ISSN: 0976-3031

Available Online at http://www.recentscientific.com

CODEN: IJRSFP (USA)

International Journal of Recent Scientific Research
Vol. 9, Issue, 10(E), pp. 29399-29404, October, 2018

International Journal of Recent Scientific Research

DOI: 10.24327/IJRSR

Research Article

ANALYSIS OF IMPREGNABLE CIPHERS IN MANET

Srividya R[1] and Ramesh B[2]

[1]Dept of Telecommunication Engineering, K. S. Institute of Technology Bangalore, India
[2]Dept of Computer Science Engineering, Malnad College of Engineering Hassan, India

DOI: http://dx.doi.org/10.24327/ijrsr.2018.0910.2855

ARTICLE INFO

Article History:

Received 13th July, 2018
Received in revised form 11th August, 2018
Accepted 8th September, 2018
Published online 28th October, 2018

Key Words:

MANET, Encryption, Decryption, Key, AES, DES, RSA, Algorithm.

ABSTRACT

The contemporary decade has seen a major growth in the sphere of Mobile Ad hoc Networks, which has exceptionally changed the way mobile devices are handled, their standards, operating systems, databases and network implementation. Mobile Ad hoc Networks, due to their inherent features make them pregnable to adversaries and spiteful or pernicious attacks. As a consequence providing security by means of cryptographic algorithms in these network genres is a factor of precedence. Amidst prolific cryptographic algorithms, encryption algorithms play a cardinal role in information security systems. Encryption algorithms are avowed to be methodical and intensive computationally. They expend notable amount of computing amenities. Outlining an energy efficient security algorithm requires in inceptive a light weight algorithm and perception of the data related to energy squander. This paper presents in detail, classification of diverse genre of encryption algorithms used in Mobile Ad hoc Networks. It also presents the applications of encryption algorithms in use till date.

INTRODUCTION

In contemporary years, Mobile Ad hoc Networks (MANETs) have emanate as posterity of wireless networking technology. However, reliability plight in MANET has become one of the cardinal concerns. As we know, MANETs are basically wireless in nature they are pregnable to security infringements in excess compared to wired networks. As a repercussion, MANETs are affected with spiteful goals that disrupt their operation.

The key snag is potential breaching of the system by submissive surveillance and subterfuge. Further it is intricate by assorted nature of wireless environment [1]. Security is provided through confidentiality, security aid of its kind. The intent of confidentiality is to sway access of sensitive information for legitimate individuals only. Since MANET uses an open medium, all nodes within the transmission horizon can procure the data. An efficient way of keep information confidential is by using encryption strategies. Nevertheless, the major threats to confidentiality are the compromised nodes, provided cryptographic keys are not encrypted and stored in the node [2].

In providing MANET security, key management is also one of the challenges. In a way to prevent malicious nodes from unifying and procuring access to symmetric encryption key, it is imperative to authenticate the nodes when they endeavor to unite. It is obligatory to design a light weight and storage efficient key management formula, due to restricted MANET resources and computational capability [3] [4].

Umpteen cryptographic and key management stratagems have been frame worked to support MANET in this regard. A minority of these adapt to be applicable to network prerequisite, while others are known to be computationally behest. These stratagems consume considerable volume of computing resources [5]. There are five primary aspects like Confidentiality, Integrity, Non-repudiation, Authentication and Key exchange, that are associated with cryptography and also there is adequate information to proclaim the efficiency of divergent encryption techniques in usage today.

Related Work

S. Sridevi Sathya Priyae *et.al*, [17]-[19], in their paper, ”Evaluation of Symmetric Encryption Algorithms”, provided information about generation of keys using fingerprint feature and devised a mixed random key generation algorithm.

