© 2018 IJSRSET | Volume 4 | Issue 1 | Print ISSN: 2395-1990 | Online ISSN : 2394-4099
Themed Section : Engineering and Technology

Performance Evaluation of IDEA Encryption Model under different Fading Channels

Jagruti A. Patil[1], Prof. Manish M. Patil[2]
[1]P.G. Scholar, Department of E&TC, Gangamai College of Engineering, Dhule, Maharashtra, India
[2]Assistant Professor, Department of E&TC, Gangamai College of Engineering, Dhule, Maharashtra, India

ABSTRACT

With the introduction of the computer and communication, huge amounts of digital information are gathered and stored in giant computer databases and transmitted between computers and terminal devices connected together in complicated communications networks. Without acceptable safeguards the confidentiality and integrity of certain information posses risk because data are vulnerable to interception, deletion, modification or addition throughout transmission. Need of a secured data transmission for exchanging information from one user to the other is increased because of advancements in processing and communication technology. The access of objects in encryption technique relies on key properties that are the basis for communication and authentication. The authentication requires the secured key for data encryption which should be possessed both by user and group. In Wireless Networks, numerous algorithms are used to encrypt/decrypt the message. In this paper the performance of international data encryption algorithm is checked. In proposed algorithm message is split into number of blocks. First block is encrypted using International data encryption algorithm (IDEA) and remaining blocks are EX-ored with the first block. The encrypted data is modulated using BPSK modulation and performance is evaluated in terms of bit error rate and throughput on Additive White gaussian Noise (AWGN) channel.

Keywords*:* IDEA , AWGN, Nakagami, Rayleigh, Rician,Fading, BER, SNR, Throughput.

I. INTRODUCTION

Fast improvement in the information technology ends up in increase in massive data transmission. The forms are completely different, however increasingly; it promotes communication via public data networks, primarily the web. This process is convenient, versatile and cheap.

Exchanging data upon web leads to security problem due to the very fact that the network is public so that anyone can capture the data during transmission. To avoid this, a technique came into existence to make our data secured against the hacking and it is referred as cryptography [32].

Cryptography is employed to secure the data by converting it into such a format which can only be read by the recipient and not by the intruders. Cryptographic algorithms (often known as as ciphers) are special programs designed to safeguard sensitive information on public communication networks. Three cryptography forms usually employed in information systems nowadays are Secret-key ciphers and Public-key ciphers and hash functions [7]:

- ✓ Secret Key Cryptography (SKC) Uses one key for both encryption and decryption; also called symmetric encryption.

- ✓ Public Key Cryptography (PKC): Uses one key for encryption and another for decryption; also called asymmetric encryption.
- ✓ Hash Functions: Uses a mathematical transformation to irreversibly "encrypt" information, providing a digital fingerprint.

Secret-key ciphers: Secret key cryptography methods use a single key for both encryption and decryption. The sender uses the key to encrypt the plaintext and sends the cipher text to the receiver [7].The receiver applies identical key to decrypt the message and recover the plaintext. As a single key is used for both functions secret key cryptography is also called symmetric encryption. With this type of cryptography, it is obvious that the key should be known to both the sender and also the receiver [34]. The most important issue with this approach is the distribution of the key.

Secret key cryptography schemes are usually divided into two classes as either stream ciphers or block ciphers. Stream ciphers operate on a single bit (byte or computer word) at a time and implement some kind of feedback mechanism so that the key is constantly changing whereas block cipher encrypts one block of data at a time using identical key on each block.

Stream ciphers have two main types: Self-synchronizing stream ciphers calculate every bit in the key stream as a function of the previous n bits within the key stream. It is known as "self-synchronizing" as the decryption process can remain synchronized with the encryption process simply by knowing how far into the n-bit key stream it is. It poses a problem of error propagation an erroneous bit in transmission will result in n erroneous bits at the receiving side. Synchronous stream ciphers generate the key stream independent of the message stream however by using a similar key stream generation function at sender and receiver. While stream ciphers don't propagate transmission errors, they are, by their nature, periodic so that the key stream will eventually repeat.

