Scientific Journal of Impact Factor (SJIF): 4.14

e-ISSN (O): 2348-4470
p-ISSN (P): 2348-6406

International Journal of Advance Engineering and Research Development

Volume 3, Issue 12, December -2016

# Analysis of Block Cipher Encryption algorithms for mobile ad-hoc network

Shrishti Sao[1], Dr.Vishnu Mishra[2], Mr. Ghanshyam Sahu[3]

[1,2,3]*Department of CSE, Bharati College of Engineering and Technology, Durg*

**Abstract** — *Currently applications on internet is growing speedily, one and all share their thoughts, feelings, personal data and many more online that's why security is one of most considerable and important issue in wireless network. Providing security in wireless network is much essential and important. Encryption algorithm play dynamic role in wireless network. A block cipher symmetric key encryption/decryption algorithm is todays widely used cryptography system to secure data so that no any intruder is able to read or modify the message or data. In Block cipher encryption there is only one key that is shared between both side that is sender and receiver of data to encrypt/decrypt the data or message. This Work provides brief analysis of 3 most important block cipher algorithms: AES, DES and BLOWFISH. We will perform these algorithms on normal and hd data with some metrics to analyses which one is best compared to other.*

***Keywords****-MANET, Block Cipher, DES, Syymetric Key:*

## I. INTRODUCTION

In world of internet, Cryptography play a main character. They can be divided into two portion i.e. Asymmetric and Symmetric key algorithms. In Symmetric Key Cryptography algorithm, here is single key that is common between sender and receiver to encrypt/decrypt data. Symmetric key algorithm is of two kinds: block ciphers and stream ciphers. Now Block ciphers are by means of on collection of blocks, for example AES (Advanced Encryption Standard), DES (Data Encryption Standard) and Blowfish. Stream ciphers are using on single bit at a time, for example RC4.In Asymmetric key algorithm here is two dissimilar key for encryption and decryption, one is public key that is used for encryption while another is secret key which is used for decryption, for example RSA algorithm. Public key is known to public and private key is only known to user. Due to large computational processing power, asymmetric key algorithm is 1000 times slower than symmetric key algorithm.

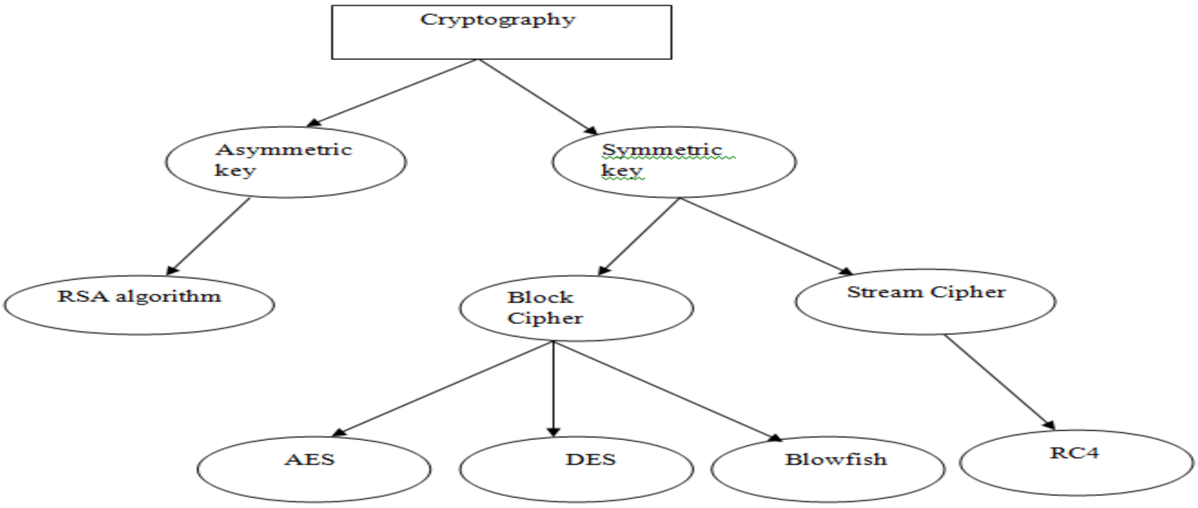


Fig1.1 Hierarchy of Cryptography

### 1.1 Symmetric key Algorithm

### 1.1.1 DES:-

Data Encryption Standard (DES)was the first encryption standard to be developed by National Institute of Standards and Technology(NIST). Data Encryption Standard is a block cipher symmetric key algorithm standard that uses the same key to encrypt/decrypt the data.Basically DES uses one 64 bits key with 64 bits block, out of 64 bits key,56 bits are used to determine the the exact cryptography transformation and remaining 8 bits are used for error detection. In DES there is total 16 round to perform their operations, the main action in each round is variation and replacement. The result of DES encryption is 64 bit cipher text. Decryption in DES is similar as encryption, first the keys are applied in opposite order.

