A Comparative Analysis of RSA and BAES for MANET Routing Protocols

Srividya R[1], Ramesh B[2]
[1]*K. S. Institute of Technology, Bengaluru*
[2]*Malnad College of Engineering, Hassan*
(E-mail: srividya.ramisetty@gmail.com, sanchara@gmail.com)

***Abstract*—** The drastic up rise in exchange of data, digitally in Mobile Adhoc network, leads to a major concern of secure data mobility in the network. This paper introduces security extinction to AES cipher, Biometric Advanced Encryption Standard (BAES). BAES is an amalgamation of biometric as key to AES with. The paper includes comparative analysis of RSA and BAES ciphers. Also the paper throws light on the polarities between the two ciphers using Avalanche effect, time complexity and memory utilized efficiency determining parameters

Keywords— *AES, MANET, RSA, BAES, Fingerprint, Biometric.*

I. INTRODUCTION

Mobile Adhoc Network (MANET) is a genre of networks which has non static and self configuring nature. Secure data mobility in such non static, decentralized network is a challenging task. Any intruder can effortlessly launch malicious attacks in such networks with no firewall. To secure data from active and passive attacks is a confronting assignment. Therefore optimum schema is to exploit the concept of cryptography and its ciphers, in encrypting the data before transmission. This is the leading motivation in designing new ciphers, with reduced complexities. Study of literature provides a bird view into adequate number of ciphers and their applications. Ciphers can be classified as symmetric and asymmetric ciphers.

Asymmetric ciphers are known to use two keys for encryption, public key and private key. Private key is private to the user, whereas public key is the shared key in the network. RSA is the cipher which can represent asymmetric ciphers genre and is most widely used asymmetric cipher. The major limitation in using asymmetric key ciphers in MANET is their high power utilization factor, with medium security provided.

Symmetric ciphers have only one shared secret key. Secret key is provided to the users when he registers with the network. Also it can be exchanged between nodes, after the authentication process and before start of any session. AES is the most popular and widely used symmetric ciphers. Comparatively symmetric ciphers prove as best since the usage of power by these ciphers is optimum in networks such as MANET s where the resources are limited.

Every genre of ciphers has their own leads and limitations [1]. Here we design a cryptographic method Biometric Advanced Encryption Standard (BAES), which is a minor addition to the sphere of ciphers. Cipher efficiency parameters such as memory utilized, time taken and Avalanche effect are considered, to analyze BAES and compare it with RSA.

II. LITERATURE SURVEY

Septimiu Fabian Mare, et al. introduced a robust steganography-based communication system using RSA and AES ciphers, together with steganography. The key used for data encryption uses a combination of randomly generated sequence and a hash of cover image's color information. The proposed steganographic algorithm introduces steganography as an additional security level and avoids advanced reverse engineering techniques [3].

Jong Yeon Park et al. described unknown and interesting characteristics of ghost key patterns using real experiments [4]. They explained about the ghost key by selected bits. Also they stated that knowledge of ghost key patterns can be a useful tool to analyze enhanced scenarios and its countermeasures.

Michael Bourg et al. proposed an RSA based biometric encryption system which can be realized on Field Programmable Gate Arrays [5]. They showed that biometric is one of the safest form of privacy and security.

Asma Chaouch et al. programmed a flexible encrypting algorithm for encrypting text and compressed images. It was based on RSA, AES and elliptic-curves methods [6]. Also they provided a fair comparison between the three methods under study, considering the parameters like key size, block size and speed.

Amish Kumar et al. presented an efficient implementation of AES on MATLAB platform. They provided an explanation to Avalanche effect in AES [2].

III. RIVEST SHAMIR ADLEMAN

RSA is one of the first successful responses developed by Ron Rivest, Adi Shamir, and Len Adleman at MIT. It was developed to overcome the challenges faced in public key cryptography. RSA is best illustrated in fig.1.

RSA cipher uses two primes with Euler's totient function to obtain the value of variable 'n'. Plain text is transformed to cipher text by raising plain text to power of encryption key 'e'. Encryption key is public key of the destination node to which cipher text needs to be transmitted. The destination node uses

its private decryption key 'd', to obtain the plain text from cipher text.

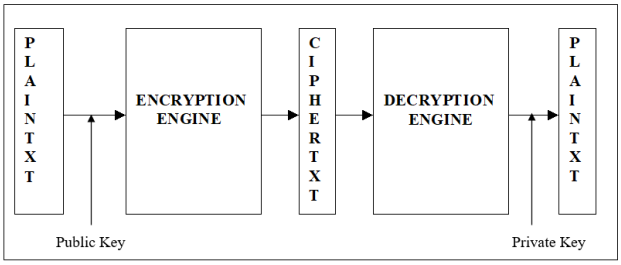

Fig. 1. RSA Cipher block diagram

There can be many approaches to attacking RSA. Attacks can happen due to side channel leakage during transmission [4]. Since the key is generated using the generator function and also there exits Ghost key patterns with actual keys in the cipher data. These ghost key patterns are vital assets in determining the performance of power analysis.