A block cipher encrypts one block of data at a time using identical key on each block. In general, identical plaintext block will always code to identical cipher text when using identical key in a block cipher whereas identical plaintext will encrypt to completely different cipher text in a stream cipher. Block ciphers can operate in one of several modes such as: Electronic Codebook (ECB) mode, Cipher Block Chaining (CBC) mode Cipher Feedback (CFB) mode, Output Feedback (OFB) mode and Counter (CTR) mode

Electronic Codebook (ECB) mode is vulnerable to a range of brute-force attacks. A single bit error within the transmission of the cipher text leads to an error in the entire block of decrypted plaintext. In Cipher Block Chaining (CBC) mode the plaintext is exclusively-ORed (XORed) with the previous cipher text block before encryption so that two identical plaintext blocks will encrypt differently. Output Feedback (OFB) mode prevents identical plaintext block from generating identical ciphertext block by using an internal feedback mechanism that generates the key stream independent of both the plaintext and ciphertext bitstreams. In OFB, one bit error in ciphertext yields one bit error in the decrypted plaintext.

II. CRYPTOGRAPHY ALGORITHMS

Secret key cryptography algorithms in use nowadays include:

A. Data Encryption Standard (DES):

DES was designed by IBM in the Nineteen Seventies and adopted by the National Bureau of standards (NBS) [now the National Institute for Standards and Technology (NIST)] in 1977 as Federal information processing Standard 46 (FIPS 46-3) for commercial and unclassified government applications. DES is a Feistel block-cipher using a 56-bit key that operates on 64-bit blocks.

FIPS-81 describes four modes of DES operation: Electronic Codebook (ECB), Cipher Block Chaining (CBC), Cipher Feedback (CFB), and Output Feedback (OFB). Despite all of these choices, ECB is the most commonly deployed mode of operation [12].

DES uses a 56-bit key. In fact, the 56-bit key is divided into eight 7-bit blocks and an eighth odd parity bit is added to every block. By using the eight parity bits for rudimentary error detection, a DES key is truly 64 bits long for computational purposes though it only has 56 bits worth of randomness.

Two vital variants that strengthen DES are:
Triple-DES (3DES): A variant of DES that employs up to three to 3 to a few 56-bit keys and makes three encryption/decryption passes over the block; 3DES is suggested replacement to DES.

DESX: A variant devised by ron Rivest. By combining 64 additional key bits to the plaintext before encryption, effectively will increase the key length to 120 bits.
NIST finally declared DES obsolete in 2004, and withdrew FIPS (Federal informatics Standards) 46-3, 74, and 81.

B. Advanced encryption standard (AES):

Advanced encryption standard became the official successor to DES in December 2001. The algorithm can use a variable block length and key length; the most recent specification allowed any combination of keys lengths of 128, 192, or 256 bits and blocks of length 128, 192, or 256 bits [13].

C. International data encryption algorithm (IDEA)

International data encryption algorithm (IDEA) is a block cipher designed by Xuejia Laiand James L. Massey of ETH-Zürich and was first delineated in 1991. The block cipher IDEA operates with 64-bit plaintext and cipher text blocks and is controlled by a 128-bit key. The IDEA encryption algorithm Provides high level security not based on keeping the algorithm a secret, but rather upon ignorance of the secret key. It can be economically implemented in electronic components (VLSI Chip)

D. RSA Algorithm:

In cryptography, RSA is an algorithm for public-key cryptography. It was the first algorithm known to be appropriate for signing as well as encryption, and one of the primary great advances in public key cryptography. RSA is widely utilized in electronic commerce protocols, and is believed to be secure given sufficiently long keys and also the use of up-to date implementations. RSA involves a public key and a private key. The public key can be known to everyone and is used for encrypting messages. Messages encrypted with the public key can only be decrypting using the private key [14].

III. FADING CHANNELS

In real world environment, over large distance, signal quality degrades even in the absence of noise this degradation is known as fading. The channel which poses such characteristic is termed fading channel. In real world environment, the radio propagation effects combine together and multipath is generated by these fading channels [19]. Fading channels which are considered for performance analysis of proposed system are listed below.

