This paper presents various stream ciphers used for data encryption in different wireless communication technologies. The main purpose of this paper is to provide information on various stream ciphers used in wireless communications.

Keywords**—** Stream Ciphers, Wireless Communications, GSM, Bluetooth, WEP

I. INTRODUCTION

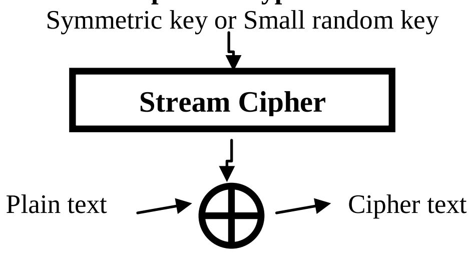
Wireless communications is a kind of transfer of information which is implemented and delivered wireless. This is a wide-ranging term that includes all processes and forms of fixing and communicating through wireless communication technologies among two or more devices using a wireless signal. Wireless communication has various forms, technology and delivery methods, the main important communications are Satellite communication, Mobile communication, Wireless network communication, Infrared communication and Bluetooth communication. Information security has widely increased due to the sensitivity of the exchange of information over public communication channels specifically mobile devises. Mobile devices are commonly used for communication. Advancement of mobile technology have contributed significantly in increasing popularity of mobile phones in our modern lifestyle. Due to this, mobile devises are using to send and receive important information like social security numbers, bank account details and passwords. Mobile phone communication uses the stream cipher encryption algorithms.

This paper is organized as follows, Section I contains the introduction of stream ciphers in wireless communications Section II contain the information about stream cipher Section III contain stream ciphers in wireless communications Section IV more stream ciphers in next generations section V conclusion and future work.

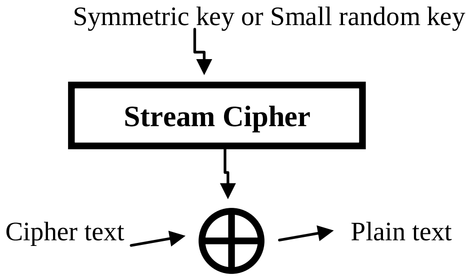
II. STREAM CIPHER

Stream cipher is a symmetric key algorithm which uses same key for encrypting plain text and decrypting cipher text. There are two kinds of symmetric key algorithm, that is, stream cipher and block cipher. But stream ciphers encrypt plain text bit by bit using XOR operation but block cipher divides the plaintext by blocks which encrypt and decrypt each block independently. Comparatively Stream cipher is faster than block cipher. Stream cipher is a pseudo random generator using secret key. Stream cipher produces same pseudorandom sequence for particular key, so secret key is same for both encryption and decryption.

A. Stream Cipher encryption:



B. Stream Cipher decryption:



III. STREAM CIPHERS IN WIRELESS COMMUNICATIONS

Wireless technologies use stream ciphers as one of the security system for their secure communication. Stream ciphers are frequently utilized for their speed and flexibility of usage in equipment, and in applications where message comes in amounts of mysterious length like a secure wireless connection. In a stream cipher, the same key always produces the same keystream. Hence, repeated use of the same key is just as bad as reusing a one-time pad. One of the approach to handle this problem is to renew the secret key from time to time. But this involves key exchange overhead. An alternative remedy is the use of initialization vectors.

A. RC4

The RC4 stream cipher was designed by Ron Rivest for RSA Data Security firm in 1987 as a propriety algorithm. In 1994, it was allegedly revealed on the internet. It is used for encrypting the internet traffic in network protocols such as Secure Sockets Layer (SSL), Transport Layer Security (TLS), and Wired Equivalent Privacy (WEP), Wi-Fi Protected Access (WPA) etc. The cipher is also used in Microsoft Windows, Lotus Notes, Apple Open collaboration Environment (AOCE), and Oracle Secure SQL. The RC4 encryption algorithm is used by standards such as IEEE 802.11 within WEP (Wireless Encryption Protocol) using 40 and 128-bit keys ([1], [2]).