Few of the other types of attacks listed in literature are Brute force attack, Mathematical attacks, Timing attacks, Hardware fault-based attack, Chosen ciphertext attacks, cipher-text only attack, known plaintext, chosen plaintext, Adaptive chosen plain text, chosen key and power analysis [1].

IV. BIOMETRIC ADVANCED ENCRYPTION STANDARD

AES is the most successfully used symmetric cipher till date in diverse fields for secure data mobility. Based on the input block size AES has three variants, AES-128, AES-192 and AES-256[7]. In AES-128, 10 rounds of transformation with 16-bytes key are applied to each input message to obtain the cipher text. Similarly in AES-192, 12 rounds of transformation with 24-bytes key are used. And in AES-256, 14 rounds of transformation with 32-bytes key are used.

It is very unlikely to hack or attack AES. Complexity of AES lies in trade off between size of the encryption key used and the level of security offered. As the key size increases, AES memory utilization and power consumption also increases but with increased security and avalanche effect.

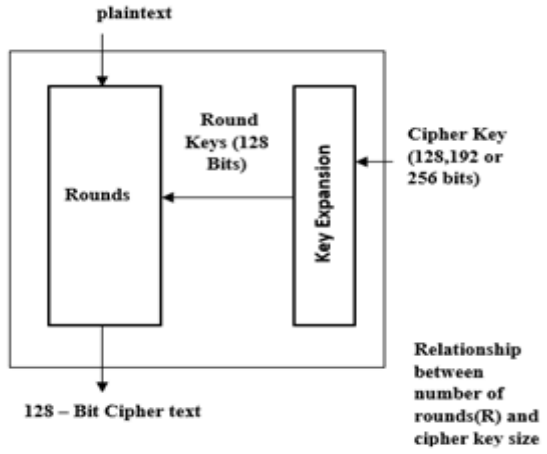

Fig. 2. Proposed BAES Architecture

However recent studies show that attacks can be launched by intruders using the data transmission power level. Since in AES, encryption key is generated using pre designed generator function, the cryptanalyst can determine its way of working and launch an attack. To overcome this limitation the key generator function needs to be improved or replaced.

This paper evaluates a new variant of symmetric key AES, BAES, which is intended to overcome such power based attacks. BAES is also compared with existing asymmetric key RSA cipher. Also BAES is best suited for use with routing protocols of decentralized networks like MANET.

BAES is a form of AES cipher. But the divergence is in the Cipher key used. BAES uses a single biometric key rather than two keys as in RSA and Add round key as in AES. In BAES, for 128-bit data input, 128-bit biometric key is used.

Biometric key is acquired by preprocessing the input biometric image obtained from the biometric device. Biometric processing includes various operations such as capturing analog input, preprocessing input image, feature extraction from the image input and finally key generation. The size of key can be 128-bits, 192-bits or 256-bits and is based on the size of data to be encrypted. BAES architecture is depicted in fig. 2.

Biometric has diverse genre [8]. A suitable biometric can be used as key for BAES without compromising preciseness of feature extraction. It is expected to be almost impossible for cryptanalyst to attack and analyze BAES keys.

In the worst case of implementation, if the intruder succeeds key can be immediately replaced.

V. IMPLEMENTATION

BAES can be implemented and used in various applications. BAES works with biometric as key as stated earlier and can encrypt data with block sizes of 256-bits or 192-bits or 128-bits. 128-bit biometric key with 128-bit BAES is taken into consideration for study.

Procedure to transform plain text to cipher text using BAES cipher is explained as follows:

- Firstly, biometric input is processed and stored as BAES secret key. The processed key is expanded into number of words matrix based on the BAES genre used.
- Input plain text in form of matrix is given to an Add Round Key function and the plain text is XORed with the expanded biometric sub key.
- The resultant matrix of XOR operation is substituted using Substitute bytes from a standard 256 values in Substitute-box or S-box matrix.
- Then Shift rows with specified number of shifts for each row, keeping the first row constant. Mix columns using mathematical concepts on the matrix obtained by shifting rows.

This procedure is repeated for specified number of times based on input data size and BAES type. Finally repeat the process of Substitute bytes, Shift rows and Add Round key for

the final round to obtain a block cipher text. Decryption algorithm involves the reverse and inverse process of encryption.

