International Journal of Emerging Trends & Technology in Computer Science (IJETTCS)
Web Site: www.ijettcs.org Email: editor@ijettcs.org, editorijettcs@gmail.com
Volume 1, Issue 3, September – October 2012 **ISSN 2278-6856**

Analysis of Avalanche Effect in Plaintext of DES using Binary Codes

Akash Kumar Mandal[1], Mrs. Archana Tiwari[2]

[1]Department of Electronics and Telecommunication
Chhatrapati Shivaji Institute of Technology,,Durg,Chhattisgarh,India

[2]Department of Electronics and Instrumentation
Chhatrapati Shivaji Institute of Technology,,Durg,Chhattisgarh,India

Abstract: ***With the fast progression of digital data exchange in electronic way, information security is becoming more important in data storage and transmission. Cryptography has come up as a solution which plays a vital role in information security system against malicious attacks. This security mechanism uses some algorithms to scramble data into unreadable text which can be only being decoded or decrypted by party those possesses the associated key. These algorithms consume a significant amount of computing resources such as CPU time, memory and computation time. In this paper a most widely used symmetric encryption technique i.e. Data Encryption Standard (DES) have been implemented using MATLAB software. After the implementation, this encryption technique was analyzed based on a parameter called Avalanche effect, using binary codes. Avalanche Effect due to one bit variation in plaintext keeping the key constant after mapping it in a binary code, Experimental results shows that the proposed algorithm exhibit significant high Avalanche Effect which improves the level of the security.***

Keywords: Data Encryption Standard (DES), Encryption, Decryption, Ciphertext, Secret key, Avalanche Effect.

1. INTRODUCTION

Transmission of sensitive digital data over the communication channel has emphasized the need for fast and secure digital communication networks to achieve the requirements for integrity, secrecy and non reproduction of transmitted information. Cryptography provides a method for securing and authenticating the transmission of information across insecure communication channels. It enables us to store sensitive information or transmit it over insecure communication networks so that unauthorized persons cannot read it. [1] Cryptography is an indispensable tool for protecting sensitive information in computer systems. Cryptography makes the message unintelligible to outside the world by various transformations. Data Cryptography is method of scrambling the content of digital data like text, image, audio and video to make it unreadable or unintelligible for others during transmission. The main goal of cryptography is to keep the data secure from unauthorized access [2]. Data containing information that can be read and understood is called plaintext or clear text. The method of scrambling the plaintext in such a way that hides its substance is called encryption. Encrypting plaintext makes the information in unreadable information called cipher text. The process of converting cipher text to its original information is called decryption. The complexity of encryption process depends on algorithm used for encryption, software used and the key used in algorithm to encrypt or decrypt the data. Security of any encryption system depends on the security principle proposed by Kirchhoff. According to the Kirchhoff, the security of the encryption system should depend on the secrecy of the encryption /decryption key rather than encryption algorithm. [3]

After extensive survey of various research papers it is observed that an encryption algorithm should produce significant change in the encrypted message when a small change is made in original message.

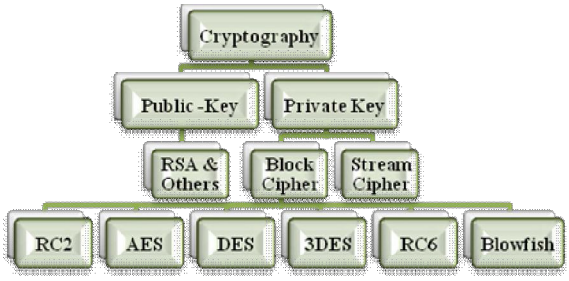

Figure.1 Overview of the field of cryptography

In research papers [8] and [9] authors analyzed various cryptographic algorithms using a parameter called Avalanche Effect. In this paper we proposed an enhancement in DES algorithm using binary codes. This proposed algorithm is expected to provide significant high Avalanche Effect.

2. CRYPTOGRAPHIC ALGORITHMS

Depending upon the number of keys used, cryptographic algorithms can be classified as asymmetric algorithms (public key) and symmetric algorithms (secret key). In

Symmetric keys encryption or secret key encryption identical key is used by sender and receiver. Data Encryption Standard (DES), 3DES, and Advanced Encryption Standard (AES) are the example of Symmetric key encryption algorithms. In asymmetric keys encryption two different keys (public and private keys) are used for encryption and decryption. Public key is used for encryption and private key is used for decryption Rivest-Shamir-Adelman (RSA) and Elliptic Curve Cryptosystem (ECC) are the example of asymmetric key algorithms.[4]A symmetric cryptosystem has five ingredients:

2.1 Plaintext

This is the original data or message to be transmitted that fed into the algorithm as input.

