# Achieving Data Security in Wireless Sensor Networks Using Ultra Encryption Standard Version – IV Algorithm

A.Praveena,
Assistant Professor, Department of Computer Science and Engineering,
Jansons Institute of Technology, Coimbatore
praveenasngp@gmail.com

***Abstract*— Nowadays wireless networks are fast, becoming more secure than their wired counterparts. Recent technological advances in wireless networking, IC fabrication and sensor technology have lead to the emergence of millimetre scale devices that collectively form a Wireless Sensor Network (WSN) and are radically changing the way in which we sense, process and transport signals of interest. They are increasingly become viable solutions to many challenging problems and will successively be deployed in many areas in the future such as in environmental monitoring, business, and military applications. However, deploying new technology, without security in mind has often proved to be unreasonably dangerous. This also applies to WSNs, especially those used in applications that monitor sensitive information (e.g., health care applications).**

***There have been significant contributions to overcome many weaknesses in sensor networks like coverage problems, lack in power and making best use of limited network bandwidth, however; work in sensor network security is still in its infancy stage. Security in WSNs presents several well-known challenges stemming from all kinds of resource constraints of individual sensors. The problem of securing these networks emerges more and more as a hot topic. Symmetric key cryptography is commonly seen as infeasible and public key cryptography has its own key distribution problem. In contrast to this prejudice, this paper presents a new symmetric encryption standard algorithm which is an extension of the previous work of the authors i.e. UES version-II and III. Roy et al recently developed few efficient encryption methods such as UES version-I, Modified UES-I, UES version-II, UES version-III. The algorithm is named as Ultra Encryption Standard version – IV algorithm. . It is a Symmetric key Cryptosystem which includes multiple encryption, bit-wise reshuffling method and bit-wise columnar transposition method. In the present work the authors have performed the encryption process at the bit-level to achieve greater strength of encryption. The proposed method i.e. UES-IV can be used to encrypt short message, password or any confidential key.***

***Keywords*—Cryptography, Sensor networks, Energy Efficient.**

## I. INTRODUCTION

In recent digital communication era, sharing of information is increasing significantly. The information being transmitted is vulnerable to various attacks. Therefore, the information security is one of the most challenging aspects of communication in any modern network. WSN's are quickly gaining popularity that they are potentially low cost solutions to a variety of real world challenges and are expected to play an essential role in the upcoming age of pervasive computing. However, the highly constrained nature of sensors imposes a difficult challenge: their reduced availability of memory, processing power and energy hinders the deployment of many modern cryptographic algorithms considered secure. For this reason, the choice of the most memory-, processing- and energy-efficient security solutions is of vital importance in WSNs. To date, several authors have developed extensive analyses comparing different encryption algorithms.

WSNs can be seen as a special type of ad-hoc network composed by a large number of tiny, cheap and highly resource constrained sensor nodes, known as motes. The sensors are distributed in the area of interest, and can then gather and process data from the environment (e.g., mechanical, thermal, biological, chemical, and optical readings). They have applications in a variety of fields such as environment monitoring which involves monitoring air, soil and water, condition based maintenance, habitat monitoring (determining the plant and animal species population and behavior), seismic detection, military surveillance, inventory tracking, smart spaces and gathering sensing information in inhospitable locations, medical and home security to machine diagnosis, chemical/biological detection etc. Motes are typically battery-powered, which has motivated considerable research efforts on the development of energy aware protocols, such as data link layer protocols. In general, one of the main goals driving the design of these schemes is to optimize network communications in order to save energy, and thus extend the network's lifetime.

Security is often very sadly considered at the very last step in the design of WSNs. Actually, most WSN deployments do not even consider security among their requirements because the execution and energy overheads it adds to the system is seen as an undesirable "extra cost" in such constrained environments. From national defense, medical applications, to the environment, the data delivered from the sensor networks are unstructured, using their own format and protocols. Sensor networks are delivering near-real-time information to scientists worldwide. Extracting this information to gain knowledge and understanding is one of the greatest challenges faced today.

978-1-5090-5778-8/17/$31.00©2017 IEEE

However, in WSN-based applications that monitor sensitive information, it is essential to prevent eavesdropping, which is typically obtained by means of encryption algorithms (e.g., symmetric ciphers). Even when the information acquired is not confidential, it is still necessary to ensure data integrity and authenticity by means of message authentication mechanisms, since the acceptance of invalid data (generated either by natural causes or with malicious purposes) could lead to mistaken actions and severe consequences. Finally, given that such algorithms depend on the existence of secret keys for their functioning, applications need also to handle these keys' distribution.