VI. EXPERIMENTAL RESULTS

BAES is simulated using MATLAB software. BAES and RSA are compared here considering various efficiency parameters. The parameters taken into consideration for study of BAES and comparison with RSA are memory utilized, processing time complexity and avalanche effect. The simulation values obtained by considering various forms of input are tabulated and graphically represented in this section.

A. Encryption and decryption of text input

The process of RSA encryption and decryption is shown using the waveform in fig. 3. The values of P and Q are assumed to be 17 and 19 respectively. P and Q are chosen such that Euler's totient function satisfies the following condition as in equation (1)

$$\emptyset(n) = 1 \qquad (1)$$

$$where\ n = P * Q$$

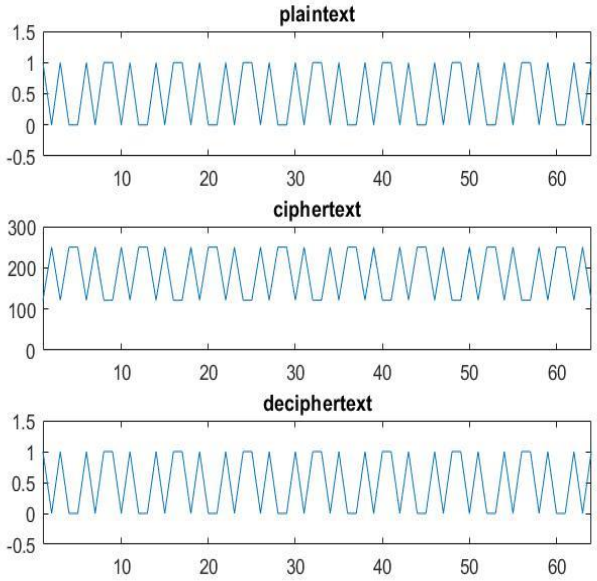

Fig. 3. RSA encryption and decryption process for text input (ASSUMED P AND Q as 17 and 19)

The BAES encryption and decryption process for text input is shown in fig. 4. It also includes waveform of the key being used.

TABLE I. COMPARISON OF RSA AND BAES FOR TEXT INPUT

Parameters	RSA	BAES
Memory utilized	30KB	16KB
Time in msec	81	97

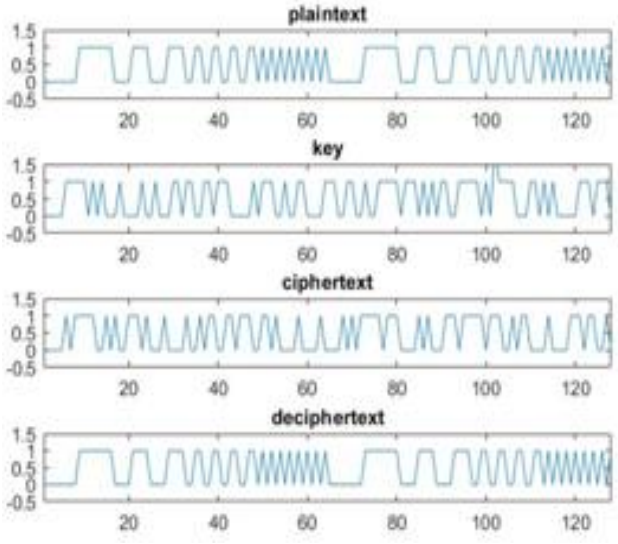

Fig. 4. BAES encryption and decryption process for text input

Table I compares execution time for RSA cipher and BAES cipher using plaintext input. Tabulated values are represented in the form of graph in Fig. 5.

Fig.5 represents time taken by RSA and BAES encryption and decryption process in transforming plaintext to ciphertext and vice versa. X-axis represents data blocks in terms of bits and Y-axis represents time taken to convert the input data to cipher in terms of milli seconds