A. AWGN channel: Additive white gaussian noise (AWGN) channel is a universal channel model for analyzing any new communication system. In this model, the channel adds a white gaussian noise to the signal passing through it. Fading does not exist or if exists than it is of very less amount. The only distortion is introduced by the AWGN. AWGN channel is a theoretical channel used for analysis purpose only.

B. Rayleigh fading channel: The Rayleigh fading is primarily caused by multipath reception. Rayleigh fading is a statistical model for the effect of a propagation environment on a radio signal. Rayleigh

fading is most applicable when there is no line of sight between the transmitter and receiver.

C. Rician fading channel: The Rician fading model is similar to the rayleigh fading model, except that in Rician fading, a strong dominant component is present. This dominant component is a stationary (non-fading) signal and is usually known as the LOS (Line of Sight Component).

D. Nakagami fading channel: it is possible to explain each rayleigh and Rician fading channel with change in only one parameter which is generally denoted mainly as m. Here, as we increase or decrease the value of the nakagami factor m, it changes the value of the probability distribution function towards the Rician or rayleigh fading distribution, respectively.

IV. PROPOSED SYSTEM

A conceptual structure for the transceiver of the proposed encryption mechanism is shown in Figure1. The transmitter structure for the proposed system is illustrated in Figure 1(a), where the incoming serial data stream (S in bits) is mapped into parallel data blocks, each with a common prespecified block length (β_l). First block undergoes a proper encryption algorithm satisfying a certain security level. All the remaining blocks are arranged systematically and enter a bitwise XOR operation with the first block (before encryption, i.e., plaintext), as can be seen from the figure. Next, the data is mapped back into a serial format before transmission to enhance transmission reliability. The data stream is then modulated using BPSK in order to be suitable for transmission. The receiver structure is illustrated Figure 1(b). The receiver completely reverses all the operations performed at the transmitter. Also, at the receiver side, only the first block is decrypted using the appropriate traditional decryption algorithm and the decryption key, whereas all the other blocks are also bit-wise XORed with the first decrypted block (plaintext). As a result, the entire data frame is transmitted securely by performing traditional encryption only on the first small amount of data within a frame or super frame.