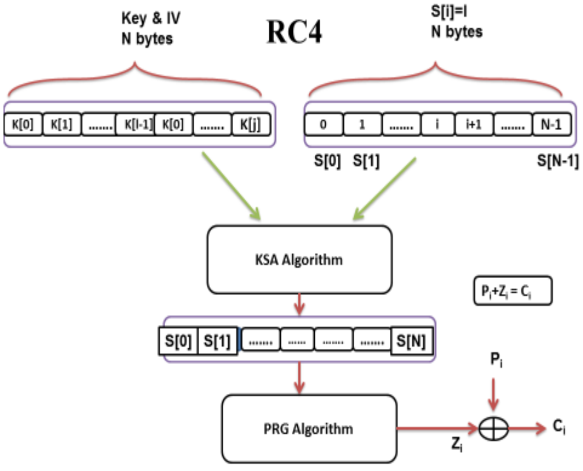


Figure 1 RC4 encryption process

RC4 algorithm has the following specifications:

Two phases of algorithm	Key scheduling Algorithm (KSA)and PRNG
Key size	1-256 bytes. Usually 40 bits.
Computational complexity	2^{13} or 2^{33}
Linear Feedback Shift Registers (LFSR)	No LFSR but byte manipulation
Word based or bit	Word - 8 bits or byte by byte

The Key Scheduling Algorithm (KSA): The KSA uses the key K to shuffle the elements of S

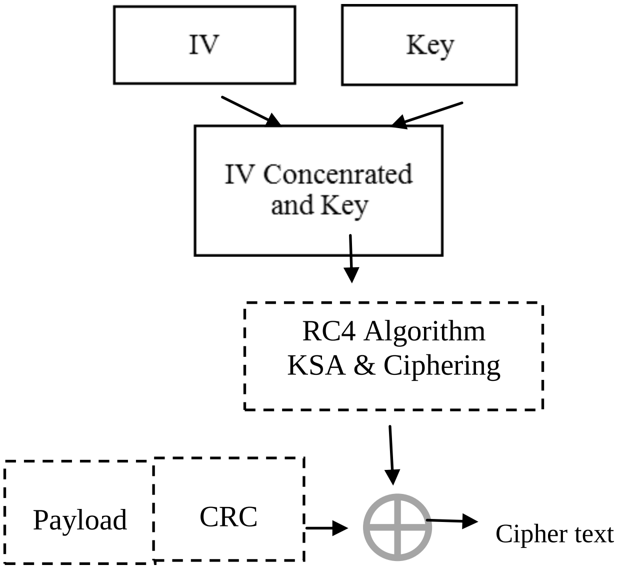
```
Input: Secret key array $K[0.....N-1]$
Output: Scrambled permutation array $S[0...N-1]$
Initialization:
for $i = 0,1,...,N-1$ do
    $S[i] = i;$
    $j = 0;$
end
Scrambling:
for $i = 0,1,...,N-1$ do
    $j = (j + S[i] + K[i]);$
    $Swap(S[i], S[j]);$
end
```

The Pseudo-Random Generation Algorithm (PRGA): The PRGA uses this scrambled permutation to generate pseudo-random keystream bytes.

```
Input: Key-dependent scrambled permutation array $S[0.....N-1]$
Output: Pseudo-random keystream bytes $z$.
Initialization:
    $i = j = 0$
Keystream generation loop:
$i = i + 1;$
$j = (j + S[i]);$
$Swap(S[i], S[j]);$
$t = S[i] + S[j];$
Output $z = S[t];$
```

In a WEP (Wired Equivalent Privacy is a protocol for encoding wirelessly transmitted packets on IEEE 802.11 networks) protected network, using the stream cipher RC4 under a common key all packets are encrypted. The following figure illustrates that the data encryption procedure using RC4 from wireless station to access point ([3]).

At Wireless Station:



At Access point: Each bit of cipher text XOR with the key stream coming from RC4 algorithm, we get payload with CRC (Cyclic redundancy check).

For secure communication WEP uses RC4 algorithm and RC4 encrypt data byte by byte. Due to this, the whole data packet must be dispose if one bit is lost. So that the sender need to resend the lost data packet again and again until the receiver accept the data packet, and WEP must reset the initial vector (IV)after transmitting each data packet. To overcome this problem improved RC4 was discussed in [4] and [5] .Application of Rc4 for wireless local area networks (WLAN) was discussed in [6].

