GE-INTERNATIONAL JOURNAL OF ENGINEERING RESEARCH
VOLUME -3, ISSUE -5 (May 2015) IF-4.007 ISSN: (2321-1717)

ANALYZING CRYPTANALYTIC TECHNIQUES OF BLOCK CIPHERS FOR SYMMETRIC ENCRYPTION

[1]N.Sreevidya [2] K. Srilaxmi [3]Dr Prasanta Kumar Sahoo

[1] Assistant Professor, Dept. of CSE, SNIST, Hyderabad, India.

[2] Assistant Professor, Dept. of IT, SNIST, Hyderabad, India.

[3] Professor, Dept. of CSE, SNIST, Hyderabad, India.

ABSTRACT

There is a lot of research going on the cryptanalysis techniques. Many authors have suggested different cryptanalytic techniques for Symmetric and Asymmetric Encryptions but this paper discusses the Cryptanalytic techniques of Block Ciphers for Symmetric Encryption. This research work is being carried out after a thorough review on primary cryptanalytic techniques that are done on Block Ciphers such as Differential Cryptanalysis, Linear Cryptanalysis, the exploitation of weak keys and Algebraic attacks. A Smart card can be viewed as an intelligent data carrier which can store data like PINS, sensitive personal data and private keys in a secured manner and ensure data security during transactions but smart card industry is facing a lot many problems which is addressed in this work. The security issues are one major area of hindrance in smart card development and the level of threat imposed by malicious attacks on the integrated software is of high concern today. So SAFER++ proposed in this research work will be a very good solution for the problems faced by the smart cards industry.

Key words: cryptography, cryptanalyst, Cryptanalytic attacks, attacker

1. Introduction:

Cryptography can be defined as the science of secure communication over a pubic channel. It can be defined as a method of storing and transmitting data in a different form so that only authorized person can only read and process it. Cryptography mainly deals with the secure communication of messages by encrypting and decrypting the plain text to cipher text and vice versa.

There are mainly two types of cryptographic techniques. One is Symmetric Encryption and the other being Asymmetric Encryption. Asymmetric Encryption is proven to be secured compared to Symmetric Encryption as it uses different keys for encryption and decryption. Symmetric Encryption uses a single secret key to encrypt as well as decrypt. This can be used for both Stream ciphers as well as for Block ciphers. Cryptographic protocols were designed over Block ciphers and mostly Block cipher is used to provide confidentiality. There are many procedures to break the cipher in order to obtain the key as well as Plain text. The procedure used to derive these is called as Cryptanalytic Attack. Basically Cryptography and Cryptanalysis are the two basic parts of Cryptology. We tried to explain on the different types of Cryptanalytic techniques that can be done on Block Ciphers and finally analyzed how each attack is working on DES.

a. Symmetric Encryption: Symmetric Encryption is the best and oldest technique which uses a secret key to change the original text to a different format that cannot be understood by anyone who reads the message in the middle [1]. This secret key is either a number or a word or simply a sequence of arbitrary letters also. Conversion of plain or original text to an unknown format or Cipher text is called Encryption and converting the Cipher text back to original text is known as Decryption. When the sender and receiver know the secret key, they can encrypt and decrypt the messages easily. Because the sender and the receiver uses same key for Encryption and Decryption, it is named as Symmetric Cryptography**.**

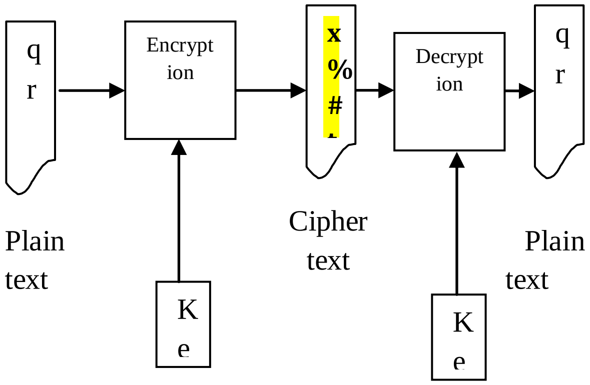

Fig 1: The Block Diagram of Symmetric Encryption

Stream ciphers or Block Ciphers, both are used by Symmetric Encryption:

- Stream ciphers: Each digit of the plain text is encrypted, single bit at a time.
- Block ciphers uses an algorithm and a key to encrypt group of bits at a time instead of single bit .Ex: Block size of 64 bits.