Umaparvathi *et.al*, [9], presented juxtaposition between Blowfish, DES, 3DES and AES encryption algorithms, in terms of power utilization. Relative study was carried on these

Corresponding author:* **Srividya R
Dept of Telecommunication Engineering, K. S. Institute of Technology Bangalore, India

encryption strategies using diverse data types. They experimented to conclude that software encrypts different file formats. Also the results were correlated and calculated to obtain throughput based on encryption and decryption time. Their simulation results inferred that efficiency of AES is superior compared to its counter parts and this is making AES an exceptional candidate.

Mandal. A. K, *et.al*, [8], presented a research that investigated globally employed symmetric encryption strategies, AES and DES. These encryption strategies were compared on specific points, were the key was kept constant and due to one bit variation in plaintext these points avalanched the effect of simulation period involved for encryption and memory entailed for implementation. Conclusively authors inferred that AES encryption algorithm has merits in terms of low memory requirement and since avalanche effect is very high in AES, it is ideal for message encryption in an unsecured channel.

Shuang Wang *et.al*, [4], put forth a method that involves non-asymmetric SW codes. This method involves following phases in relation to biometric processing viz., feature extraction, non-asymmetric SW encryption or non-asymmetric SW decryption and lastly an authentication technique as Privacy preserving authentication, whose objective is to fix security discrepancy in existing biometric approaches.

Taneja. S, *et.al*, [14] suggested a conventional secret key construction for symmetric encryption techniques using DH key agreement protocol, over Ad hoc networks. The authors devised a protocol consisting of subsequent stages, the key generation and key exchange, shared secret key creation, data encryption using symmetric key and encrypted data transmission. It is mandatory, primarily for public parameters to be set and then choose the secret numeral of source and destination. Lastly source sends the shared key to destination. As an ultimate step, source and destination create a common and arcane session key.

Cryptographic Methods

In cryptography, block cipher and stream cipher are two genres of cipher and symmetric key and symmetric key are two genres of keys used. Block cipher, a symmetric key cipher operating on aggregation of bits with fixed length and immutable transformation is termed as a *block*. Spectrum of the cryptographic methods is shown in figure.1.

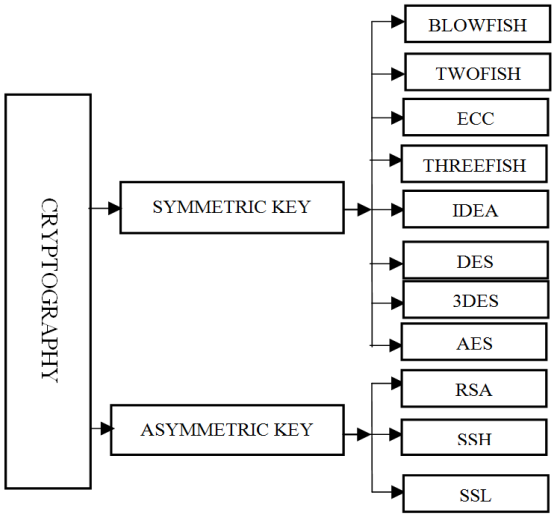

Fig 1 Classification of cryptographic methods

As an illustration, in the process of encryption, a block cipher accepting plaintext input of 128-bit generates a block of 128-bit cipher text. This transformation is predominated by a secret key which acts as its second input. Decryption process involves, cipher block of 128-bit in cooperation with the secret key to yield original plaintext of 128-bit block.

In contrast with block ciphers [22] a stream cipher acts on individual digits and during encryption process the transformation differs. Contradistinction between these two types is difficult. Effectiveness of encryption can be measured based on length of the key and type of the algorithm. Two variants of encryption/decryption keys are available. In few encryption techniques two systems that are communicating use identical algorithm and in most occasions same key. In few other encryption techniques, for this purpose different but related keys are made use of. Cryptographic algorithms are classified based on the genre of keys used. Symmetric algorithms use secret keys also called symmetric keys and asymmetric algorithms use public and private keys also called asymmetric keys [10].

Diverse cryptographic methods depicted in figure.1 are Elliptical Curve Cryptography, International Data Encryption Algorithm, Twofish, Threefish, Rivest Shamir Adleman algorithm, Data Encryption Standard, BLOWFISH, Triple DES and Advanced Encryption Standard. These methods are explained in this section in detail.