B. A5/1 ,A5/2 and A5/3 in GSM standards

A5/1, A5/2 and A5/3 stream cipher used in data encryption to provide security in the GSM cellular telephone standard. Figure-2 (GSM link in references) shows the encryption process in GSM.

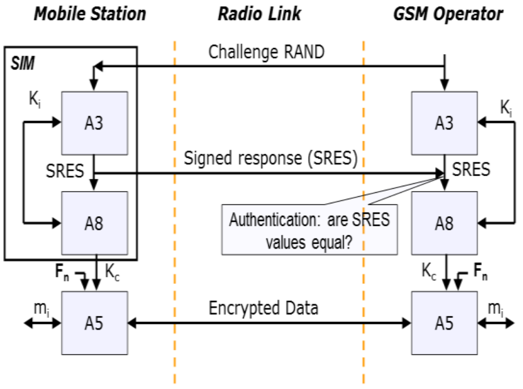
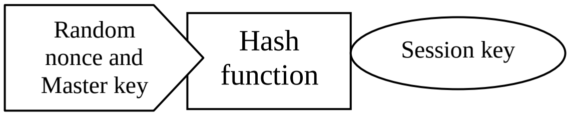


Figure 2 Encryption process in GSM

The A3 algorithm for authentication, A8 for key generation and A5 for data encryption. Master key shared between Operator and phone to derive session key.

Session key: Session key is generated by applying hash functions to Random nonce and Master key.



A5/1(A5/2 or A5/3) algorithm used in data encryption with session key, in the following figure-3 one can understand the role of A5/1(A5/2 or A5/3) in communications from base station to cell phone.

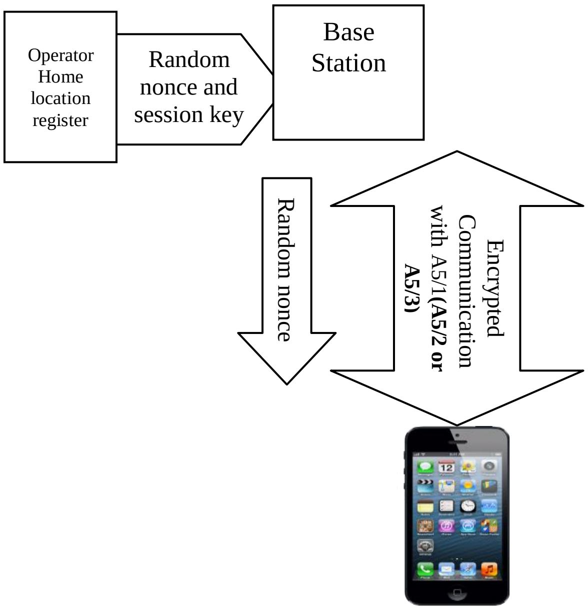

Operator Home location register
Random nonce and session key
Base Station
Random nonce
Encrypted Communication with A5/1(A5/2 or A5/3)

Figure 3 Role of A5/1 in communications from base station to cell phone

A5/1 is robust comparing with A5/2 and the countries who are members of CEPT (European Conference of Postal and Telecommunications Administrations). The GSM Memorandum of Understanding (MoU) controls the use of these (A5/1 and A5/2) algorithms. A5/3 is a key stream generator based on block cipher Kasumi algorithm that is defined by the 3rd Generation Partnership Project (3GPP) at 2002. It can be supported on dual-mode phones that are capable of working on both 2G and 3G systems ([7],[8]).A summary of GSM network and cryptanalysis of A5(A5/1 and A5/2) cipher were discussed in Ross Anderson 1998, [9],[10],[11],[12] and [13].Improved A5/1 cipher based image encryption procedure with image bit plane separation to improve the security of image data communicated over wireless network was discussed in [14].