Because Block ciphers are building blocks of Cryptographic protocols and the major use of Block cipher is to provide confidentiality i.e. preventing eavesdropper from knowing the contents of the message. So we are mainly concentrating on Symmetric Block Ciphers so as to present the attacks on Block Ciphers. So Block ciphers are discussed below here [2]-[4]:

b. Block Ciphers

Plaintext is divided into blocks of fixed length and every block is encrypted one at a time. A block cipher is a set of 'code books' and every key produce a different code book. The encryption of a plaintext block is the corresponding cipher text block entry in the code book. We have c = ek (m) where: m is the plaintext block, k is the secret key, e is the encryption function, c is the cipher text as stated in Fig 2.

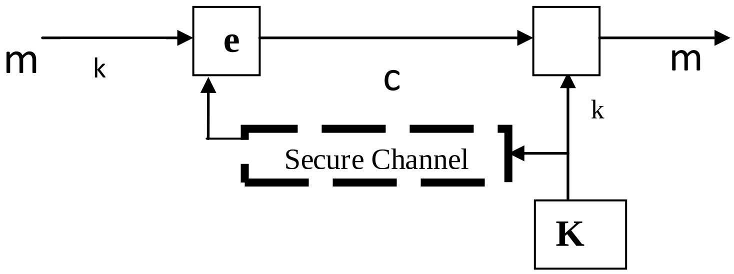

Fig 2: Symmetric Cryptography in the form of an equation

In addition we have a decryption function d such that: Decryption is given by m = dk(c). Where m= message, d =Decryption function, k=secret key, c=cipher text, KG = key generator. Both sides need to know the key k, but k needs to be kept secret. This is called as Symmetric key, secret-key, single-key or one-key algorithms.

2. Cryptanalysis:

Cryptanalysis [5]-[6] refers to the study of ciphers, cipher text or cryptosystems (i.e. to secret code systems) with a view to find weaknesses in them that will allow obtaining the plain text from the cipher text without knowing the key or the algorithm. This is known as *breaking* the cipher, cipher text, or cryptosystem.

Cryptanalytic attacks scenarios: The main goal of cryptanalyst is to obtain the maximum information about the plain text (original data). There are many procedures to break the cipher in order to obtain the key as well as Plain text. The procedure used to derive these is called as Cryptanalytic Attack. Classification of Cryptanalytic attacks [7] is done on the following basis. They are:

- **Cipher text-only attack:** Here the attacker has right to use only to cipher text.
- **Known-plain text attack:** Here the attacker has a cipher text and its equivalent plaintext
- **Chosen – cipher text attack:** In this attack, the cryptanalyst can *select* cipher texts and find their equivalent plaintexts.
- **Chosen – plain text attack:** In this, the cryptanalyst can *select* a plaintext and find their cipher texts.
- **Adaptive Chosen Plain Text:** This is similar to Chosen Plain text except that the attacker selects the succeeding set of plain text which is based on the information obtained from previous encryption methods.
- **Adaptive Chosen Cipher Text**: This is similar to Chosen Cipher text except that the attacker selects the succeeding set of Cipher text which is based on the information obtained from previous encryption methods.
- **Related Key Attack:** This is similar to Chosen plain text attack in which attacker can get cipher text encrypted with two keys. Here the keys are not known but the relationship between the keys is known. Ex: two keys differ by a single bit.

3. Types of Attacks on Block ciphers

There are several attacks/cryptanalytic techniques which are specific to block ciphers [8]. The most important on symmetric block ciphers are:

a. Differential cryptanalysis: Differential cryptanalysis [9] was first presented by Biham and Shamir at CRYPTO '90 to attack on DES. This generalized form of cryptanalysis is applied to block ciphers but also applied to stream ciphers and cryptographic hash functions. In block ciphers, it refers to a procedure where difference in network of transformations and cipher depicts different behavior helps to find the secret key. It's a chosen plain text attack that can be used on iterative block ciphers. It is based on the analysis of the differences between two related plaintexts as they are encrypted using common key. So by analyzing the obtained data, probabilities are assigned to each of the possible keys, and finally the most probable key is recognized as the correct one. It's a chosen plain text attack, assumes that the attacker knows (plain text, cipher text) pairs. It involves comparing XOR of two plain texts to the XOR of two corresponding cipher texts. Difference $\Delta p = p_1 \oplus p_{2,}$ $\Delta_c = c_1 \oplus c_{2.}$ By distributing Δ_c's, given Δp may get the information about certain bits of the key. After finding several bits, using Brute force for the rest of the bits reveals the key. In DES, S-boxes were designed to resist the Differential Cryptanalysis.