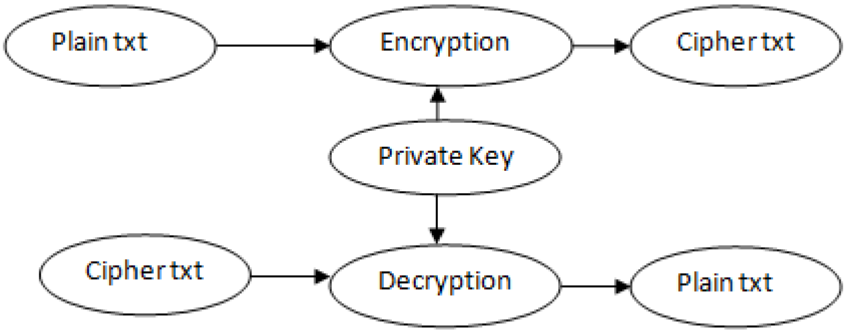


*Fig1.2 Symmetric Key Encryption/Decryption*

**1.1.2 AES:-**

AES(Advanced Encryption Standard)**:**The FEDERAL INFORMATION PROCESSING STANDARDS PUBLICATION(FIPS) specifies the AES(Advanced Encryption Standard) also known as Rijndael (Rain-doll) after introducing the DES. It is also Block cipher encryption standard that uses 10, 12, or 14 rounds with 128,192 or 256 bits sizes key depending on the number of rounds. Each processing round involves four steps-

1. Substitute bytes
2. Shift rows
3. Mix columns
4. Add round key

**1.1.3 Blowfish:-**

Blowfish is another member of symmetric block cipher encryption standard that is developed by Bruce Schneier in 1993 and it can be efficiently used for encryption and decryption of data significantly. Basically it has adjustable length key from 32 to 448 bits. It is open source, and is available for all uses. It is fast i.e. encryption rate on 32 bit microprocessor is 28 clock cycles/sec.Basically Blowfish is suitable for applications where the key remains constant for a long interval of time. Table I shows the comparison of Block cipher algorithm

TABLE I
COMPARISON OF BLOCK CIPHER KEY ALGORITHM

| **Algorithm** | **Key Size** | **Block Size** | **Rounds** |
|---|---|---|---|
| **DES** | 56 bits | 64 bits | 16 |
| **3DES** | 112 bits or 168 bits | 64 bits | 48 |
| **AES** | 128 bits, 192 bits, 256 bits | 128 Bits | 10, 12 or 14 |
| **Blowfish** | 32-448 bit . | 64 bits | 16 |

## II. LITERATURE REVIEW

**[Patil, A., et. al. 2013]** presented AES algorithm that describes the effective security for data storage in mobile devices by implementing for encryption and decryption and finds that embedded systems similar to Mobile phones, GPS receivers, Wireless Sensor Nodes etc hold sensitive data, hence requires data security mechanisms. AES algorithm which is a standard algorithm for data encryption is appropriate for such scenarios where memory and processing power constraints are very high.

**[Bambodkar, R., et. al. 2013]** presented a methodology for Fast Encryption Algorithm for Streaming Video over Wireless Networks. In this paper, it designed a new lightweight, efficient, scalable, format-compliant video encryption algorithm, which is based on the DCT (Discrete Cosine Transformations) coefficients scrambling. The simulation shows that the proposed video encryption algorithm consumes low computation resource while achieves high scalability and confidentiality, which is in compliance with the design goal of video streaming over wireless applications. The proposed algorithm is a Compression-Logic based video encryption algorithm. Instead of randomly permuting 8×8 coefficients of a single DCT block, the random permutation is applied to a number of permutation groups. Each permutation group contains the DCT coefficients of the same frequency (index of 8×8 DCT matrix) from every single block of a frame, regardless of I, P or B frame. This paper, proposed a computationally efficient, yet secure video encryption scheme. It uses RC5 for encryption of the DCT coefficients and ECC for small key sized generation .The proposed scheme is very fast, possesses good security and adds less overhead on the codec. It slightly decreases the compression rate of the video, which is negotiable for higher security. In fu-ture it would be to reduce the encrypted video size by modifying the default Huffman tables and hence come up with an ideal video encryption algorithm which takes less encryption time and causes no overhead on video size. It can also be extended to videos like MPEG-4, H.261, and H.264 etc.