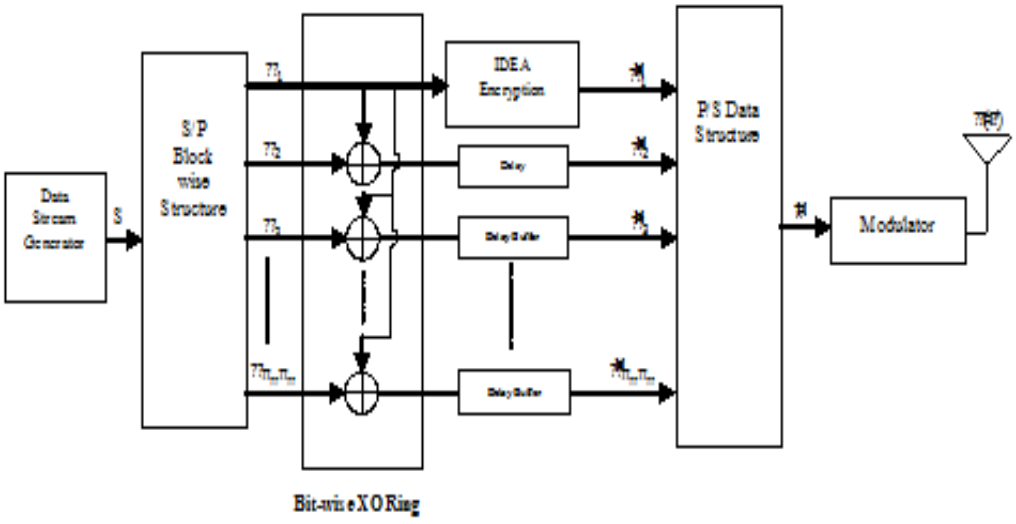

Figure1 (a). Transmitter of proposed system

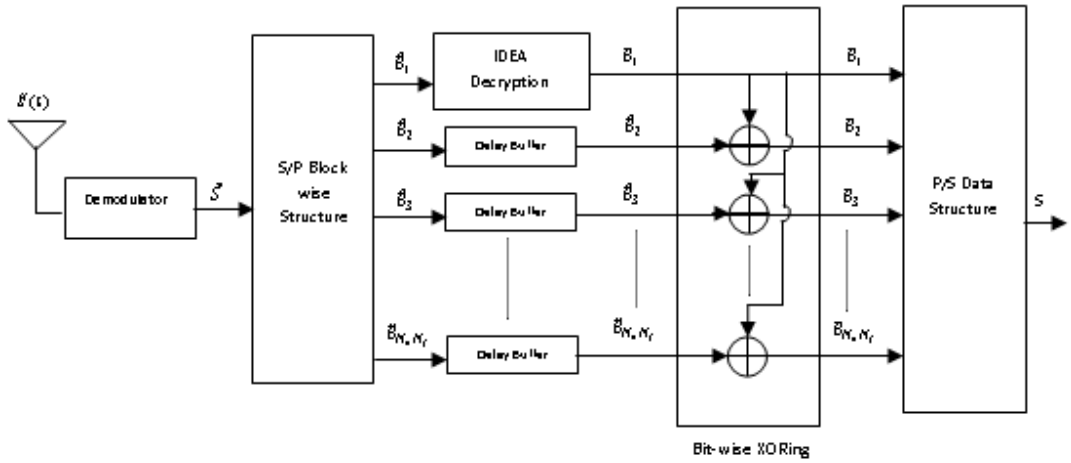

Figure 1(b). Receiver of proposed system

Where,

$S = [B_1, B_2, \dots, B_{N_b N_f}]$

$B_k = [m_1^k, m_2^k, \dots, m_{B_l}^k], k = 1,2,3 \dots, N_b N_f$

$\tilde{B}_1 = E_k[B_1]$

$\tilde{B}_k = B_1 \oplus B_k, k = 2,3, \dots, N_b N_f$

$\tilde{S} = [\tilde{B}_1, \tilde{B}_2, \dots, \tilde{B}_{N_b N_f}]$

V. ALGORITHM

We assume that we have a data sequence composed of N superframes. Each superframe contains N_F frames, and each frame consists of N_b blocks, each of $K = \beta_l$ bits size. We first encrypt the first block, B_1, with the IDEA. Following this step, the rest of the $N_b - 1$ blocks will be used as plain texts(i.e., will not undergo IDEA encryption).In these steps that follow, a bit-wise XOR operation is performed between the plaintext of the first block with each of the remaining $N_b - 1$ blocks and then transmitted to the destination. Consequently, the first block will not be recovered without performing the decryption process, which is assumed to be very immune for cryptanalysis, and therefore the other blocks will not be detected by the intruders since the plaintext of the first block is required to undo the XOR operation. This latter operation can be performed only after decrypting the first block (B_l) at the receiver (see Figur1(b)). By performing the proposed encryption algorithm, following the steps provided in Algorithm, where the first block is first traditionally encrypted and then the XOR operation is performed for the remaining blocks with the plaintext of the first block, the whole resultant data stream will then be secure with security level as high as the security level of the first block. The whole data stream will share the same security level since the XOR operation is a one-to-one mapping function and the data will not be recovered by any intruder without breaking the first cipher. Without loss of generality, we consider a block size of 128 bits. The proposed encryption algorithm is repeated every one superframe or multiple of superframes with a new encryption key. The main reason for having this algorithm repeated every superframe ($N_F$frames) is to use a new key for each superframe to enhance security and reliability of the transmission.