i) Substitution: This substitution is also known as S-Box. S-boxes are used to Change the input bits to output bits and vice versa. These are used in encryption as well as decryption methods. The same S-box method is used well in known plain text attack and cipher text – only attacks of block ciphers.

ii) Permutation (P-Box): P-box Substitution is simply a mapping of one value to another whereas permutation is a reordering of the bit positions for each of the inputs. Ex: the first bit of the output is taken from the 58th bit of the input; the second bit from the 50th bit, and so on, with the last bit of the output taken from the 7th bit of the input. These techniques are used a number of times in iterations called rounds.

iii) **Key mixing:** Key mixing involves all the below steps. They are of three types such as:

a) Expansion — the 32-bit half-block is enhanced to 48 bits using the ***expansion permutation***, by duplicating half of the bits. The output contains eight 6-bit (8 * 6 = 48 bits) pieces, each having a copy of 4 matching input bits and a copy of the next bit from each of the input pieces to either side.

b) Key mixing — Now the result is shared with a *subkey* using an XOR operation. Sixteen 48 bit subkeys, one for each round are derived from the main key using the key schedule described below.

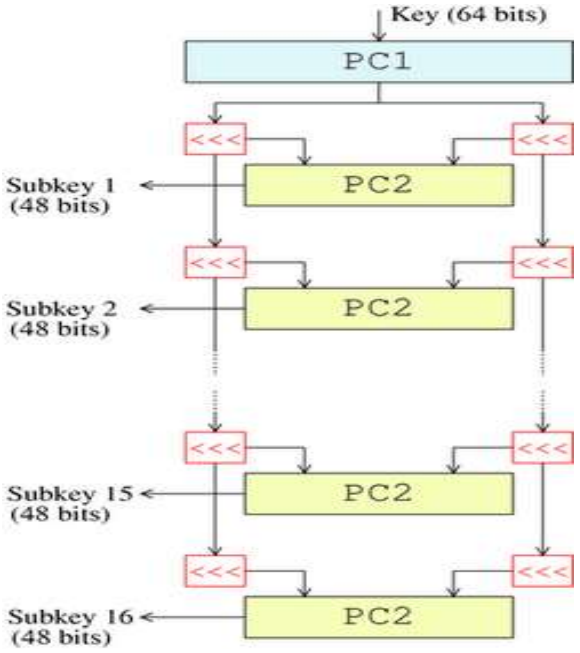

Fig 3: Key schedule of DES

c) Key schedule: Figure 3 represents an algorithm that generates subkeys for the encryption. Out of the 64 available bits, 56 bits are selected by (PC-1) permuted choice 1, the left over 8 bits are either not needed or used as parity check bits.56 bits are divided into two 28 bit halves. Each half is separately treated. In succeeding rounds, the two halves are rotated left by one and two bits (for each round), and then 48 subkeys bits are selected by (*PC-2*) permuted choice 2, 24 bits from left half and 24 bits from right half. "<<<" in diagram represents rotations i.e. different set of bits is used in each subkeys. Each bit is roughly used in 14 out of the 16 subkeys. Similarly the key schedule for decryption process contains subkeys in reverse order. Except this, remaining procedure is same as encryption. The similar 28 bits are passed to all the rotation boxes.

i) Substitution : The block is separated into eight 6-bit pieces after mixing in the subkeys and before processing by S-boxes. In all the 8 S-boxes the 6 input bits are replaced with 4 output bits following the non-linear transformation in the lookup table. Without S-boxes, the cipher would be linear and easily breakable.

ii) Permutation : Finally the 32 outputs from the S-boxes are arranged following the fixed permutation P-box. This is done because after the p-box, each of the S-box's outputs is reached across the four different S-boxes in the next round.