**[Umaparvathi, M., et. al. 2012**] presented a methodology to compare the performance of various symmetric key algorithms based on some performance analysis like encryption/decryption time and throughput. The different algorithms have been implemented in Java and the experiment has been passed out using a laptop, with 2.00 GHz Intel Pentium core -2 Duo processor. Future work for this paper is the percentage of battery power consumed by the various encryption algorithms based on the CPU clock cycles.

[**Goyal, S., 2012]** presented a summary of cryptography, where it is applied and its usage in various forms. It has emerged as a secure means for transmission of information. It mainly helps in curbing intrusion from third party. It provides data confidentiality, integrity, electronic signatures, and advanced user authentication. The methods of cryptography use mathematics for securing the data. In this paper the areas of applicability of cryptography and its variants have been explained. The amount of distinction among all the variants of cryptography is less because the entity in all the algorithms is information that needs to be secured. In this research paper the applicability of cryptography in data security has been studied and summarized. Also the various cryptographic techniques have been observed and their specific areas of applicability have been found out and a summarized table has been developed.

**[Pavithra, S., et. al. 2012]** presented a study and performance analysis of cryptography algorithms. In this study is made for the cryptography algorithms, particularly algorithms are compared and performance is evaluated. In this paper various cryptographic algorithms and majorly deals the encryption and decryption process for protecting the text files and images using some of the cryptographic algorithms are studied. The presented simulation results of audio files show the points. It was concluded that Blowfish has better performance than AES in terms of Average time.

**[Mandal, P., et. al. 2012]** proposed a simulation on java and finds that the performance evaluation of selected symmetric algorithms (AES, DES, 3DES, BLOWFISH).
The simulation have been carried out by using Pentium IV of 2.4 GHz CPU speed with 4 GB RAM. In this experiment the text files sizes variety from 50 KB to 22300 KB. From the presented simulation it has been concluded that Blowfish has better performance than other algorithms.

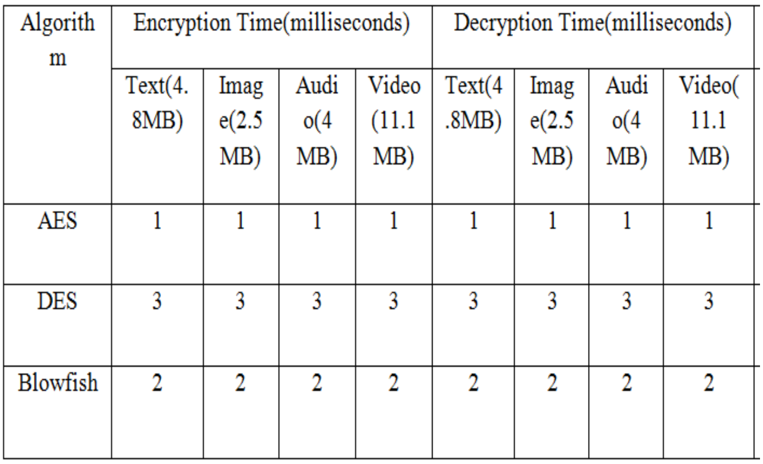
**[Soni, S., et. al. 2012]** presented a work on analysis and comparison of AES and DES algorithms. They compare AES and DES based on nine parameter. An image size of 128*128 (e.g. cameraman, pepper, aero, etc.,) is measured as plain (Original) image and DES and AES encryption and decryption is performed using MATLAB and finds that AES algorithm consumes least encryption and decryption time as compared to DES algorithm [Hirani, S., 2008].