VI. SIMULATION PARAMETERS AND RESULTS

For performance evaluation of proposed system we have considered following parameters:

A. Bit Error rate: The bit error rate or bit error ratio (BER) is the number of bit errors divided by the total number of transferring bits during a studied time interval. BER is a unit less performance measure, often expressed as a percentage.

$$BER = \frac{No.\ of\ bit\ errors\ recieved}{Total\ number\ of\ bits\ transmitted}$$

B. Signal-to-Noise Ratio (SNR): It is a measure which compares the level of a desired signal to the level of background noise. It is defined as the ratio of signal power to the noise power. The ratio is usually measured in decibels (dB). A ratio higher than 1:1 (greater than 0 dB) indicates more signal

than noise. In other words, signal-to-noise ratio is defined as the power ratio between a signal (meaningful information) and the background noise (unwanted signal)

$$\text{SNR} = \frac{\text{P}_{\text{signal}}}{\text{P}_{\text{niose}}}$$

C. **Throughput:** It is defined as the rate of successful message delivery over a communication channel. Mathematically it can be expressed as:

$\text{T} = \text{R}(1 - p_e)^{B_l}$

Where, R = Bit rate

p_e = Bit error probability

B_l = Block length

Table 1 shows simulation parameters used

Table1. Simulation parameters and their values

Simulation Parameter	**Value**
Encryption Technique	IDEA
Modulation Technique	BPSK
Communication Channels	4
No of bits	2560 bits
SNR	0-30 db
Throughput	1366-2560
BER	Varying (10^0 to 10^{-4})

Simulation Results:

Performance of IDEA encryption model for BPSK based secured communication system has been compared over AWGN, Rayleigh, Rician and Nakagami fading channels with a 128 bit key. Simulation is carried out using MATLAB 2015a. Bit error rate and throughput are measured and recorded at distinct values of signal to noise ratio (SNR)through graph is generated as shown in figure 2 and 3.

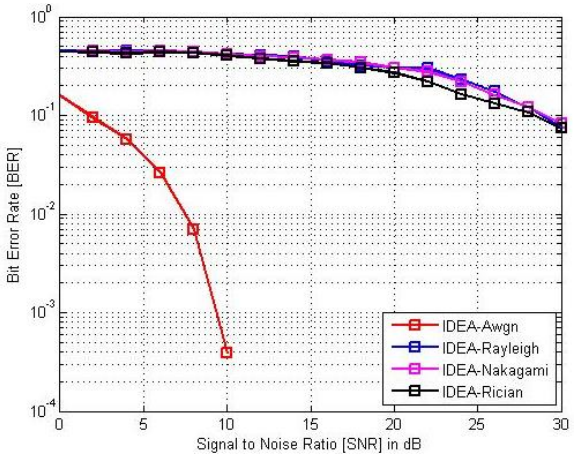

Figure 2. BER performance of IDEA encryption model over AWGN, Rayleigh, Nakagami and Rician channels

Figure 2 shows the comparative analysis of BER performance for IDEA encryption model using different fading channels (AWGN, Rayleigh, Rician and Nakagami). The X axis indicates the SNR value and Y axis is the logarithmic representation of BER. It was found that the BER performance of AWGN channel is better than other communication channels.

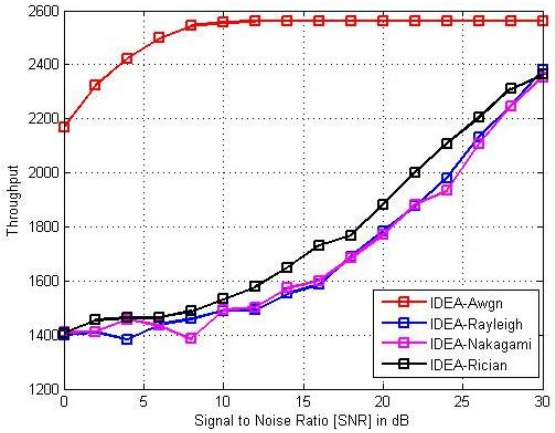

Figure 3. Throughput performance of IDEA encryption model over AWGN, Rayleigh, Nakagami and Rician channels

Figure 3 shows the comparative analysis of throughput performance for IDEA encryption model using different fading channels (AWGN, Rayleigh, Rician and Nakagami). The X axis indicates the SNR value and Y axis is the average throughput. It was found that the throughput performance of AWGN channel is better than other communication channels.