Differential cryptanalysis was not effective against DES in practice. Differential cryptanalysis requires 2^{47} chosen plain texts to generate the DES key. This method has been used against many ciphers with varying degrees of success.

b) Linear cryptanalysis: Matsui and Yamagishi first devised ***linear cryptanalysis* in** an attack on **Fast Data Encipherment Algorithm (FEAL) [10].** It was developed by Matsui to attack DES. It is the widely used attack on Block cipher. This is a known plain text attack that uses linear approximation to explain the behavior of block ciphers. If sufficient number of pairs of plain text and its equivalent cipher text are provided, some bits of information about the key can be found. With more information, the probability of success will be high. There are 2 parts in linear cryptanalysis. The first part is to construct linear equations involving plain text, cipher text and key bits that have high bias as close to 0 or 1. The second part is to use these linear equations in combination with known plain text, cipher text pairs to obtain key bits.

i) Constructing linear equations: A linear equation will tell us the equality of two expressions containing binary variables with XOR operation. For ex: the following equation, from a hypothetical cipher, shows the XOR sum of the first plain text bits (P1) and third plain text bits(P3) (as in block cipher's block) and the first cipher text bit(C1) is equal to the second bit of the key(K2) : $P1 \oplus P3 \oplus C1 = K2$ In an ideal cipher, any linear equation having plain text, cipher text and key bits would have probability 0.5. As the equations in linear cryptanalysis have variance in probability, they are termed as linear approximations. Constructing approximations is different for each cipher. The common type of block cipher, substitution network and analysis is mainly on S-boxes. For small S-boxes it is possible to itemize every possible linear equation relating the S-box's input and output bits calculate their biases and choose the best ones. Linear approximations for S-boxes must be combined with other actions such as Permutation and Key mixing to derive linear approximations for the entire cipher. For small S-boxes we can find linear equation containing S-boxes input and output bits, calculate the bias and select the best ones. A useful tool for this combination is Pilling-up lemma.

ii) Deriving key bits: After obtaining linear approximation of the form:

$\mathbf{P_{i1} \oplus P_{i2} \oplus \ldots\ldots.. \oplus C_{j1} \oplus C_{j2} \oplus \ldots\ldots. = K_{k1} \oplus K_{k2} \oplus \ldots\ldots..}$ where$\mathbf{P_{i1}} \oplus \mathbf{C_{j1}}$ represents a plaintext-cipher text pairs and $\mathbf{K_{k1}}$ refers to partial key. Now we can apply Matsui's algorithm2 having known plain text-cipher text pairs to guess the values of key bits. On right hand side for each set of values of key bits, assume count T that counts how many times the approximation holds good for all known plain text-cipher text pairs. The partial key who's T has the highest absolute difference from half the number of plain text-cipher text pairs is referred to as the most likely set of values for those key bits. It is understood that the correct partial key will cause the approximation to hold with high bias. The same technique can be applied to other linear approximations by guessing values of key bits until the number of unknown key bits is less, that they can be attacked with brute force.

M. Matsui showed(1993/1994) that DES can be broken in 8 rounds with 2^{21} known plain texts and in 16 rounds with 2^{43} known plain texts taking 40 days to generate the plain text and cipher text and takes 10 days to find the key. But the attack requires too many pairs to be implemented in real world.

This method requires 2^{43} known plain texts to generate the DES key compared to 2^{47} selected plain texts in Differential Cryptanalysis [11]**.** Many improvements to the attack have been suggested using multiple linear approximations resulting in a generalized partitioning cryptanalysis.

c) Exploitation of Weak keys*:*

Weak keys [8] are the keys that make the same sub key to be generated in more than one round. There are 2^{56} ($7.21 * 10^{16}$) possible keys for DES, of which only four are weak keys. They are

- 01010101 01010101

- FEFEFEFE FEFEFEFE

- E0E0E0E0 F1F1F1F1

- 1F1F1F1F 0E0E0E0E

Using weak keys, the outcome of the Permuted Choice 1 (PC1) in DES key schedule results in round keys with either all 0's, all 1's or alternate zero, one combinations. Because all the subkeys are similar and DES is a Feistel network, the encryption function becomes self-inverting; that is, encrypting twice with a weak key K produces the original plain text. E_K (E_K (x)) =x for all x, i.e., the encryption and the decryption are the same. Weak keys are secret keys with a definite value for which the block cipher will exhibit certain regularities in encryption or poor level of encryption. Therefore weak keys should be avoided at key generation. IDEA is a replacement for DES algorithm which is a Symmetric Block Cipher algorithm developed by Xueja Lie and James.L.Massey was used in PGP(Pretty Good Privacy) v2.0 developed at ETH in 1990. IDEA consists of 64 bit plain text and size of the key is 128 bits and this key is divided in 52 sub keys. Cipher text is also 64 bit. There are 8 identical rounds in which each round uses 6 keys. We have 48 keys like this and in last round another 4 keys (6*8=48+4=52) are being used by both Encryption and Decryption.