**[Shanta, et. al. 2012]** provides the dedicated work to evaluate performance of Symmetric Key Algorithms: AES (Advanced Encryption Standard) and DES (Data Encryption Standard).
This paper provides evaluation of the most common encryption algorithms namely: AES (Rijndael) (Advanced Encryption Standard) and DES (Data Encryption Algorithm). A comparison has been conducted for those encryption algorithms at different setting speed, time and cost. This results showed that AES is more suitable than DES.
For their experiment, they use a laptop 2GB Memory, in which performance data is collected. In the experiments, the laptop encrypts different algorithms of AES and DES. It uses the Microsoft Visual Studio and VC++ that support wodcrypto- tool in which performance data is collected. In the experiments, AES and DES algorithms are encrypted in .NET and wodcrypto- tool. The wodcrypto-tool use the 4.30MB size, 2.1.4 version, 128MB RAM Windows 7/Vista/XP/2000 system. This paper presents a performance evaluation of AES and DES symmetric encryption algorithms. The performance metrics of the encryption throughput, speed, time and cost. The AES encryption/decryption algorithm in c# in Microsoft visual studio is give the better results. Like the AES algorithm, DES algorithm in c# in Microsoft visual studio is giving the better results.

## III. RESULT AND DISSCUSSION

After studying various research article, We perform analysis and found results based on encryption/decryption and throughput of block cipher algorithm and gives their priority in the form of 1,2 and 3. This result will help researchers to select algorithm according to nature of data for cryptography, which is shown in Table 1I

TABLE II
OVERALL ANALYSIS



| Algorith m | Encryption Time(milliseconds) | | | | Decryption Time(milliseconds) | | | |
|---|---|---|---|---|---|---|---|---|
| | Text(4.8MB) | Image(2.5 MB) | Audio(4 MB) | Video (11.1 MB) | Text(4.8MB) | Image(2.5 MB) | Audio(4 MB) | Video(11.1 MB) |
| AES | 1 | 1 | 1 | 1 | 1 | 1 | 1 | 1 |
| DES | 3 | 3 | 3 | 3 | 3 | 3 | 3 | 3 |
| Blowfish | 2 | 2 | 2 | 2 | 2 | 2 | 2 | 2 |

## IV. CONCLUSION

We all need security in this digital world, cryptography is prime requirement for us. In this article, we try to simulate various research journal and presents my results in Table II. We hope that this result will help researchers and academician to select algorithm based on their need to secure the system.

## REFERENCES

[1] Singh, S. and Shan, H. S. (2002) “Development of Magneto Abrasive Flow Machining Process”, International Journal of Machine Tools & Manufacturing, vol. 42, 2, 2002, pp. 953-959.

[2] Ruangchaijatupon, and Krishnamurthy P.(2001), "Encryption and Power Consumption in Wireless LANs-N,’’ The Third IEEE Workshop on Wireless LANs - September 27-28, 2001- Newton, Massachusetts.

[3] Hardjono(2005) "Security In Wireless LANS And MANS," Artech House Publishers 2005.

[4] Stallings W.(2005), "Cryptography and Network Security 4th Ed," Prentice Hall , 2005,PP. 58-309.

[5] Coppersmith, D.(2010) "The Data Encryption Standard (DES) and Its Strength Against Attacks. "IBM Journal of Research and Development, May 1994,pp. 243 - 250.

[6] Schneier B.(2008) The Blowfish Encryption Algorithm Retrieved October 25, 2008, http://www.schneier.com/ blowfish.html

[7] Daemen, J., and Rijmen, V. (2009)"Rijndael: The Advanced Encryption Standard."D r. Dobb's Journal, March 2001,PP. 137-139.

[8] N. El-Fishawy , "Quality of Encryption Measurement of Bitmap Images with RC6, MRC6, and Rijndael Block Cipher Algorithms", International Journal of Network Security, , Nov. 2007, PP.241–251.

[9] Diaa Salama Abdul. Elminaam, Hatem Mohamed Abdul Kader and Mohie Mohamed Hadhoud, “Performance Evaluation of Symmetric Encryption Algorithms”, International Journal of Computer Science and Network Security, VOL.8 No.12, December 2008.

[10] S.Hirani, "Energy Consumption of Encryption Schemes in Wireless Devices Thesis," university of Pittsburgh, April 9,2003. Retrieved October 1, 2008, at: portal.acm.org/ citation.cfm?id=383768

[11] "A Performance Comparison of Data Encryption Algorithms," IEEE [Information and Communication Technologies, 2005. ICICT 2005. First International Conference ,2006-02-27, PP. 84- 89.