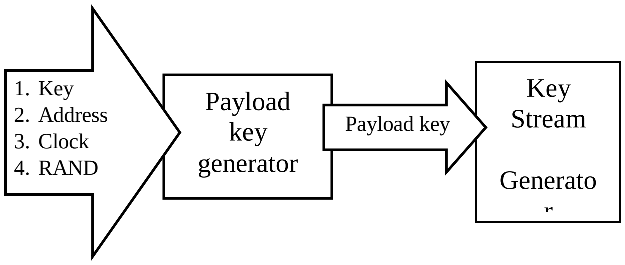
GSM data encryption algorithm has the following specifications:

	A5/1	*A5/2*	*A5/3*
two phases of algorithm	Key scheduling Algorithm (KSA)and PRNG	Key scheduling Algorithm (KSA)and PRNG	Inside kasumi block cipher
Key size	*64 bit*	*64 bit*	*64 bit*
Computational complexity	4/3(2^{23}-1)	2^{17}	2^{76}
Linear Feedback Shift Registers (LFSR)	3LFSR with irregular clocking	4LFSR with irregular clocking	Inside kasumi block cipher
Word based or bit	bit	bit	bit

C. Stream cipher E0 in Blue tooth

Bluetooth security mechanism involves, encryption, authentication and key management functions in Link layer ([15],[16]). It uses E0, E1, E2and E3 algorithms. 4 bit PIN entered by the user produces Link key applying E2 algorithm which is then used by the E3 algorithm to generate the encryption key. Then the key stream generated by E0 algorithm along with the encryption key is used to encrypt the plaintext to generate the cipher text.

The following figure shows the Stream Cipher System E0



E1 for authentication algorithm, E2 for key generating algorithm. Following figure ([17]) shows the encryption process in Bluetooth.

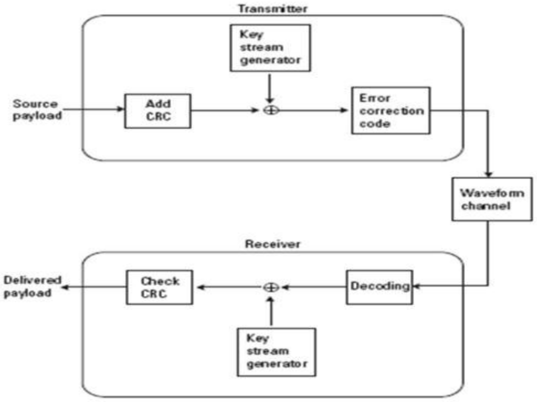


Figure 4 Encryption process in Bluetooth

IV. MORE STREAM CIPHERS IN NEXT GENERATIONS

SNOW 3G has been designed for the use as the base algorithm for the second set of 3GPP confidentiality and integrity algorithms ([18]). SNOW 3G, a word oriented stream cipher which generates a pseudorandom sequence of 32-bit words using 128-bit key and a 128-bit initialization variable. Initially a key initialization is executed, that is the cipher is clocked without producing output, and produces a 32-bit word of output ([19], [20]). SNOW 3G involves two interacting components, a Linear Feedback Shift Register (LFSR) and a Finite State Machine (FSM).It is used in 4G LTE networks. The ZUC algorithm involves a LFSR which produces *m*-sequences over the prime field GF (2^{31}-1) as basis of the algorithm, which is extensively differ from stream ciphers that are based on *m*-sequences over the finite field GF(2) or its extension field GF(2^n).ZUC also used in LTE network([21]). Espresso is a stream cipher can use in 5G wireless communication systems, whose 1-bit per cycle version has 1497 GE area, 2.22 Gbits/sec throughput and 232 ns latency, meeting needs of most 5G applications in future. Link Encryption Algorithm (LEA) is a word based stream cipher used for transformation on Pentium IV processor ([22]).In [23] Mahdi Madani et.al. 2017, discussed Improved LTE Stream Cipher which is Snow-3G Based on Hyperchaotic PRNG. More information about GSM standards were discussed in [24], [25], and [26]. Algorithms for voice and packet encryptions were discussed in [27].Cryptography automatic key generation was discussed in [28] and [29].

Algorithms for voice encryption:

Algorithm		Application
A5/1	Un weakened	GSM encryption algorithm
A5/2	weakened version of A5/1	GSM encryption algorithm
A5/3	KASUMI	3G
A5/4	SNOW3G	4G LTE networks
A5/0	No encryption	GSM

Algorithms for packet data encryption:

Algorithm			Application
GEA/1	64 bit key,96 bit state-Broken	proprietary stream cipher	GSM GPRS/EDGE/3G/4G
GEA/2	64 bit key,125 bit state-Broken	proprietary stream cipher	GSM GPRS/EDGE/3G/4G
GEA/3	64 bit key,128 bit state-limited break	KASUMI	GSM GPRS/EDGE/3G/4G
GEA/4	128 bit key,128 bit state	KASUMI	GSM GPRS/EDGE/3G/4G
GEA/0	No encryption, sake of completeness		GSM

V. Conclusion and Future Scope

In this paper, various stream Ciphers Used in Wireless communication technogies, that is, RC4 in WEP and WLAN, A5/1, A5/2 and A5/3 in GSM, E0 in Bluetooth, SNOW 3G and ZUC in LTE 4G and expresso in 5G were discussed. Some practical implementation problems and their improvements to overcome the problems were stated. This study motivates young researchers towards the design of new stream cipher applicable for wireless communications.