Due to complexity of calculation the public key cryptosystem may not be suitable in a case like sensor networks where the excess battery voltage consumption is not permissible. So in sensor networks we have to adopt some effective encryption method which should not consume the battery voltage too much. In the present work the author have proposed a new symmetric key method called Modern Encryption Standard Version II (MES-II) which can be used to encrypt data in sensor network, mobile network, and ATM network, defense or even in corporate sector also. The present method may be very useful to encrypt password, short message, encryption key etc.

### *A. Contributions of the Paper*

This paper is intended to be an introduction to WSN—with an emphasis on structural and environmental monitoring applications. A thorough but general survey of the area and referring to several papers in the computer science and engineering literature detailed information were given. In this paper for achieving security the author have used a new encryption algorithm called Ultra Encryption Algorithm version – IV (UES ver – IV). The algorithm provides the combined strength of bit-level reshuffling and a Bit-wise columnar transposition method. The rest of the paper is described as follows. Section 2 discusses the background information for architecture of WSN and components of a sensor node. The motivation for the proposed scheme presented is discussed in Section 3. Section 4 discusses related work. Section 5 discusses the proposed scheme. Conclusions and future work conclude the paper.

## II. Sensor Networks Architecture

The sensor nodes are usually scattered in a sensor field. Each of these scattered sensor nodes has the capabilities to collect data and perform partial or no processing on the data. Each sensor node has the required infrastructure to communicate with the other nodes. Data are routed back to the sink/base station by a multihop infrastructure less architecture through the sink. A distinguished special type of node is called as gateway node. Gateway nodes are connected to components outside of the sensor network through long range communication (such as cables or satellite links), and all communication with users of the sensor network goes through the gateway node.

The sink node communicates with the task manager via core network which can be Internet or Satellite. Since Sensors are low cost, low power, and small in size, the transmission power of a sensor is limited. The data transmitted by a node in the field may pass through multiple hops before reaching the sink. Many route discovery protocols (mostly inherited from Ad hoc networks) have been suggested for maintaining routes from field sensors to the sink(s). Due to low memory, scarcity of available bandwidth and low power of the sensors, many researchers considered these separate route discovery mechanisms undesirable.

Once sensors are deployed they remain unattended, hence all operations e.g. topology management, data management etc. should be automatic and should not require external assistance. In order to increase the network life time, the communication protocols need to be optimized for energy consumption. It means a node must be presented lowest possible data traffic to process.

The sensor node is made up of four basic components: a sensing unit, a processing unit, a transceiver unit and a power unit. They may also have additional application-dependent components such as a location finding system, power generator and mobilizer. Sensing units are usually composed of two subunits: sensors and analog to digital converter. The analog signals produced by the sensors based on the observed phenomenon are converted to digital signals by the ADC, and then fed to the processing unit. The processing unit is generally associated with a small range a small storage unit, manages the procedures that make the sensor node collaborate with the other nodes to carry out the assigned sensing tasks. A transceiver unit connects the node to network. One of the most important components is the power unit. Power unit may be supported by power scavenging units such as solar cells. There are also other subunits that are application dependent.

The emergence of sensor networks as one of the dominant technology trends in the coming decades has posed numerous unique challenges to researchers. These networks are likely to be composed of hundreds, and potentially thousands of tiny sensor nodes, functioning autonomously, and in many cases, without access to renewable energy resources. Cost constraints and the need for ubiquitous, invisible deployments will result in small sized, resource-constrained sensor nodes. While the set of challenges in sensor networks are diverse, we focus on fundamental security challenges in this paper.

## III. Security Issues in WSN

Because the sensor nodes are battery powered, increasing the autonomous lifetime of a WSN is a challenging optimization problem. Communication of data within a WSN is one of the most energy-expensive tasks a node undertakes – using data compression to reduce the number of bits sent reduces energy expended for communication. Data compression which highly reduces the communication overhead by aggregating and compressing data packets can be performed at intermediate sensor nodes. However, compression requires computation, which also expends energy. Fortunately, trading computation for communication can save energy that typically on the order of 3000 instructions can be executed for the energy cost required to communicate one bit over a distance of 100 m by radio.

Apart from achieving energy efficiency many WSN applications that span military and civilian use assume that the sensor nodes will be deployed hostile environments and thus be prone to a wide variety of malicious attacks. As a result, security becomes a key concern. WSN's are particularly vulnerable to several key types of attacks, such as denial of service attacks, traffic analysis, privacy violation, physical attacks, node take overs, attacks on routing protocols, etc.