Elliptic Curve Cryptography (ECC)

Elliptic Curve Cryptography was devised as an auxiliary mechanism to implement public-key cryptography. These algorithms were widely in use during 2004 and 2005. ECC is mainly based on elliptic curve theory. ECC has the capability of creating smaller and faster, effective keys comparatively with its counterparts. In ECC elliptic curve equation is made use of for encryption. ECC yields an effective security level with 164 bit key, whereas its counterparts may require 1024 bit key to achieve an equivalent level of security. Hence ECC offers at most security with reduced bit sizes, while being power efficient [7].

A plane curve over a finite field can be addressed as an elliptic curve and basically it consists of point values that satisfy equation (1),

$$y^2 = x^3+Ax+B \quad (1)$$

where A and B are constant point values.
The simplest way of employing Elliptic curve cryptography in encryption process is discussed here.

According to ECC encryption technique,

- Sender first encodes a message ‘M’ as a point on an elliptic curve ‘Pm’.
- User first encodes a message ‘M’ as a point on the elliptic curve ‘Pm’.
- Specify a suitable curve and point ‘G’.
- Each user chooses a private key ‘n’, where A<n and computes public key PA

$$PA= nAG \quad (2)$$

- For encryption, encrypt point ‘Pm’ on the elliptic curve to obtain Cm,

$$Cm = \{kG, Pm + kPb\} \quad (3)$$

where k is a random number, Pb is public key
For decryption, decrypt Cm, compute Pm,

$$Pm = Pm + kPb - nB(kG) = Pm + k(nBG) - nB(kG) \quad (4)$$

Elliptic curves are applicable in several factorization algorithms having applications in cryptography. They also find usage in digital signatures, encryption and pseudo-random generators.

International Data Encryption Algorithm (IDEA)

International Data Encryption algorithm is one of the genres of block encryption algorithms which were illustrated initially in 1991. The native algorithm was subjected to series of modifications and eventually acquired the name International Data Encryption Algorithm [11]. IDEA operates with blocks of 64 bit cipher text and 64 bit plain text, which is further divided into four 16 bits sub-blocks for encryption purpose. It is governed by 128 bit key. Most of the decryption process is the reverse process of encryption and IDEA is no exception.

IDEA was made use of in Pretty Good Privacy [4] and is also an optional algorithm in Open PGP standard.

Twofish

Two fish is one of the illustrations for symmetric block cipher based algorithms, having a symmetric structure. It came into existence in 1998 and embellished later on. It works effectively with firmware or software on smaller processor. It permits developers to tailored encryption celerity, size of the code and time complexity involved in key setup, to balance performance requirements. Two fish encryption operates with 128, 192 or 256 bits key sizes. If 128 bits block size is employed, 16 rounds of encryption will eventuate in Two fish algorithm.

It is suitable and is used in stream cipher, hash function and Media Access Control

Three fish

Three fish a symmetric key block cipher was first proclaimed in 2008 and is a tweak able block cipher. It has a direct reference to Blowfish and Two fish. Input to a tweak able block cipher algorithm is a block of message, a key and a tweak. In Three fish every block of message is encrypt using unique 128 bits nibble value. The keys employed for encryption in Three fish are equal to the block size and may be varying in length as 256 bits, 512 bits or 1024 bits. Therefore, three block sizes may be used and generally 72 rounds of encryption will eventuate in Three fish algorithm. Neither the S-BOX nor table lookups are used in Three fish to avoid timing attacks [21].Three fish using 1024 bits block, encrypts data at the rate of 6.5 clock cycles per byte.

Rivest-Shamir-Adleman-RSA Algorithm

The RSA [15] a public-key encryption algorithm is one of the most standard and impregnable encryption algorithms. This algorithm exploited the fact that a no proper way existed to factor numbers of huge magnitude ranging from 50 to 200 digits.