REFERENCES

[1] Goutam Paul and Subhamoy Maitra (2012), RC4 Stream Ciphers and its variants, CRC Press ,Taylor & Francis Group.

[2] RC4 Link https://www.vocal.com/cryptography/rc4-encryption-algoritm/- R

[3] Lazar Stošić, Milena Bogdanović (2012), RC4 stream cipher and possible attacks on WEP, International Journal of Advanced Computer Science and Applications, Vol. 3, No. 3, 2012.

[4] Shenam Chugh, Kamal(2015),Securing data transmission over Wireless LAN (802.11) by redesigning RC4 Algorithm, 2015,IEEE International Conference on Green Computing and Internet of Things (IeGCloT).

[5] Olakanmi.O, Nigeria (2012), RC4c : A Secured Way to View Data Transmission in Wireless Communication Networks , International Journal of Computer Networks & Communications (IJCNC) Vol.4, No.2, March 2012.

[6] Yao Yao, Jiang Chong, Wang Xingwei(2010), Enhancing RC4 algorithm for WLAN WEP Protocol, IEEEChinese Control and Decision Conference,2010.

[7] Mohsen Toorani, Ali A. Beheshti (2008), Solutions to the GSM Security Weaknesses, Proceedings of the 2nd International Conference on Next Generation Mobile Applications, Services, and Technologies (NGMAST'08), pp.576-581, University of Glamorgan, Cardiff, UK, Sep. 2008.

[8] Slobodan petrovie and Amparo Fuster sabater(2000), Cryptanalysis of The A5/2 algorithm, Instituto de Fisica Aplicada serrano 144 ,28006,Madrid,Spain. Shahzad

[9] Marc Briceno, Ian Goldberg, DavidWagner (1998): A pedagogical implementation of A5/1,http://www.gsm-security.net/papers/a51.shtml.

[10] Jovan Dj. Goli´c: Cryptanalysis of Alleged A5 Stream Cipher, Springer-Verlag (1998).

[11] Thomas Stockinger (2005), GSM network and its privacy-the A5 stream cipher, http://citeseerx.ist.psu.edu/viewdoc/summary?doi=10.1.1.465.8718.

[12] Eli Biham, Orr Dunkelman (2000), Cryptanalysis of the A5/1 GSM Stream Cipher,Progress in Cryptology - INDOCRYPT 2000, First International Conference in Cryptology in India, Calcutta, India, (pp.43-51).

[13] Ross Anderson (1998): The GSM cipher, http://groups.google.com/group/sci.crypt/msg/ba76615fef32ba32.

[14] Ch. Naveen, Vishal R. Satpute (2016), Image encryption technique using improved A5/1 cipher on image bit planes for wireless data security, International Conference on Microelectronics, Computing and Communications (MicroCom), 2016.

[15] Komal Rege, Nikita Goenka, Pooja Bhutada, Sunil Mane(2013) ,Bluetooth Communication using Hybrid Encryption Algorithm based on AES and RSA, International Journal of Computer Applications (0975 – 8887) Volume 71– No.22, June 2013.

[16] Wuling Ren and Zhiqian Miao(2010), "A Hybrid Encryption Algorithm Based on DES and RSA in Bluetooth Communication", Second International Conference on Modelling, Simulation and Visualization Methods, 2010.