The data transported and exchanged between sensor nodes is critical. Such data has to be protected against threats in a way so classic security properties like integrity, authenticity or confidentiality can be guaranteed[12].To accomplish such security goals in modern networks like the Internet or companies LAN cryptographic primitives like encryption / decryption as well as signature schemes are usually needed. Keys for encryption purposes must be agreed upon by communicating nodes. Due to resource constraints, achieving such key agreement is non-trivial. Many key agreement schemes used in general networks, such as Diffie-Hellman and public-key based schemes, are not suitable for WSN's. Pre-distribution of secret keys for all pairs of nodes is not viable due to the large amount of memory used when the network size is large.

The lack of a fixed infrastructure and ad hoc nature of WSN deployments suggest that ability to encrypt and decrypt confidential data among arbitrary sensor nodes while enabling undisputed authentication of all parties will be a fundamental prerequisite for achieving security. To do this, nodes must be able to establish a secret key and know who their counterparts are. Thus, it becomes highly desirable to have a secure and efficient distribution mechanism that allows simple key generation for large-scale sensor networks while facilitating all the necessary authentications.

Although a variety of key-generation methods have been developed, they cannot be directly applied to sensor network environments due to the problems such as very limited resources (memory, power), unreliable communication (unreliable transfer, conflicts, latency), Unattended Operation (Exposure to Physical Attacks, Managed Remotely, No Central Management Point) etc. Due to these constraints it is difficult to directly employ the existing security approaches to the area of wireless sensor networks.

## IV. Previous Work

Because of the problems mentioned in previous section security is commonly considered as a delicate problem. One security aspect that receives a great deal of attention in WSN is the area of key management. The two possibilities for achieving security are to use symmetric cryptography and public key cryptography. Two of the major techniques used to implement public-key cryptosystems are RSA and elliptic curve cryptography (ECC).

But most security work on WSN focuses on the search for and development of alternatives to classical public-key algorithms and public key infrastructures. Recent work has challenged notion that Diffie-Hellman and public key based schemes are infeasible in WSNs. In [1] Gura et al. report that both RSA and elliptic curve cryptography are possible using 8-bit CPUs with ECC demonstrating a performance advantage over RSA. Another advantage is that ECC's 160-bit keys result in shorter messages during transmission compared the 1024 bit RSA keys. In particular Gura et al. demonstrate that the point multiplication operations in ECC are an order of magnitude faster than private-key operations within RSA, and are comparable to the RSA public-key operation [1].

In [2], Watro et al. show that portions of the RSA cryptosystem can be successfully applied to actual wireless sensors, specifically the UC Berkeley MICA2 motes [2]. In particular, they implemented the public operations on the sensors themselves while offloading the private operations to devices better suited for the larger computational tasks.

Shamir proposed the idea of identity-based cryptography in 1984, and described an identity-based signature scheme in the same article. However, practical Identity-based encryption (IBE) schemes were not found until recently with the work of Boneh and Franklin and Cocks in 2001. Cocks's scheme is based on the Quadratic Residuosity Problem, and although encryption and decryption are reasonably fast (about the speed of RSA), there is significant message expansion, i.e., the bit-length of the ciphertext is many times the bit-length of the plaintext. We must note that ID-based encryption has some disadvantages. Private key generator (PKG) is responsible for generating private keys for all users, and it is a performance bottleneck for organizations with large number of users. Another disadvantage is that, PKG knows Bob's private key, i.e., key escrow is inherent in ID-based systems. Review of security issues and various attacks and summary of security schemes is given.

The generalized modified vernam cipher method with feedback with fixed block size was developed by many authors. After that the work was done on "Symmetric key Cryptography using two-way updated – Generalized Vernam Cipher method: TTSJA algorithm" [13], where the use of two different algorithms were made to make the encryption process too hard. It was applied on some known text where the same character repeats number of times and we found that after encryption in the output pattern there is no repetition of pattern in the output string. The key matrix is of size 16x16.

This key may be generated in 256! ways. This method uses modified vernam cipher method and vernam cipher method using XOR operation. This method too is a block cipher method and is hard to implement due to complex computational operations. Here, new encryption algorithm concept "Ultra Encryption Standard (UES) Version-I: Symmetric Key Cryptosystem using generalized modified Vernam Cipher method, Permutation method and Columnar Transposition" by Satyaki Roy et. al, method came to the scene of Cryptosystem. It combines three different methods namely, Generalized Modified Vernam Cipher method, Permutation method and Columnar Transposition method. Using combination of different encryption algorithms doesn't lead to good security ethics.