Employing the encryption key (e,n), RSA algorithm can be accomplished. Initially the message 'M' is represented as an integer acquiring values between 0 to n-1. Huge messages are segmented into number of tiny blocks and represented by an integer in the specified range.

By raising segmented message block to e^{th} power modulo n, encrypt it, which results in generating a ciphertext 'C'. To decrypt 'C', raise it to power d modulo n Key (e,n) is devised to be public and key (d,n) to be private. For every required operation, Rivest, Shamir, and Adleman provide efficient algorithms [4].

RSA encryption algorithm works by encrypting the plain text as given below:

$$\text{Plaintext m is } m < n < p = \text{""} > \quad (5)$$

$$\text{where } n = p*q \quad (6)$$

p, q are large prime number

$$m = (\text{mod } ((p-1)*(q-1)))/d \quad (7)$$

$$\text{'d' is chosen such that } GCD(d,((p-1)*(q-1))) = 1 \quad (8)$$

Ciphertext, 'C' is generated.
RSA decryption algorithm works by decrypting 'C' as below:
Ciphertext, 'C' is set as input to decryption algorithm

$$\text{Plaintext 'M' is computed as, } M = C * d \bmod n \quad (9)$$

RSA Algorithm is used in desktop systems and mobile devices.

Data Encryption Standard (DES)

DES is a cryptographic scheme employing a symmetric structure called Feistel system, for construction of block ciphers. It operates using 16 cycle Feistel system, with a 56-bit key which is permuted a prior into 16-bit and 48-bit sub keys, one for each cycle, for all the 16 cycles.

In decryption, an identical algorithm is used but the order of sub keys is reversed. Blocks are divided as P and R, which are 32 bits data block each, yielding an overall block size of 64 bits. The hash function 'f', uses S-boxes and takes as input a data block and one of the sub keys to produce 32 bits output. Occasionally DES uses a 64-bit key, out of which 8 bits are for parity checking. Hence effective key size for DES is 56 bits [9].

In DES plaintext is broken into 64 bits block and encryption is block wise. A message block initially goes through permutation 'IP' and then it is divided into two parts P0 and Q0, where P0 is the left part of 32 bits and Q0 is the right part of the 32 bits.

Encryption procedure in DES includes following procedures:

Round 'i' has input Pi-1, Qi-1 and output Pi, Qi are obtained as

$$Pi = Qi\text{-}1 \quad (10)$$

$$Qi = Pi\text{-}1 \oplus f(Qi\text{-}1, Ki) \quad (11)$$

where 'Ki' is the sub key for the 'ith' round and $1 \leq i \leq 16$

$$P1 = Q0, \quad Q1 = P0 \oplus f(Q0, K1)$$
$$P2 = Q1, \quad Q2 = P1 \oplus f(Q1, K2)$$
$$P3 = Q2, \quad Q3 = P2 \oplus f(Q2, K3)$$
$$\ldots\ldots\ldots\ldots \quad \ldots\ldots\ldots\ldots$$
$$P16 = Q15, \quad Q16 = P15 \oplus f(Q15, K16) \quad (12)$$

For decryption algorithm to have structure similar to encryption algorithm after 16th round, P16 and Q16 are swapped. Finally, the received cipher block undergoes an inverse process, the permutation IP-1 and then output is generated. Decryption procedure in DES includes the following, for each 'i':

$$Qi\text{-}1 = Pi \quad (13)$$

$$Pi\text{-}1 = Qi \oplus f(Pi,Ki) \quad (14)$$

Output of encryption is IP-1 (Q16, P16) as the result of swap operation after 16th round encryption. The reverse encryption process can be summarized as follows:

$$Q15 = P16, \quad P15 = Q16 \oplus f(P15,K15)$$
$$Q14 = P15, \quad P14 = Q15 \oplus f(P14,K14)$$
$$Q13 = P14, \quad P13 = Q13 \oplus f(P13,K13)$$
$$\ldots\ldots\ldots\ldots \qquad \ldots\ldots\ldots\ldots$$

$$Q1 = P2, \quad P1 = Q2 \oplus f(P2,K2) \quad (15)$$

If IP-1(Q16, P16) is given as input to decryption algorithm with round sub keys ranging from K16 to K1, where K16 is used in first round, K15 in the second, so on and K1 is used in 16th round. The output generated is IP-1(P0, Q0), which is the original message block