For other block cipher with large set of weak keys picking a weak key is too difficult. In that case the presence of weak keys will have a definite impact on the block cipher security.

d) Algebraic attacks:

These are the type of techniques that relies on Block ciphers that show a high degree of mathematical structure [12]. For ex: it is believed that block cipher shows a group structure. If this is the case, then encrypting the plain text with one key and encrypting the result with another key would be same as single encryption using some other single key. So in this case multiple encryptions also do not provide security compared to single encryption.

Algebraic attacks works in this manner: First by knowing the particular cipher, one must convert the cipher and some additional information such as file formats into a system of polynomial equations usually over GF (2).The second step is to solve the system of equations and find the secret key of the cipher from the solution. The first step i.e. system of equations is solved with SINGULAR, MAGMA and with SAT.

Algebraic techniques provide a unique attack methodology for several areas of cryptography and this is one of the few choices when very few pairs of plain text and cipher text are available. It can also be combined with differential cryptanalysis and side-channel cryptanalysis. Following is the table showing different complexities of attacks for Linear Cryptanalysis and Differential Cryptanalysis.

Attack Method	Known	Chosen	Storage complexity	Processing complexity
Linear Cryptanalysis	2^{43} 2^{38}	- -	For texts	2^{43} 2^{50}
Differential Cryptanalysis	- 2^{55}	2^{47} -	For texts	2^{47} 2^{55}

Table 1 : Table showing different complexities of attacks

Additional attacks that can be done on Block Ciphers are SAFER, Skipjack, Blowfish, CAST256 [9]. They are explained below:

4. Proposed Solution:

SAFER (Secure And Fast Encryption Routine) [13] is developed by Massey in 1993 for Cylink Corporation [Mas93]. This is not a proprietary **block cipher** technique like the other techniques. It is a byte oriented algorithm that uses 64-bit block size or 64-bit key size. It requires minimum 6 rounds but allows variable number of rounds. Consequently SAFER with 64-bit key is named as SAFER K-64 and SAFER with 128-bit key is named as SAFER K-128 and these both are attacked by Differential and Linear Cryptanalysis when the number of rounds are greater than 6.Soon SAFER SK-64 and SAFER SK-128 followed with a strengthened key schedule but a recent version SAFER SK-40 with 40-bit key and five number of rounds which is less than the minimum number of rounds required for SAFER is proven to be more secure against Differential and Linear Cryptanalysis. SAFER++ is the latest cipher in the safer-family of ciphers. The main difference between SAFER++ and the earlier ciphers lies in the linear layer. It has 128-bit block and 256-bit key version with 10 rounds. By increasing the number of rounds in SAFER++ $_{128}$, the attack is impractical, as the amount of data and time required is too high [14].

Coming to Crypto-Protocol [15] which comes under the logical attacks on Smart Cards that handles consecutive cryptographic operations to perform transactions, if such a protocol is not carefully designed it may present opportunities for attackers to perform replay attacks or related exploits. SAFER uses different techniques for Encryption and Decryption compared to other block ciphers. So Byte based operations are involved in SAFER for its use in smart card-based applications to overcome such attacks [16].

Skipjack is an encryption algorithm that uses 80-bit key to encrypt 64-bit blocks of data which is expected to be more secure than DES which uses 56-bit keys. But this is never finalized.

Blowfish[17] developed by Bruce Schneier which is a 64-bit block cipher with Feistel structure and each round consists of a key-dependent permutation and a key and data dependent substitution. All operations are dependent on XORs and additions on 32-bit words. The key has a length i.e. variable (with a maximum length of 448 bits) and is used to generate several subkeys arrays. This cipher is specifically designed for 32-bit machines and is faster than DES. But the three-round version of Blowfish is proven to be secure even with the existence of certain weak keys. The AES Twofish is based on Blowfish.

CAST-128: Another popular technique called CAST-128 (Carlisle Adams and Stafford Tavares) with 64 bit Feistel cipher allows up to 128 bit key size. It contains 16 non-identical rounds, where each round contains integer and bit wise addition and bit wise rotation. CAST-256 which uses key of 256 bit size is proven to be more secure.