Also combination of different algorithms came into picture for effective encryption results. "An Integrated Symmetric Key Cryptographic Method – Amalgamation of TTJSA Algorithm, Advanced Caesar Cipher Algorithm, Bit Rotation

and Reversal Method: SJA Algorithm" by Somdip Dey, Joyshree Nath, Asoke Nath. [17] In these work three different algorithms are used namely TTJSA, Caesar Cipher & Bit Rotation Method to make the encryption process unbreakable from standard cryptographic attack. The spectral analysis shows that method is unbreakable. The output results were same as compared to above algorithm in respect of repetition of pattern. It was tested closely and has found satisfactory result in almost all cases. But, the obvious pattern of Caesar Cipher Encryption Method, is not used, instead variable numerical number should be used.

And finally the independent algorithm came into effect rather than combination of two or three or more algorithms i.e. "Modern Encryption Standard (MES) Version-I: An Advanced Cryptographic Method" by Somdip Dey, Asoke Nath [13]. The proposed method was Modern Encryption Standard version-I (MES version-I) and, the method is achieved by splitting the file, which is to be encrypted, and encrypting the split sections of the file in various ways using TTJSA and DJSA cipher methods. The method has been tested on different files and the results were very satisfactory.

The Modern Encryption Standard (MES): Version-I has satisfactory results but was less secure due to noncomplex & obvious encryption technique. Also, many authors have put forward the ideas and concept behind Symmetric Key cryptography. Integration or combinations of various different encryption algorithms such as DJSA, DJMNA, NJSSA, SJA, Advanced Caeser Cipher Method, etc. have special impact on security.

## V. Proposed Work

As the literature review has the greater impact on efficiency and more secure cryptography, we have to implement Modern Encryption Standard Cryptography for Data security purpose. Also we need to cross check that the processing and implementation of the algorithm should not cause corruption of information in the original data or message and also the size of the enciphered text should not be larger than the original plain text. And there should be no repetition of pattern in the output, which is to be taken care of, while implementing the Modern Encryption Standard (MES) algorithm. The cryptographic method suggested in this paper is a type of new symmetric encryption standard algorithm which is an extension of the previous work of the authors i.e. UES version-II and III. Roy et al recently developed few efficient encryption methods such as UES version-I, Modified UES-I, UES version-II, UES version-III. Here the authors have used three different type of cryptographic method .Those methods are multiple encryption, bit-wise reshuffling method and bit-wise columnar transposition method. This system is the extension of UES-III and partly UES II.

The UES Version- IV algorithm comprises of two distinct methods (i) Bit-level Encryption Technique with Columnar Transposition method which the author used in UES-I in byte level, (ii) Bit-level reshuffling method. Now we will describe in detail UES IV algorithm.

### *A. Encryption Algorithm*

The algorithm integrates bit-level columnar transposition and bit wise reshuffling. It computes 'cod' which controls the multiple encryption number and 'v' which is the columnar sequence generator. It splits the plain files into bits, encrypts it and then converts it back to bits. The diagram below shows the working of the UES IV algorithm. It initially extracts 2 bytes at a time and performs bitwise reshuffling and columnar transposition of the extracted data. It then extracts the next 2 bytes and performs the same process until the entire file is encrypted or the number of residual bytes is less than the number of extracted bytes. It then repeats the same procedure by extracting 8, 32 and 128 bytes of plain text bytes at a time.