[17] Bluetooth link-https://krazycoder.wordpress.com/2010/09/08/basics-of-bluetooth-security/

[18] 3GPP specifications: Link http://www.3gpp.org/specifications
[19] ETSI/SAGE Specification (2006): Specification of the 3GPP Confidentiality and Integrity Algorithms UEA2 & UIA2, Document 2: SNOW 3G Specification, September 2006.
[20] ETSI/SAGE Technical report (2006): Specification of the 3GPP Confidentiality and Integrity Algorithms UEA2 & UIA2. Document 5: Design and Evaluation Report, Version 1.1, September 2006.
[21] ETSI/SAGE Specification(2011): Specification of the 3GPP Confidentiality and Integrity Algorithms 128-EEA3 & 128-EIA3. Document 1: 128-EEA3 and 128-EIA3 Specification; Version: 1.6; Date: 1st July 2011.
[22] Hadia M.S. El Hennawy , Alaa E.A. Omar , Salah M.A. Kholaif(2015), LEA: Link Encryption Algorithm Proposed Stream Cipher Algorithm, Ain Shams Engineering Journal (2015) 6, 57–65.
[23] Mahdi Madani, Ilyas Benkhaddra, Camel Tanougast, Salim Chitroub, and Loic Sieler (2017), Digital Implementation of an Improved LTE Stream Cipher Snow-3G Based on Hyperchaotic PRNG, Hindawi Security and Communication Networks Volume 2017, article ID 5746976, 15 pages.
[24] GSM link-http://pages.cpsc.ucalgary.ca/~szrrizvi/cpsc329/t2.html
[25] Romil Gandhi, Amitha Nair, Jason D'Souza (2014), GSM Networks: Substantiation of GSM Stationed algorithm, International Journal of Scientific & Engineering Research, Volume 5, Issue 7, July-2014 153.
[26] Khan,Shahzad, Shahid Peracha, Zain Ul Abideen Tariq(2014), Evaluation of Cryptanalytic Algorithm for A5/2 Stream Cipher, International Journal of Computer Science and Information Security, Vol. 12, No. 4, April 2014.
[27] Voice and packet encryption - https://security.stackexchange.com/questions/99559/cellular-encryption-algorithms-currently-in-use-globally
[28] Harsh Bhasin, Neha Kathuria Cryptography Automata Based Key Generation, International Journal of Scientific Research in Network Security and Communication , p 15-17,Volume-1, Issue-2, June- 2013
[29] P. Sharma, D.Mishra,V.K. Sarthi,P. Bhatpahri,R. Shrivastava,Visual Encryption Using Bit Shift Technique, International Journal of Scientific Research in Computer Sciences and Engineering, vol.5, Issue.3, pp.57-61, June (2017)

Authors Profile

Mr.Nagendar Yerukala is presently working as an research assistant in CRRAO AIMSCS, Hyderabad. He did his M.Tech from NITK surathkal and M.Sc from Kakatiya university. He is pursuing his Ph.D from JNTUH Hyderabad. His areas of interest are Network security and Cryptology.

Prof.V.Kamakshi Prasad is working as Director Evaluation and Professor in the Department of Computer Science and Engineering in JNTU Hyderabad. He obtained his PhD from the Indian Institute of Technology (IITM), Madras. He published his publications in several international journals and international conferences. He held several positions in JNTU Hyderabad. His research interests are in the areas of speech recognition, image processing, data mining and security

Prof.Allam Apparao is a chairman of NATIONAL INSTITUTE OF Technical TEACHERS TRAINING AND RESEARCH, Chennai. Alllam Appa Rao is a former Director of CR Rao Advanced Institute of Mathematics, Statistics, and Computer Science (AIMSCS), University of Hyderabad Campus, Hyderabad. He was the first to receive Ph.D from Andhra University in Computer Engineering in the year 1984. During his more than four decades of professional experience, such as first Vice Chancellor, JNTUK, Kakinada, A.P, Principal, College of Engineering (Autonomous), Andhra University. Indian Science Congress Association (ISCA) conferred him with "Srinivas Ramanujan Birth Centenary Award" Gold medal for his significant and life time contribution to the development of Science and Technology in the country specifically in the area of Computational Biology, Software Engineering and Network Security.

Dr. G. Padmavathi is working as an assistant professor in CRRAO AIMSCS, Hyderabad. She received Gold medal in M.Sc (Maths) from Acharya Nagarjuna University, Guntur, Andhra Pradesh, India. Awarded Ph.D in Mathematics from JNTUH University, Hyderabad. Her main research interest includes Cryptology, Machine learning, Modelling and Analysis.