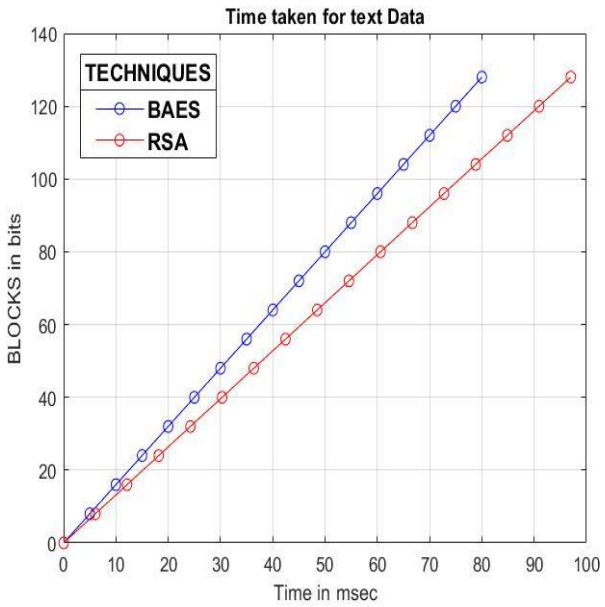

Fig. 5. Comparison of Time taken to execute RSA and BAES for text input

B. Encryption and decryption of image input

Table II compares execution time for RSA cipher and BAES cipher using image input. Tabulated values are represented in the form of graph in Fig.6

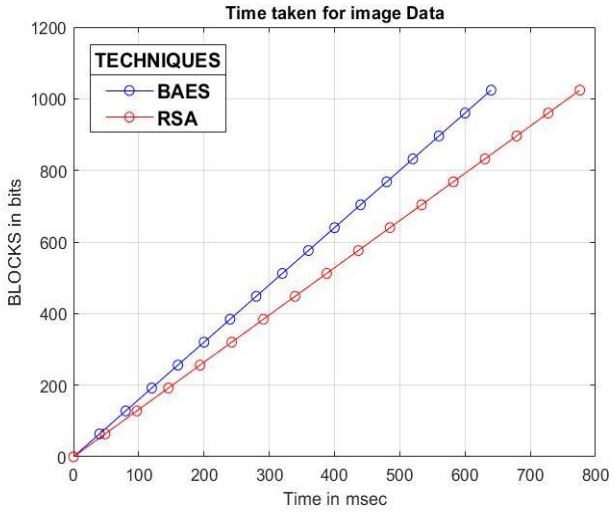

Fig. 6. Time taken to execute RSA and BAES for image input

Fig.6 represents time taken by RSA and BAES encryption and decryption process in transforming image input to ciphertext and vice versa.

TABLE II. COMPARISON OF RSA AND BAES FOR IMAGE INPUT

Parameters	RSA	BAES
Memory utilized	150KB (128 bits data)	128KB (64 bits data)
Time in milli sec	710	776

As stated already X-axis represents data blocks in terms of bits and Y-axis represents time taken to convert the input data to cipher in terms of milli seconds

C. Avalanche Effect

The magnitude of change in the cipher bits due to change in one bit input data or one bit key is known as Avalanche effect. Efficiency of any cipher can be measured using this [2].

TABLE III. AVALANCHE EFFECT IN BAES

Sl No	Input to BAES	Key	Cipher	% of Change
1	0 5 0 5 10 15 10 15 0 5 0 5 10 15 10 12 0 0 5 5 0 0 5 5 10 10 15 15 10 10 15 12	35 41 59 5d 4f 52 67 69 58 5f 7c 83 74 4d e f	2 15 2 10 4 15 11 8 4 14 8 15 5 3 13 15 4 7 10 6 11 5 9 8 10 15 2 15 15 12 1 3	100
2	1 5 0 5 10 15 10 15 0 5 0 5 10 15 10 12 0 0 5 5 0 0 5 5 10 10 15 15 10 10 15 12	35 41 59 5d 4f 52 67 69 58 5f 7c 83 74 4d e f	7 12 15 12 5 14 4 8 0 3 13 13 15 4 12 12 2 8 6 8 3 7 10 9 3 2 15 3 11 11 12 8	96.8
3	0 5 0 5 10 15 10 15 0 5 0 5 10 15 10 12 0 0 5 5 0 0 5 5 10 10 15 15 10 10 15 15	35 41 59 5d 4f 52 67 69 58 5f 7c 83 74 4d e f	3 7 15 0 11 3 2 5 6 0 7 7 1 8 8 4 15 9 10 5 11 6 12 8 8 13 1 6 9 10 2 12	100

Table IV clearly shows Avalanche effect in RSA asymmetric cipher and Table III represents Avalanche effect in BAES symmetric cipher for same data input. It also depicts the percentage change occurred in ciphertext due to a one bit change in the input data.