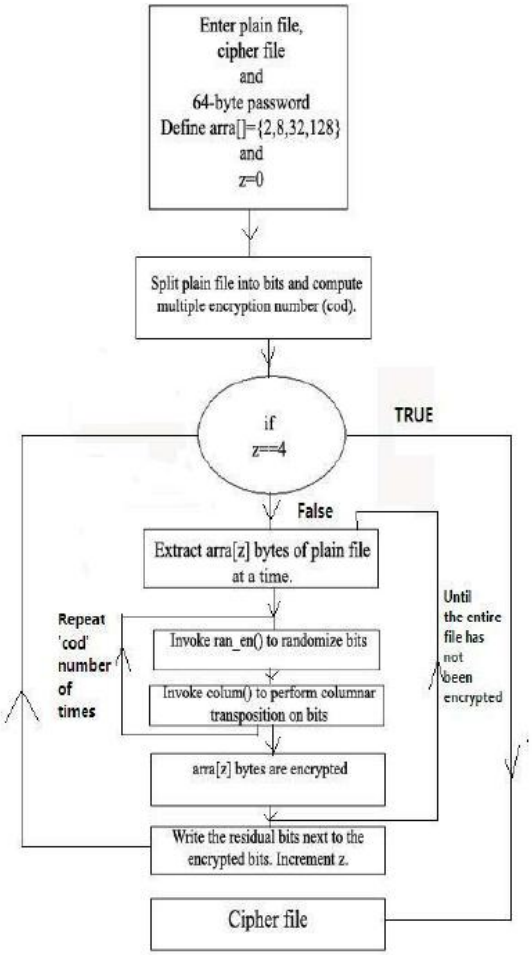


Fig. 1. Representation of UES IV

## VI. Conclusion and Future Enhancements

As the applications of WSN tend to increase more rapidly, the problem of achieving energy efficient communication and securing them against attacks becomes much more important. Without proper security, it is impossible to completely trust the results reported from sensor networks deployed outside of controlled environments. In this paper we have seen how one can use UES –IV algorithm to achieve secure communication. The method is very much flexible in comparison to any standard methods. the authors have combined the two modules

of bit-level randomization and Advanced Bit-wise Encryption Technique with columnar transposition. The algorithm works at the bit-level and the quality and strength of encryption obtained is significantly higher than the techniques that work with bytes. This method is applicable to different type of fields such as banking sectors, defense, short message encryption as well as large text encryption.

In the previous endeavors of UES Version-I, UES Modified Version-I and UES Version-II, the authors have worked exclusively on bytes. In the present work the entire encryption process is performed at the bit-level. The algorithm takes care of plain text inputs such as ASCII 2 and many occurrences of same character. Even when the same characters are provided as input, the cipher files have almost no occurrence of repetitive patterns. The columnar transposition module with bits has been utilized for the first time. The use of multiple encryptions and the role of the password provided by the user have also been demonstrated in the test results.

This method is too hard to break by using any kind of brute force method. As mentioned before have applied our method on some known text where the single character repeats itself for a number of times and we have found that after encryption there is no repetition of pattern in the output file. Moreover, it must be remembered, if the cipher file is tampered and certain character(s) in the file get altered, it would be impossible to retrieve the plain file, since the feedback generated will be different for different characters. The present method will not work if the plain text file contains all ASCII character 255 or ASCII character 0.

## REFERENCES


[1] N. Gura, A. Patel, A. Wander, H. Eberle, and S. Shantz, 2004 Comparing elliptic curve cryptography and RSA on 8-bit cpus. *In 2004 workshop on Cryptographic Hardware and Embedded Systems,* Aug.

[2] R. Watro, D. Kong, S. Cuti, C. Gardiner, C. Lynn, and P. Kruus, 2004 Tinypk: Securing sensor networks with public key technology. *Proceedings of 2nd ACM workshop on Security of Ad hoc and Sensor Networks (SASN '04)*, pp. 59–64. ACM Press.

[3] William Stallings, 2003, Cryptography and Network Security. P.Hall.

[4] G. Hanaoka, T. Nishioka, Y. Zheng, and H. Imai. An efficient [hierarchical identity based key-sharing method resistant against collusion-attacks, *in Advances in Cryptology – Asiacrypt 1999, Lecture Notes in CS **1716** (99),* Springer, 348–362.

[5] J. Horwitz and B. Lynn. Toward Hierarchical Identity-Based Encryption, *in Advances in Cryptology – Eurocrypt 2002, Lecture Notes in Computer Science **2332** (2002), Springer,* 466–481.

[6] Aashima Singla and Ratika Sachdeva, Review of Security Issues and attacks in WS N, in International Journal of Advanced Research in Computer Science and Software Engineering, Vol 3, Iss 4, Apr 13, ISSN 2277-128X.

[7] Symmetric key cryptosystem using combined cryptographic algorithms Generalized modified Vernam Cipher method,MSA and NJJSAA: TJSA algorithm-Proceedings of Information and Communication Technologies(WICT), 2011, held at Mumbai 11th -14th, Dec2011, pg 1175 – 1180.

[8] Al-Sakib Khan Pathan, Hyung-Woo Lee,, Choong Seon Hong, Security in Wireless Sensor Networks: Issues and Challenges, ICTACT, 2006, ISBN – 89 – 5519 – 129 – 4.