2.2 Encryption Algorithm

The algorithm performs various transformations and substitutions on the plaintext.

2.3 Secret key

This is another input to the algorithm and the value of secret key is independent of the plaintext. Depending on the specific key the algorithm will produce a different output.

2.4 Encryption Algorithm

This is the scrambled or encrypted message produced as output. This output depends on the plaintext and the secret key.[5]

2.5 Decryption Algorithm

This is essentially the encryption algorithm operate in reverse. It takes the ciphertext and the secret key as input and produces the original plaintext as output.

3. DES ALGORITHM

The Data Encryption Standard (DES) designed to encrypt and decrypt blocks of data consisting of 64 bits under control of a 64-bit key. Encrypting data converts it to an unreadable cryptorgaphic security of the data depends on the security provided for the key used to encipher and decipher the data. [4]form known as cipher. Decrypting cipher converts the data back to its original form known as plaintext. Both encryption and decryption operations are performed using a binary number called a key. A DES key is a 64 bit binary number of which 56 bits are randomly generated and used directly by the algorithm. The remaining 8 bits, which are not used by the algorithm while encryption, can be used for error detection. The 8 error detecting bits are set to make the parity of each 8-bit byte of the key odd, i.e., there is an odd number of "1"s in each 8-bit byte. Authorized users of encrypted computer data must have the key that was used to encipher the data in order to decrypt it. The encryption algorithms specified in this standard are commonly known among those using the standard. The Data can be recovered from cipher only by using exactly the same key used to encipher it. Unauthorized recipients of the cipher who know the algorithm but do not have the correct key cannot derive the original data algorithmically. However, it may be feasible to determine the key by a brute force "Exhaustion attack" Also, anyone who does have the key and the algorithm can easily decipher the cipher and obtain the original data. A standard algorithm based on a secure key thus provides a basis for

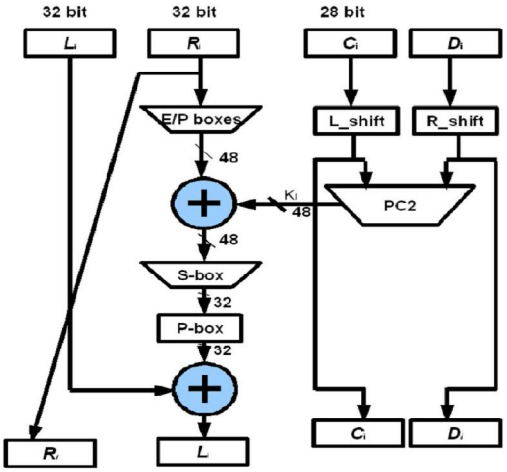

Figure 2 DES (Data Encryption Standard) process

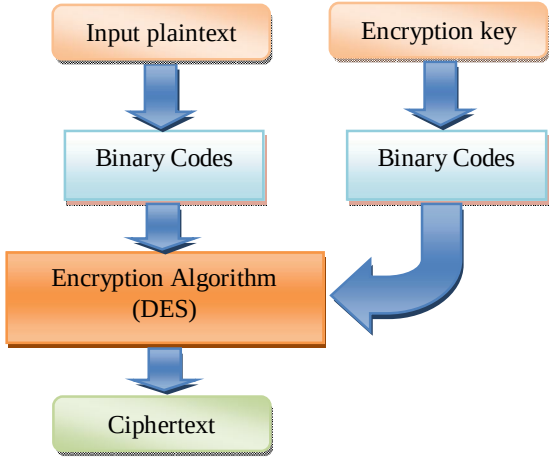

Figure 3 DES process when input plaintext and input key are mapped in binary code

exchanging encrypted computer data by issuing the key used to encipher it to those authorized to have the data. Data that is considered sensitive by the responsible authority, data that has a high value, or data that represents a high value should be cryptographically protected if it is vulnerable to unauthorized disclosure or undetected modification during transmission or while in storage. [6]

4. METHODOLOGY

We have implemented Data Encryption Standard (DES) algorithm in MATLAB 7.0 software. This encryption technique takes 64 bit data block as input and encrypt this data block using 64 bit key. Figure 3 shows the block diagram of algorithm that we have used for our experiments. In our experiments we have mapped input plaintext and encryption key into various binary codes before providing the input to the DES algorithm.