It has been widely speculated that the cryptic S-boxes was not impregnably designed, allowing few, known to effectively crack DES. Regardless of flaws in hash function, rapid advances in electronic circuitry operating speed over few decades, amalgamated with natural symmetric structured Feistel ciphers and relatively small size of key used, has rendered DES algorithm obsolete [16]. Few of its successors are triple DES, DES-X and G-DES. DES is used to secure smart cards, ATM, in online economic trades, transactions at highway toll stations and petrol stations. Also used with standard transfer specifications to secure data transferred to and from pre payment meters.

Blowfish

Blowfish is a block cipher processing 64-bit blocks and was designed to replace DES. Significant merits of this algorithm are its length key, varying in the range 32 bits to 448 bits and the available variants of 14 rounds or less. BLOWFISH Encryption comprehends following strategy:

- Assume the plain text 'P' comprises E-PL_0 and E-PR_0 portions.
- The 'i^{th}' round output would be[6]:

$$E - PRi = E - PLi \text{ XOR } Pi \quad (16)$$

$$E - PLi = F\,[E - PRi] \text{ XOR } E - PRi - 1 \quad (17)$$

- Computed cipher text would be[6]:
-

$$E - PR17 = E - PL16 \text{ XOR } P18 \quad (18)$$

$$E - PR17 = E - PL16 \text{ XOR } P17 \quad (19)$$

$$C = E - PR17 + E - PL17 \quad (20)$$

Cipher text obtained by encryption process acts as input for decryption algorithm which is similar to encryption algorithm, with a simple variation of reverse order key fashion being used. Decryption process includes following procedures:

- Assume the cipher text 'C' comprising D-CL_0 and D-CR_0 portions.
- The 'i^{th}' round output would be[6]:

$$D - CRi = D - CLi \text{ XOR } P19 - I \quad (21)$$

$$D\text{-}CLi = F\,[D{-}CRi] \text{ XOR } D\text{-}CRi{-}1 \quad (22)$$

For each round, output of equations (16) and (21) and equations (17) and (22) are same, due to reversibility of encryption and decryption strategy.

The benefit of Blowfish is its availability to users as license-free software and is unpatented. Blowfish is one of the speedy block ciphers invented but agonizes having awful keys. Yet there are no reports of any confront being successful till date. Blowfish finds its application in military for secure voice transmission

Triple DES

Triple DES designed to address inadequacy in DES is just advancement to existing DES without modeling entirely a new cryptosystem. Triple DES applies DES algorithm thrice in succession using three identical keys by simply extending the key size of DES. The amalgamated key size of Triple DES is 3 times of 56 which is equivalent to 168 bits. 168 bits key size cannot be easily surpassed by brute-force practices. No serious flaws in design of Triple DES have been discovered.

3DES involves time and processing complexities, as a consequence it shows poor performance results [9]. It finds its applications in a number of Internet protocols [8] [9].

Advanced Encryption Standard (AES)

Advanced Encryption Standard was designed by Rijndael [8]-[13], to overcome the flaws in the previously designed encryption algorithms.AES security is a relation between cost and time. Today's actual systems can handle key lengths of about 70 bits. 128-bit length for AES key was considered after analysis of safety requirements and to brute force a confidential key, which is depicted in figure below.