VII. CONCLUSION

In this paper we have analyze the performance of wireless communication in terms of BER and Throughput analysis by using IDEA encryption algorithm. For analysis purpose this data is modulated using BPSK modulation technique. The analysis is derived for BER and throughput assuming different channels wiz; AWGN, Rayleigh, Rician and Nakagami fading channels. It was found that the IDEA encryption model performs better in case of AWGN channel as compared to other communication channels on the basis of BER and Throughput results. It was observed that the performance of Rayleigh fading channel was worst among all channels on the basis of BER and Throughput results. Additionally it conclude that the performance of rician fading channel is worse than that of AWGN channel and better than that of Rayleigh and Nakagami fading channels in terms of BER and Throughput..

VIII. REFERENCES

[1]. M. Matsui, Linear cryptanalysis method for DES cipher, Advances in Cryptology, EUROCRYPT'93, Lecture Notes in Computer Science, vol. 765, T. Helleseth ed., Springer-Verlag, 1994.

[2]. Eli Biham, Adi Shamir, Differential Cryptanalysis of DES-like Cryptosystems, Springer Verlag, 1993.

[3]. A. Menezes, P. Van Oorschot, S. Vanstone, Handbook of Applied Cryptography, CRC Press, 1996.

[4]. Xuelija Lai, On the Design and Security of Block Ciphers, Hartung-Gorre Verlag Konstanz, 1992.

[5]. Vinod Shokeen, Niranjan Yadav, "Encryption and Decryption Technique for Message Communication", IJECT, Vol. 2, Issue 2, June 2011.

[6]. C. Kaufman, R. Perlman, and M. Speciner, Network Security: Private Communication in a Public World, Prentice Hall PTR, 1995.

[7]. "An overview of cryptography" Online available at: https://www.garykessler.net/library/crypto.html

[8]. "An Introduction to Cryptography". Network Associates, Inc., 1999. Online available at: http://www.pgpi.org/doc/pgpintro.

[9]. "The SSL Protocol", version 3.0. Netscape, Inc., 1999. Online available at: http://home.netscape.com/eng/ssl3/draft302.txt.

[10]. Ekta Agrawal, Dr. ParashuRam. Pal, "Refined Polygram Substitution Cipher Method: A Enhanced Tool for Security", International Journal of Engineering and Innovative Technology (IJEIT), ISSN: 2277-3754, Volume 2, Issue 1, July 2012.

[11]. Schneier, Bruce, Applied Cryptography. Protocols, Algorithms, and Source Code in C, New York: Wiley & Sons, 1996.

[12]. Stallings, W. Cryptography and Network Security: Principles and Practice, Prentice-Hall, USA, Second Edition, 1999.

[13]. S. Sudha, V. Madhu Viswanatham "Implementation of Enhanced Data Encryption Standard on MANET with less energy consumption through limited Computation" International Journal of Engineering Research and Development, Volume 2, Issue 4, July 2012.

[14]. Yang Xiao, Bo Sun , Hsiao-Hwa Chen , Sghaier Guizani & Ruhai Wang "Performance Analysis of Advanced Encryption Standard (AES)," in IEEE Communications Society subject matter experts for publication in the IEEE Globocom proceedings 2006.

[15]. Rania Salah el-Sayed "An Efficient Signature System Using Optimized RSA Algorithm" JCSNS International Journal of Computer Science and Network Security, VOL.8 No.12, December 2008.

[16]. Electronic Frontier Foundation, "DES challenge III broken in record 22 hours," January1999. Online available at http://www.eff.org/Privacy/Crypto/Crypto_misc/DESCracker/HTML/19990119_deschallenge3.html .

[17]. J. Daemen, R. Govaerts, and J. Vandewalle, Weak keys for IDEA, Advances in Cryptology - Crypto '93, Springer-Verlag pp. 224-231, 1994.