[9] Somdip Dey, Asoke Nath, "Modern Encryption Standard (MES) Version-I: An Advanced Cryptographic Method", , *Proceedings of IEEE 2nd World Congress on Information and Communication Technologies (WICT- 2012), pp. 242-247*.

[10] Dripto Chatterjee, Joyshree Nath, Sankar Das, Shalabh Agarwal and Asoke Nath, Symmetric key Cryptography using modified DJSSA symmetric key algorithm:. *Proceedings of International conference Worldcomp 2011 held at LasVegas 18-21 July 2011, Page-306-311, V1*

[11] Symmetric key Cryptography using two-way updated – Generalized Vernam Cipher method: TTSJA algorithm. *International Journal of Computer Applications (IJCA, USA), Vol 42, No.1, March, Pg: 34 - 39(2012).*

[12] Ultra Encryption Standard(UES) Version-I: Symmetric Key Cryptosystem using generalized modified Vernam Cipher method, Permutation method and Columnar Transposition method: Satyaki Roy, Navajit Maitra, Joyshree Nath,Shalabh Agarwal and Asoke Nath. *Proceedings of IEEE sponsored National Conference on Recent Advances in Communication, Control and Computing Technology-RACCCT 2012, 29-30 March held at Surat, Page 81-88(2012).*

[13] An Integrated Symmetric Key Cryptographic Method – Amalgamation of TTJSA Algorithm, Advanced Caesar Cipher Algorithm, Bit Rotation and reversal Method: SJA Algorithm. *International Journal of Modern Education and Computer Science, Somdip Dey, Joyshree Nath, Asoke Nath,(IJMECS), ISSN: 2075-0161 (Print), ISSN: 2075-017X (Online), Vol-4, No-5, Page 1-9,2012.*

[14] Symmetric Key Cryptography using Random Key generator: Asoke Nath, Saima Ghosh, Meheboob Alam Mallik: *Proceedings of International conference on security and management (SAM'10" held at Las Vegas, USA Jull 12-15, 2010), Vol-2, Page: 239-244(2010).*

[15] *Advanced* Symmetric key Cryptography using extended MSA method: DJSSA symmetric key algorithm: Dripto Chatterjee, Joyshree Nath, Soumitra Mondal, Suvadeep Dasgupta and Asoke Nath, *Jounal of Computing, Vol 3, issue-2, Page 66-71,Feb(2011).*

[16] New Symmetric key Cryptographic algorithm using combined bit manipulation and MSA encryption algorithm: NJJSAA symmetric key algorithm: Neeraj Khanna, Joel James,Joyshree Nath, Sayantan Chakraborty, Amlan Chakrabarti and Asoke Nath *: Proceedings of IEEE CSNT-2011 held at SMVDU(Jammu) 03-06 June 2011, Page 125-130(2011).*

[17] An Integrated symmetric key cryptography algorithm using generalized vernam cipher method and DJSA method: DJMNA symmetric key algorithm : Debanjan Das, Joyshree Nath, Megholova Mukherjee, Neha Chaudhury and Asoke Nath: Proceedings of IEEE International conference : World Congress WICT-2011 to be held at Mumbai University 11-14 Dec, 2011, Page No.1203-1208(2011).

[18] Ultra Encryption Standard (UES) Version-II: Symmetric Key Cryptosystem using generalized modified Vernam Cipher method, Permutation method, Columnar Transposition method and TTJSA Method, Satyaki Roy, Navajit Maitra, Shalabh Agarwal and Asoke Nath, Proceedings of the 2012 International Conference on Foundation of Computer Science, held at Las Vegas, July 14-19, Page 97-104.

[19] Ultra Encryption Standard (UES) Version-III: Symmetric Key Cryptosystem With Bit-level Encryption Algorithm, Satyaki Roy, Navajit Maitra, Shalabh Agarwal, Joyshree Nath, Asoke Nath, International Journal of Modern Education and Computer Science (IJMECS), Volume 4 Number 7, July 2012.

[20] Advanced Steganography Algorithm using encrypted secret message : Joyshree Nath and Asoke Nath, International Journal of Advanced Computer Science and Applications, Vol-2, No-3, Page-19-24, March(2011).

[21] Advanced Digital Steganography using Encrypted Secret Message and Encrypted Embedded Cover File, JoyshreeNath, SaimaGhosh and AsokeNath, International Journal of Computer Applications(IJCA 0975-8887), Vol 46, No-14, May ,(2012).