5. Conclusion: Cryptography is the only solution to today's information age, which is surrounded by so many security problems. This paper discussed the various types of Cryptanalysis techniques related to block ciphers in Symmetric Encryption such as Differential Cryptanalysis, Linear Cryptanalysis, the Exploitation of Weak keys, and Algebraic attacks. This research work reviewed the basic fundamentals related to various attacks in block ciphers. This paper also identifies the various problems in smart card development. This work suggests using SAFER++ in smart card-based applications which is very difficult to cryptanalysis. Knowing in advance various types of cryptanalytic attacks helps us to make our system more secure from any cryptographic attack in future. It is concluded that block ciphers are very prone to attacks and so we proposed to use byte oriented cipher like SAFER +, SAFER ++ which is exponentially hard to cryptanalysis in smart card.

6. References:

[1] William Stallings, "Network Security Essentials (Applications and Standards)", Pearson Education, 2004.

[2] Raphel C., W Phan and M umar siddiqui, "A Framework for Describing Block Cipher cryptanalysis", IEEE transactions on computers, vol.55, no.11, 2006.

[3] J.Daemen, L.Knudsen and V.Rijmen, "The Block Cipher Square" in Fast Software Encryption, 4th International Workshop, Volume 1267 of Lecture Notes in Computer Science, pages pp.149-165.Springer -Verlag Heidelberg, 1997.

[4] Atul Kahate (2009)," Cryptography and Network Security", 2nd edition, McGraw-Hill.

[5] Cryptography and Network Security Principles and Practice by Williams Stallings, 5th edition, PEARSON Publications page no: 92-93.

[6] Ashish Kumar Kendhe, Himani Agrawal, "A Survey Report on Various Cryptanalysis Techniques", IJSCE ISSN: 2231-2307, Volume-3, Issue-2, May 2013

[7] Bruce Scheneir ,"A Self study Course in Block Cipher Cryptanalysis " in Cryptologia, v.24, n.1, Jan 2000, pp. 18-34.

[8] http://www.emc.com/emc-plus/rsa-labs/

[9] Paul Kocher, Joshua Jaffe and Benjamin Jun, "Differential Power Analysis", in proceedings of Advances in Cryptology, CRYPTO '99, Springer Verlag, 1999.

[10] Liam Keliher , "Refined Analysis of Bounds Related to Linear and Differential Cryptanalysis for the

AES", published in International Association for Cryptologic Research, 2005.

[11] M.E.Hellman and S.K.Langford, *Differential–linear cryptanalysis*, Advances in Cryptology - Proc. Crypto'94, LNCS 839, pages 26–39. Springer Verlag, 1994.

[12] Bard, G. Algebraic Cryptanalysis, chapter 2, http://www.springer.com/978-0-387-88756-2, 2009.

[13] J.L.Massey, "Safer K-64: A Byte-oriented block-ciphering Algorithm" in Fast Software Encryption, Cambridge Security workshop proceedings, Springer-Verlag, 1994, pp. 1-17.

[14] James L. Massey, Gurgen H. Khachatrian, and Melsik K. Kuregian in nomination of SAFER++ as Candidate Algorithm for the NESSIE by Cylink Corp., September 2000.

[15] Hoon Ko and Ronnie D. Caytiles, "A Review of Smartcard Security Issues" in proceedings of SERSC available at http://www.sersc.org/journals/JSE/vol8_no3_2011/3.pdf

[16] Marc Witteman, Power Analysis on Unknown Crypto Algorithms, presented at the workshop Cryptographic Security Aspects of Smart Cards & the Internet, Amsterdam, June 2002.

[17] Ahmadou A. SERE, Julien Iguchi-Cartigny, Jean-Louis Lanet "Evaluation of Countermeasures Against Fault Attacks on Smart Cards", IJAST Vol.4, No.1, April, 2011)

Biographies:

N. Sreevidya , M.Tech CSE from JNTUH, Hyderabad. She possesses 11 years of experience in Academic and has guided many UG students. Currently she is working as Asst.Professor at Sreenidhi Institute of Science and Technology, Hyderabad. Her areas of interest include Mobile Computing, Networks, Information Security, Software Engineering and Big Data Analytics.

K.Srilaxmi, M.Tech CSE from JNTUH, Hyderabad. She possesses 12 years of experience in Academic and has guided many UG students. Currently she is working as Asst.Professor at Sreenidhi Institute of Science and Technology, Hyderabad. Her areas of interest include Information Security and Big Data Analytics.