If there are n quantities in a group, a code of b binary digits or bits may represent all quantities unequally. [7]

$$n \leq 2^b$$

4.1 Natural BCD Code (8421 code)

Natural BCD code or 8421 code is used whenever decimal information is transferred in or out of a digital system. In this code straight assignment of binary equivalent is used with weights.

4.2 2421 Code

These are weighted ,reflected and self-complementing codes, In 2421 codes if a number has more than one representation then choose the code that uses the lower binary weights (for number 0-4 only)

4.3 5421 Code

These are weighted code with weight 5-4-2-1. In 5421 codes if a number has more than one representation then choose the code that uses the lower binary weights.

4.4 7421 Code

These are weighted code with weight 7-4-2-1. For decimal number 7 choose code with least number of 1's.

4.5 5311/5211 Code

These are weighted code with weight 5-3-3-1. In these codes if a number has more than one representation then choose the code with least number of 1's and use first the 1 from extreme right that uses the lower binary weights.

4.6 Gray Code

It is also known as "reflected and unit distance code" which is a reflected mirror image. Unit distance exhibit only a single bit change from one code to the next. It is also an unweighted and not an arithmetic code.

4.7 3321/4221 Code

These are weighted code with weight 3-3-2-1/4-2-2-1.

5. EVALUATON PARAMETER

Each of the encryption technique has its own strong and weak points. In order to apply an appropriate technique in a particular application we are required to know these strengths and weakness. Therefore the analysis of these techniques is critically necessary. A desirable property of any encryption algorithm is that a small change in either the plaintext or the key should produce a significant change in the cipher text.

$$\text{Avalanche Effect} = \frac{\text{Number of flipped bits in ciphered text}}{\text{Number of bits in ciphered text}}$$

However, a change in one bit of the plaintext or one bit of the key should produce a change in many bits of the cipher texts. This property is known as Avalanche Effect [8, 9].Avalanche Effect can be calculated by using above equation.

The performance of proposed algorithm is evaluated using Avalanche Effect due to one bit variation in plaintext(before being mapped in various binary codes) keeping encryption key constant in a binary code .

Avalanche Effect is calculated for various combination of plaintext and encryption key by mapping them in various binary codes.

Table 1: Data code is fixed in 2421 code and key varied

Data in **2421**	Key : '3B3898371520F75E'		Avalanche Effect
	Data:'ABCDEF01 23456789'	Data:'ABCDEF01 27456789'	
2421	'C79E3C7 A3E1763CF'	'2A8EA04C 65B41C60'	37
3321	'B466EBF3 64DB1F96'	'778AD655 703CF8A7'	35
4221	'194DBB9E 9849A99D'	'AAADCE33 FE7F47B7'	35
5211	06A844B0 3889B6DD'	'0CF914C3 1991F112'	26
5311	'19324425 F522CD27'	'ED577EB1 B746B3F6'	31
5421	'E9CCABBF AB908BD4'	'7FFC85C3 72360A1A'	31
7421	'B009AA52 8D569E46'	'4441B255 993F9517'	24
GRAY	'F711F8F9 ED42BAEB'	'03185F61 B8746736'	35
8421	'9AE993DC 123AB963'	'0C10DF1A A3137F98'	35

Table 2: Data code is fixed in 3321 code and key varied

Data in **3321**	Key : '3B3898371520F75E'		Avalanche Effect
	Data:'ABCDEF01 23456789'	Data:'ABCDEF01 27456789'	
2421	'652B8E48 7B6CDBCE'	'294BB964 1F5F0368'	28
3321	'CB680809 5F84B565'	'9E491AA1 47C57E49'	23
4221	'24EF7640 3736F683'	'EE6C3558 7527CA87'	21
5211	'3F185FBF 6A755D53'	'0A9AF76F 9BB0E34A'	30
5311	'7A7BA88D 8F3A90F7'	'B35CD18E C0C0EDD4'	35
5421	'8810A024 17FA2897'	'EBC5F8BD 8677C366'	34
7421	'C704C1E9 1A7E781D'	'D75E1AD5 9B1082ED'	32
GRAY	'4F63A1D2 752949BC'	'2DD55D83 E0ED740E'	33
8421	'B7B7D97B E0F284A3'	'68D8052D 69799089'	34