TABLE IV. AVALANCHE EFFECT IN RSA

Sl. No	P	Q	Input to RSA	Cipher	% of Change
1	15	18	05051015 101505051 0151012005 50055101015 1510101512	162 107 162 107 199 162 199 107 199 162 199 107 162 107 162 107 199 162 199 107 199 162 199 260 162 162 107 107 162 162 107 107 199 162 199 162 199 107 199 107 199 162 199 162 199 107 199 260	2.08
2	15	18	15051015 101505051 0151012005 50055101015 1510101512	199 107 162107 199 162 199 107 199 162 199 107 162 107 162 107 199 162 199 107 199 162 199 260 162 162 107 107 162 162 107 107 199 162 199 162 199 107 199 107 199 162 199 162 199 107 199 260	2.08
3	15	18	05051015 101505051 0151012005 50055101015 1510101515	162 107 162 107 199 162 199 107 199 162 199 107 162 107 162 107 199 162 199 107 199 162 199 260 162 162 107 107 162 162 107 107 199 162 199 162 199 107 199 107 199 162 199 162 199 107 199 107	2.08

Comparing tables III and IV it is clearly evident that BAES outperforms RSA with respect to the percentage of change in cipher text, when one bit input is changed. This clearly indicates that BAES cipher provides higher level of security in analogous with its counterpart RSA cipher.

VII. CONCLUSION

As the challenge in MANETs is securing data mobility, ciphers play a major role. Most of the present day ciphers pave a way to various types of security breaches by cryptanalysis.

To overcome the limitations, this paper attempts to design a new cipher. Simulation results show that, memory utilized by BAES is less when compared to RSA. BAES shows greater Avalanche effect compared to RSA. Comparatively BAES provides better security with minimal time overhead. The time overhead in BAES is due to processing of biometric key.

BAES cipher can be implemented just like any other ciphers, to secure data being exchanged in the networks.

BAES can be adopted in securing data mobility in various fields. It can be used in banking systems, in military applications, in emergency response systems in industries.

In future it is expected to replace all the applications where AES is currently being used, with an added advantage of biometric security.

REFERENCES

[1] William Stallings, "Cryptography and Network Security Principles and Practice", Pearson Education Inc., 6th Edition, 2014, ISBN: 978-93-325- 1877-3 2.

[2] Amish Kumar and Namita Tiwari, " EFFECTIVE IMPLEMENTATION AND AVALANCHE EFFECT OF AES",published in International Journal of Security, Privacy and Trust Management (IJSPTM), Vol. 1, No 3/4, August 2012.

[3] Septimiu Fabian Mare, Mircea Vladutiu and Lucian Prodan, "Secret data communication system using Steganography, AES and RSA", proceedings of 2011 IEEE 17th International Symposium for Design and Technology in Electronic Packaging (SIITME), 20-23 October 2011, Timisoara, Romania.

[4] Jong Yeon Park, Dong-Guk Han, Okyeon Yi and Dooho Choi, "Ghost Key patterns with equidistant chosen message attack on RSA-CRT", proceedings of 2011 Carnahan Conference on Security Technology, 18-21 October 2011.

[5] Michael Bourg and Pramod Govindan, "RSA Based Biometric Encryption System Using FPGA for Increased Security", 978-1-5090-1071-1/16, 2016 IEEE.

[6] Asma Chaouch, Belgacem Bouallegue and Ouni Bouraoui, "Software Application for Simulation-Based AES, RSA and Elliptic-Curve Algorithms", proceedings of 2nd International Conference on Advanced Technologies for Signal and Image Processing- ATSIP'2016, March 21-24,2016, Monastir, Tunisia.

[7] S. Sridevi Sathya Priya, P. Karthigaikumar, and N.M. SivaMangai , "Generation of 128-Bit Blended Key for AES Algorithm", © Springer International Publishing Switzerland 2015 S.C. Satapathy et al. (eds.), Emerging ICT for Bridging the Future Volume 2, Advances in Intelligent Systems and Computing 338, DOI: 10.1007/978-3-319-13731-5_47.

[8] Srividya. R and Ramesh. B, " Impregnable Biometrics – a Survey", published in International Journal of Scientific and Research Publications, 2018, ISSN 2250-3153.

Srividya R. completed her B.E degree in Computer Science Engineering and M.Tech degree in Digital Electronics from Visvesvaraya Technological University, Belgaum, India, in 2009 and 2011 respectively. Currently she is working as Assistant Professor in the Department of Telecommunication Engineering at K S Institute of Technology, Bengaluru, India. Her areas of interest include encryption algorithms, authentication techniques, security issues in routing protocols and Mobile Ad-Hoc Networks.

Ramesh B. completed his B.E degree in Computer Science Engineering from Mysore University, Karnataka, India in 1991 and M.Tech degree in Computer science from DAVV, Indore, Madhya Pradesh, India, in 1995 and Ph.D degree from Anna University in 2009. Currently he is working as a Professor in the Department of Computer Science and Engineering at Malnad College of Engineering, Hassan, India. His research interests are in the areas of cryptography, congestion control, QoS-aware routing algorithms in ad hoc networks and multimedia network.