[18]. J. Borst, L.R. Knudsen and V. Rijmen, Two Attacks on Reduced IDEA, Advances in

Cryptology - EUROCRYPT 1997, Springer-Verlag, pp. 1-13, 1992.

[19]. T. M. Cover and A. A. E. Gamal, "Capacity theorems for relay channel", IEEE Trans info Theory,vol.25, no.5,pp. 572-84, Sept 1979.

[20]. A. Sudhir Babu, Dr. K.V Sambasiva Rao, "Evaluation of BER for AWGN, Rayleigh and Rician Fading Channels under Various Modulation Schemes", International Journal of Computer Applications, ISSN: 0975 – 8887, Volume 26, No.9, July 2011.

[21]. Nuzhat Tasneem Awon, Md. Mizanur Rahman, Md. Ashraful Islam, A. Z. M. Touhidul Islam, "Effect of AWGN & Fading (Raleigh & Rician) channels on BER performance of a WiMAX communication System", International Journal of Computer Science and Information Security (IJCSIS), Vol. 10, No. 8, August 2012.

[22]. M. N. Rindani, A. A. Bavarva, "Ber Performance Comparison of 4×4 Extended Alamouti Scheme for Different Fading Channels", International Journal of Advanced Research in Electrical, Electronics and Instrumentation Engineering, Vol. 2, Issue 3, March 2013.

[23]. Battu Deepa, P.Sudhakara Reddy, "Comparison of Bit Error Rate and Signal to Noise Ratio for Multi-User MIMO Wireless Applications", International Journal of Innovative Technology and Exploring Engineering (IJITEE), ISSN: 2278-3075, Vol. 3, Issue 3, August 2013.

[24]. Sutanu Ghosh, "Performance Analysis on the basis of a Comparative Study between Multipath Rayleigh Fading and AWGN Channel in the presence of various Interference", International journal of Mobile Network Communications & Telematics (IJMNCT) Vol. 4, No.1, February 2014

[25]. Vinod Shokeen, Niranjan Yadav, "Encryption and Decryption Technique for Message Communication",International Journal of Electronics & Communication Technology (IJECT), ISSN: 2230-7109, Vol. 2, Issue 2, June 2011.

[26]. E. Thambiraja & Dr. R. Umarani , "A Survey on Various Most Common Encryption Techniques", International Journal of Advanced Research in Computer Science and Software Engineering ,Volume 2, Issue 7, July 2012.

[27]. Mustafa M. Matalgah, Amer M. Magableh, "Simple Encryption Algorithm with Improved Performance in Wireless Communications", IEEE, Radio and Wireless Symposium (RWS), January 2011.

[28]. Agarwal, Dafouti & Tyagi "Performance analysis of data encryption algorithms (DES)", Electronics Computer Technology (ICECT), 3rd International Conference on 10 April 2011.

[29]. Suying Yang, Hongyan Piao, Li Zhang and Xiaobing Zheng, "An Improved IDEA Algorithm Based on USB Security Key", Third International Conference on Natural Computation (ICNC), 2007.

[30]. De-Hong ZHU, "An Attack on 5.5-round IDEA", IEEE International Conference on Intelligent Computing and Intelligent Systems (ICIS), Vol. 2, PP. 18 – 21, 2010.

[31]. Sandipan Basu "International data encryption algorithm (IDEA)" Journal of Global Research in Computer Science Volume 2, No. 7, July 2011.

[32]. Harivans Pratap Singh, Shweta Verma, Shailendra Mishra, "Secure-International Data Encryption Algorithm", International Journal of Advanced Research in Electrical, Electronics and Instrumentation Engineering, ISSN: 2278 – 8875, Vol. 2, Issue 2, February 2013.

[33]. Archita Bhatnagar, Monika Pangaria, Vivek Shrivastava, "converting international data encryption algorithm (idea) into asymmetric key cipher", International Journal of Innovative Research in Science, Engineering and Technology volume 2 issue 10, October 2013

[34]. Ayushi, "A Symmetric Key Cryptographic Algorithm",2010 International Journal of Computer Applications (0975 - 8887) Volume 1 – No. 15