Table 3 : Data code is fixed in 4221 code and key varied

Data in 4221	Key : '3B3898371520F75E'		Avalanche Effect
	Data:'ABCDEF01 23456789'	Data:'ABCDEF01 27456789'	
2421	'8B5B700C 691E1058'	'894E1AEC BD04568D'	26
3321	'A144F374 DA022507'	'D0A60E85 3F47C3B4'	38
4221	'B957F5F4 82D45CEF'	'B87C3338 B128D8D5'	29
5211	'64A2C1D2 DE1D3305'	'1EFC9935 0AAB90B8'	38
5311	'1F0FDC21 CDFA29C9'	'1A42DA38 5EE5ABA8'	25
5421	'9AC6B870 4A6678EC'	'54B93B6B 62F10F4C'	34
7421	'F4B1C37B 50E1B589'	'44C50BD7 2B691BC6'	32
GRAY	'92931295 0EEB83BE'	'71FF1693 EA3BC103'	27
8421	'1F662D0D 6B46637E'	'2C31111E 56C69688'	34

Table 4: Data code is fixed in 5211 code and key varied

Data in **5211**	Key : '3B3898371520F75E'		Avalanche Effect
	Data:'ABCDEF01 23456789'	Data:'ABCDEF01 27456789'	
2421	'5A03A883 636691ED'	'9F178264 36E12D59'	32
3321	'0626106C 4D70D77E'	'657F95BA F8B39712'	30
4221	'49A36E42 2A0AB541'	'7D28BBA7 9CC3502E'	37
5211	'FF3F1829 C25C624B'	'606887B4 98D07A7A'	34
5311	'B6B2B32D 84A532B1'	'DD9011ED 34B9156B'	27
5421	'FCACF8A8 C9190426'	'7D2D0376 E6E95E0F'	33
7421	'698879F4 012FA33C'	'E17EA595 430B9385'	27
GRAY	'08FFED9B E65CFA72'	'000A83E9 785D4423'	31
8421	'628E24E3 836C514C'	'4FD31484 E523AAF4'	36

Table 5: Data code is fixed in 5311 code and key varied

Data in 5311	Key : '3B3898371520F75E'		Avalanche Effect
	Data:'ABCDEF01 23456789'	Data:'ABCDEF01 27456789'	
2421	'EBEA650A 7AF76C6A'	'2F3EB840 FF8C714A'	30
3321	'F7C35243 B5B430D9'	'31861342 AFCFAA01'	27
4221	'BC97CB1E F1AA793C'	'14DD040D BFECC01E'	29
5211	'F5FD9950 A58F9625'	'B0ADB3DE C20918A4'	26
5311	'87A9D7F8 8039D29A'	'5EDDEA69 02AA2480'	32
5421	'DC0EA148 3B7BFAF9'	'BDA40C2C 94FF242C'	34
7421	'22F18389 21C903B5'	'BBB2D53B 60358BC8'	31
GRAY	'45FE6645 04AC7392'	'03E14029 DA8B3323'	30
8421	'E1AB8427 DAA84878'	'849CBFCC 6EBAF394'	37

Table 6: Data code is fixed in 5421 code and key varied

Data in 5421	Key : '3B3898371520F75E'		Avalanche Effect
	Data:'ABCDEF01 23456789'	Data:'ABCDEF01 27456789'	
2421	'1257BE96 584FB519'	'E9A6E23A B3FDC969'	38
3321	'198FFB39 937E2A4E'	'269F50AD 108795B9'	38
4221	'FFF0916F 34676E67'	'0A389293 E366880B'	33
5211	'5C7D7ACC 75E75E63'	'5226D440 811454FF'	33
5311	'0C46CAFD 5B6662C6'	'77FB5147 2C8D3A6B'	42
5421	'A0290F6B C8B80958'	'30073919 E2130A8B'	29
7421	'FE072BB2 460EBE63'	'3ECF2987 33B7D0A9'	29
GRAY	'C524D34C B28AEE6A'	'825A1CEA CD0615D5'	44
8421	'FE4162F3 9FA9CB93'	'76E1750A D505CBF6'	25

Table 7: Data code is fixed in 7421 code and key varied

Data in 7421	Key : '3b3898371520f75e'		Avalanche Effect
	Data:'ABCDEF01 23456789'	Data:'ABCDEF01 27456789'	
2421	'6E71BE89 C69A9E91'	'59812BF9 8C465E56'	31
3321	'A4EEC70E 309CD030'	'7C8BA5B5 0CCC2A48'	33
4221	'B53E4DDD D3F2CCEF'	'B820F613 7E199153'	39
5211	'F99DE434 E34A0978'	'D171EDD4 C2EEE4FA'	25
5311	'F380A3AB F1803EA4'	'99D0796F 3DE20FBB'	29
5421	'A3A3A7B4 30E95256'	'098FA674 01889CCA'	25
7421	'3CEB3C55 CB15E1D0'	'4520A9BD 0A181228'	35
GRAY	'A9585152 2B048EB5'	'44ECD251 56709934'	31
8421	'BE4E60D5 31E8F758'	'6EA1FA47 A2A81565'	31