Fig 2 AES-128 states

a_{00}	a_{01}	a_{02}	a_{03}
a_{10}	a_{11}	a_{12}	a_{13}
a_{20}	a_{21}	a_{22}	a_{23}
a_{30}	a_{31}	a_{32}	a_{33}

$$a = (a_{00}, \ldots . a_{30}, a_{01}, \ldots . , a_{31}, a_{02} \ldots . , a_{33}) \quad (23)$$

Equation (23) represents different states of AES algorithm. In AES, each byte is regarded as an element of the field [4].

$$K = \frac{F2[x]}{< f(x) >} \cong F2^8 \quad (24)$$

where f(x) and F2[x] is the irreducible polynomial x8 + x4 + x3 + x + 1 and F2[x] is element of f(x)y [4].

Specification of a round in AES is defined in terms of three transformations explained below.

The AES S-Box

The operation in AES for generating cipher is by using non-linear S-Box. A table look-up which is a combination of three

transformations is used to substitute the value of each byte in the array [4].

The processes involved in first and last rounds have related but identical manifestation in computational and algebraic aspects of Advanced Encryption Standard [20] [23]

Input data 'w' is mapped onto x as $x = w^{(-1)}$ (25)

where $w^{(-1)}$ is represented by[4]

$$w^{(-1)} = w^{254} \begin{cases} w^{-1} & w \neq 0 \\ 0 & w = 0 \end{cases} \quad (26)$$

'x', an intermediate value generated is regarded as vector-F2, having dimension 8 and transformed later into a vector 'A · x' where LA is 8×8 F2-matrix. The vector 'LA · x', is regarded as an element of 'K'. (LA · x) + d is the output produced by AES S-Box, where d is a constant element of K.

The AES linear diffusion (mixing) layer

Individual rows of an AES array are rotated by a certain number of byte positions and this operation is regarded as ShiftRow. Likewise, individual column 'o' regarded as a vector in K4, is remodeled as column C · o, where C is 4×4 K-matrix and this operation is termed as MixColumn.

Addition AES subkey

Before encryption original key in AES is expanded into eleven round subkeys each having 16 bytes and during encryption, every byte of the round subkeys is added with corresponding bytes in array.

Other than exhaustive search or possible brute force method, currently there are no flaws in AES that can make it vulnerable to any security attacks. AES is mainly used in banking, in online transactions and military applications

CONCLUSION

This paper is merely a study of encryption techniques. Restyling of encryption genre based on current studies, is vital in successive year's security systems. Usage of encryption techniques in networks for secure data mobility is no more a military application but a necessity component in every mobile communication.

Encryption techniques should be modeled in such a way that they are scalable, can easily be employed in any mobile device and be adoptable in any type of network. A secure and robust encryption process will never yield to attacks.