Table 8: Data code is fixed in Gray code and key varied

Data in GRAY CODE	Key : '3B3898371520F75E'		Avalanche Effect
	Data:'ABCDEF01 23456789'	Data:'ABCDEF01 27456789'	
2421	'0FFDC969 A15579D6'	'5B09DD97 D24C60A3'	33
3321	'DE3421D9 F1914AFA'	'8A1A69A7 C1E6821A'	29
4221	'AA751B0F 4B793D34'	'47A225FE F7814848'	42
5211	'DFAA06E8 6358D5A2'	'2595DA13 61073C2D'	41
5311	'0C09060A E712B990'	'89BAAA24 E9951723'	33
5421	'BD9D1869 1E3E4079'	'7B7F2D04 36674668'	27
7421	'7BA6CB456 344DC2A'	'1719D41E 937C9F7F'	35
GRAY	'B86DD181 396BF433'	'38D1CE1B 658D3BFB'	33
8421	'259BFC32 3B640C7A'	'D3380DF5 4FBCDAE0'	37

Table 9: Data code is fixed in 8421 code and key varied

Data in 8421	Key : '3B3898371520F75E'		Avalanche Effect
	Data:'ABCDEF01 23456789'	Data:'ABCDEF01 27456789'	
2421	'51D5C358 87F225E0'	'03241206 D5267CB6'	32
3321	'6ACE01AB 18E3BEED'	'B9F3503E 7E76ACD8'	31
4221	'893371A0 F35E9D42'	'F083D019 1F904366'	34
5211	'E26D679B F2125563'	'94384BFE 31820A7D'	32
5311	'30FB4B88 3305A7BF'	'80C37F91 586D4D14'	30
5421	'BB0F578DE ECDB8E7'	'4B2773FE 67DC2A9C'	27
7421	'DE361067 6242E21F'	'6625F098 86BEA3C3'	35
GRAY	'7C19449A 55C9A64B'	'9B80FD64 17BA3ECD'	35
8421	'7D0DFC6A BA2C587D'	'02E82396 14B9CFB1'	43

Table 10: Analysis of Avalanche Effect Due to one bit change in plaintext

Key	Data in Different Code Format								
	2421	3321	4221	5211	5311	5421	7421	GRAY	8421
2421	37	28	26	32	30	38	31	33	32
3321	35	23	38	30	27	38	33	29	31
4221	35	21	29	37	29	33	39	42	34
5211	26	30	38	34	26	33	25	41	32
5311	31	35	25	27	32	42	29	33	30
5421	31	34	34	33	34	29	25	27	27
7421	24	32	32	27	31	29	35	35	35
GRAY	35	33	27	31	30	44	31	33	35
8421	35	34	34	36	37	25	31	37	43

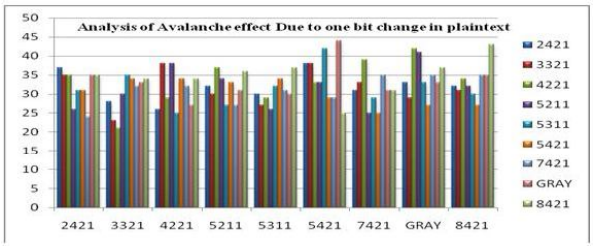

Figure 4 Analysis of Avalanche Effect Due to one bit change in plaintext

6. EXPERIMENTAL RESULTS AND ANALYSIS

Analysis for Data Encryption Standard (DES) algorithm is shown in following tables. The original data to be encrypted and the encryption key used for encryption are mapped into various binary codes.

Table 1 shows the Avalanche Effect when input plaintext kept fixed in a 2421code and encryption key is varied in different codes. Avalanche Effect is calculated by counting the number of flipped bits in the ciphertext due to one bit change in the original plaintext before being mapped in binary code while key remains constant throughout the experiment. Similarly from table 2 to table 9 shows the Avalanche Effect in different conditions when input plaintext kept fixed in a particular binary code and encryption key is varied in different binary codes.

By analyzing table 10 it is clear that Avalanche Effect is maximum (i.e. 44 bits out of 64 bits) when key remain fixed in Gray code and 1 bit is varied in data when it is mapped in 3321 binary code. Figure 4 shows analysis of Avalanche Effect Due to one bit change in plaintext when encryption key is constant .it is clear from figure that maximum Avalanche Effect can be obtained when encryption key is

mapped in Gray code and data is mapped in 3321 binary code. Therefore, if one desires a good avalanche effect; DES is a good option.

7. CONCLUSION

In this paper a slight modification in DES algorithm is proposed. In the proposed algorithm, we have mapped input plaintext and encryption key into various binary codes, instead of giving plaintext directly to the DES algorithm. This leads significant increase in Avalanche Effect of encryption algorithm. We got maximum avalanche effect of **44/64**, when key is mapped in Gray code and Data is mapped in 5421.But due to invertible property of 5421 code some of the code may be duplicated. Therefore this mapping is not suggested as some code (duplicated code) may be decoded wrongly. Our future work will include experiments on image and focus will be to improve security level.

8. ACKNOWLEDGMENT

This paper is a part of our M.E. project. We are grateful to our project guide for valuable suggestions, comments and contribution.

REFERENCES

1. P.Karthigaikumar, Soumiya Rasheed"Simulation of Image Encryption using AES Algorithm" *IJCA Special Issue on "Computational Science - New Dimensions & Perspectives" NCCSE, 2011*
2. Diaa Salama Abd Elminaam, Hatem Mohamad Abdual Kader,Mohiy Mohamed Hadhoud, "Evalution the Performance of Symmetric Encryption Algorithms", international journal of network security vol.10,No.3,pp,216-222,May 2010.
3. Nidhi Singhal, J.P.S.Raina "Comparative Analysis of AES and RC4 Algorithms for Better Utilization" International Journal of Computer Trends and Technology- July to Aug Issue 2011.
4. Akash Kumar Mandal, Chandra Parakash, Mrs. Archana Tiwari "Performance Evaluation of Cryptographic Algorithms:DES and AES" IEEE Students' Conference on Electrical, Electronics and Computer Science (SCEECS), March 2012
5. William Stalling "Cryptography and network security" Pearson education,2nd Edition.

6. Data Encryption Standard Announced by the Federal Information Processing Standards Publication 46-3, 1999 October 25
7. A.Anand Kumar ,"Fundamentals of Digital Circuits", PHI Learning Pvt.Ltd.,2nd Edition
8. Himani Agrawal and Monisha Sharma "Implementation and analysis of various symmetric cryptosystems " Indian Journal of Science and Technology Vol. 3 No. 12 (Dec 2010)
9. Sriram Ramanujam,Marimutha Karuppiah "Designing an algorithm with high avalanche effect" International Journal of Computer Science and Network Security, VOL.11 No.1, January 2011
10. A.Nadeem, "A performance comparison of data encryption algorithms", IEEE information and communication technologies, pp.84-89, 2006.Bn
11. NeetuSettia."Cryptanalysis of modern Cryptography Algorithms". International Journal of Computer Science and Technology. December 2010.
12. Diaasalama, Abdul kader, Mohiy Hadhoud, "Studying the Effect of Most Common Encryption Algorithms", International Arab Journal of e-technology, Vol 2, No.1, January 2011.
13. Ruangchaijatupon,P.Krishnamurthy,"Encryption and power consumption in wireless LANs-n," The Third IEEE workshop on wireless LANS, pp. 148-152, Newton, Massachusetts, sep. 27-28, 2001.

Akash Kumar Mandal received his B.E degree in Electronics and Telecommunication from Pt. Ravi Shankar Shukla University, Raipur, in 2007 and pursuing his post graduation from Swami Vivekananda Technical University, Bhilai in Communication Engineering. His areas of interest Information Security and Cryptography. He is a member of Indian Society for Technical Education (ISTE) and The Institution of Electronics and Telecommunication Engineers (IETE).

Prof. Archana Tiwari received her B.E degree in Electronics and Telecommunication from Amravati in 1994 and completed her post graduation from GEC Jabalpur in 2005. She is pursuing her PhD from Swami Vivekananda Technical University, Bhilai. She has to her credit, more than 20 papers in various International and National Journals and Conferences. With more than 16 years of teaching and research experience .She is currently serving as Associate professor & head in the department of Electronics and Instrumentation, Chhatrapati Shivaji Institute of Technology, Durg. Her areas of interest include image processing, information security and digital watermarking. She is a life member of Indian Society for Technical Education (ISTE) and Institution of Electronics and Telecommunications Engineers (IETE).. She is member of IEEE also.