References

1. Nadeem. A and Howarth. M. P, "A Survey of MANET Intrusion Detection & Prevention Approaches for Network Layer Attacks", published in IEEE Communications Surveys & Tutorials, 15(4), 20272045, 2013.
2. Chen.J, and Wu. J, "A Survey on Cryptography Applied to Secure Mobile Ad hoc Networks and Wireless Sensor networks", published in Handbook of Research on Developments and Trends in Wireless Sensor Networks: From Principle to Practice, IGI Global, AH ALTALHI, 5, 2414-2424,2010.
3. Du. D, and Xiong. H, "A Dynamic Key Management Scheme for MANETs", presented at Cross Strait Quad-Regional Radio Science and Wireless Technology Conference (CSQRWC), IEEE, 1, 779-783, 2011.
4. Mokhtarnameh.R, Muthuvelu. N, Ho. S. B and Chai. I, "A Comparison Study on Key Exchange-Authentication Protocol", published in *International Journal of Computer Applications*,7(5), 5-11, 2010.
5. Abdul. D. S, Elminaam. H. M. A. K and Hadhoud. M. M, " Performance Evaluation of Symmetric Encryption Algorithms", published in *International Journal of Computer Science and Network Security*, 8(12), 78-85, 2009.
6. Alanazi. H, Zaidan. B, Zaidan. A, Jalab. H. A, Shabbir. M and Al-Nabhani. Y, " New comparative study between DES, 3DES and AES", within nine factors arXiv, preprint arXiv:1003.4085, 2010.
7. Stallings. W, "Cryptography and Network Security: Principles and Practice", 5th edition, India: Pearson Education, 2006
8. Mandal. A. K, Parakash. C and Tiwari. A, "Performance Evaluation of Cryptographic Algorithms: DES and AES", presented at Electrical, Electronics and Computer Science (SCEECS), IEEE Students Conference, IEEE, 1-5. 2012.
9. Umaparvathi. M and Varughese. D. K, "Evaluation of Symmetric Encryption Algorithms for MANETs", presented in Computational Intelligence and Computing Research (ICCIC), IEEE International Conference, 1-3, 2010.
10. Sahu. S. K and Kushwaha. A, "Performance Analysis of Symmetric Encryption Algorithms for Mobile Ad hoc Network", published in *International Journal of Emerging Technology and Advanced Engineering* IJETAE, 4(6), 2014.
11. Norouzi. M, Esmaeel Akbari.M and Souri. A, " Optimization of Security Performance in MANET", published in Journal of American Science, 8(6), 2012.
12. Kashani. A. A and Mahriyar. H, "A New Method for Securely Streaming Real-time Video in Ad hoc Networks", published in Advances in Environmental Biology, 8(10), 1331-1338 , 2014.
13. Sandhiya. D, Sangeetha. K and Latha. R. S, "Adaptive ACKnowledgement Technique with Key Exchange Mechanism for MANET", presented at Electronics and Communication Systems (ICECS), 2014 International Conference, IEEE, 1-5, 2014.
14. Taneja. S, Kush. A and Hwang C. J, "Secret Key Establishment for Symmetric Encryption over Adhoc Networks". Published in Proceedings of the World Congress on Engineering and Computer Science (Vol. 2), 2011.
15. Ramesh Yegireddi and R Kiran Kumar, " A Survey on conventional encryption algorithms of cryptography", published in proceedings of International Conference on ICT in Business Industry & Government (ICTBIG), 2016.
16. Elminaam. D. S, Kader. H. M. A and Hadhoud. M. M, "Energy Efficiency of Encryption Schemes for Wireless Devices", published in *International Journal of Computer Theory and Engineering*, 1, 302309, 2009.
17. Biham. E, "Fast Software Encryption",4th International

Workshop, FSE'97, Haifa, Israel, January 20-22, 1997, Springer, Proceedings (Vol. 1267).
18. Nazariy. K, Shaydyuk and Timothy Cleland, "Biometric Identification Via Retina Scanning With Liveness", Security Technology (ICCST), IEEE International Carnahan Conference, 2016.
19. S. Sridevi Sathya Priya, P. Karthigaikumar, "Mixed Random 128 Bit Key Using Finger Print Features and Binding Key for AES Algorithm", presented at Contemporary Computing and Informatics (IC3I), International Conference, 2014.
20. Carlos Cid, Sean Murphy and Matthew Robshaw, "Computational and Algebraic Aspects of the Advanced Encryption Standard", published in springer, 2006.
21. Susan Landau, "Polynomials in the Nation's Service: Using Algebra to Design the Advanced Encryption Standard", American Mathematical Monthly, pages 89-117, February 2004.
22. Nicolas Courtois and Josef Pieprzyk, "Cryptanalysis of Block Ciphers with Overdefined Systems of Equations", In Yuliang Zheng, editor, Advances in Cryptology - ASIACRYPT 2002, volume 2501 of Lecture Notes in Computer Science, pages 267-287. Springer, 2002.
23. Sean Murphy and Matthew Robshaw, "Essential Algebraic Structure within the AES", In M. Yung, editor, Advances in Cryptology - CRYPTO 2002, volume 2442 of LNCS, pages 1-16. Springer-Verlag, 2002

How to cite this article:

Srividya R and Ramesh B. 2018, Analysis of Impregnable Ciphers in Manet. *Int J Recent Sci Res.* 9(10), pp. 29399-29404.
DOI: http://dx.doi.org/10.24327/ijrsr.2018.0910.2855

****