Security Enhancement Using Multi-Symmetric Cryptographic Technique

Tushar Anil Patil[1], Prof.Dr.Mrs.K.V.Kulhalli[2]
Department of ME (E & TC)
[1, 2]D. Y. Patil college of Engg. & Tech. kasaba bavada Kolhapur,Maharashtra, India

Abstract-*Cryptography is the technique to provide secure communication to maintain information securities such as data confidentiality, data integrity, authentication, and non-repudiation. Security in today's world is one of the important challenges that people are facing. For achieving faster communication most of confidential data is circulated through network as electronic data. In order to secure the confidential data encryption is done. Encryption is a mechanism that protects valuable information from unwanted people accessing or changing it. Cryptography is the science of using the mathematics to encrypt and decrypt data. In this paper a survey of some important encryption algorithm is provided and comparative study with respect to speed, time. The goal of this method is to overcome the problem of symmetric cryptography failure when the shared key is exposed. The security analysis shows that our scheme withstands all security attack models with different knowledge of the adversary. AMSC produces Cryptography is the technique to provide secure communication to maintain information securities such as data confidentiality, data integrity, authentication, and non-repudiation. In terms of time complexity, AMSC produces the cipher-text in polynomial time with respect to the number and size of the plaintexts and keys.*

Keywords-Symmetric cryptography, Brute force attack, Cipher-text only attack, Deniable encryption, Multi encryption, Ambiguous encryption, Honey encryption.

I. INTRODUCTION

Cryptography is the technique that makes data or network secure by providing security. It is the science of devising methods that allow information to be sent in a secure form in such a way that the only the intended recipient can retrieve the information. Network security is highly based on cryptography. Basically, Cryptography is an art of hiding information by encrypting the message. Ambiguous Multi-Symmetric Cryptography (AMSC) that hide multiple plain-texts in a cipher-text using the same number of keys. Ambiguous Multi Symmetric Cryptography (AMSC) that conceals multiple plain-texts in a cipher-text using the same number of keys. The proposed method AMSC is a cryptographic primitive that preserves plausible deniability after a cryptographic key is discovered. We evaluate AMSC in terms of security and complexity.AMSC can be used in different applications. In cryptography original message is basically encoded in somen on readable format. This process is called encryption. The only person who knows how to decode the message can get the original information. This process is called decryption. On the basis of key used encryption algorithms as asymmetric key algorithms and symmetric key algorithms. Asymmetric key algorithms are those in which encryption and decryption is done by two different keys and symmetric key algorithms are those in which same key is used for both encryption and decryption.

AMSC

AMSC used to send one cipher-text with multiple messages to different receivers. This can be used in different domains. One interesting domain is message broadcasting. Send one message to different receivers on the same IP address. Each receiver will decrypt and get a different content.

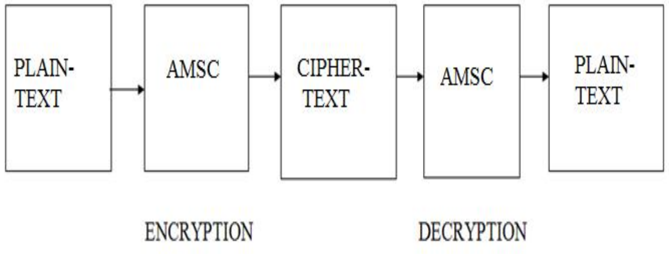


Fig.1:- Block Schematic

Plain-text:-This is original data or message that is fed into the algorithm as input. Data that can be read and understood without any special measures. The plain-text includes message, audio-video files, ATM, credit card and other banking information, private data.

Encryption algorithm:-The encryption algorithm performs Various substitutions and transformation on the plain text. In the encryption plaintext is hide and unreadable form. The encryption ensures that information is hidden from anyone. There are different symmetric key algorithm Advanced Encryption Standard (AES), Data Encryption Standard (DES), Triple DES (3DES).

AMSC:-The AMSC can implement by AMSC1 and AMSC2. The AMSC produces the one cipher text from multiple plain texts using same number of key. The AMSC1 and AMSC2 compare then which one better performance that can be chosen.

Secret key:-The secret key is also input to the encryption algorithm. The value of key independent of the plaintext and of the algorithm. The algorithm will produce a different output depending on the specific key being used at the time. The exact substitution and transformation performed by the algorithm depend on the key. The symmetric key algorithm use same keys are both sender and receiver.

Cipher-text:-This is the scrambled message produced as output. It depends on the plaintext and the secret key. The cipher text is an apparently random stream of data and as it send. The block cipher processes the input one block of elements at a time, producing an output block for each input block. The stream cipher processes input elements constantly, generating output one element at a time.

Decryption algorithm:- This is essentially the encryption algorithm run in reverse. It takes the Cipher text and secret key and produces the original plaintext. The decryption process of degenerate Cipher text to its original plaintext.

II. SCOPE

AMSC used to send one cipher-text with multiple messages to different receivers. This can be used in different domains. One interesting domain is message broadcasting. Send one message to different receivers on the same IP address. Each receiver will decrypt and get a different content.

B) Objective:

- Encrypt multiple variable size plain text with multiple variable size keys into one cipher text.
- Decrypt cipher text with particular key to obtain particular original message.
- Implement AMSC algorithm.
- Plot the timing of encryption with different number of plain texts.
- Compare the results with other symmetric key technique.

C) Methodology:

The proposed work will be implemented by following techniques.

AMSC1:-

The AMSC1 is based on (n-1) linear Diophantine equations. AMSC1 takes n plain-text and n keys with variable size and forms different equations in the form:

$$C=Ki*ai+ Pi$$

Using these equations generate the cipher-text. The necessary encryption steps to compute cipher text C using linear Diophantine equations.

AMSC2:-

The Chinese Remainder theoremused in AMSC2. Expect that m1, m2,…,mrare pair wise relatively prime positive integers, and let a1, a2,…,ar be integers. Then the system of congruence, $x_{\equiv}$ ai(mod mi) for $1 \le i \le r$, Has a unique solution modulo M = m1 * m2 * …* mr, which is given by:

$$x_{\equiv} a1M1ya + a2M2y2 + \ldots + arMryr(\mathrm{mod}\ M),$$

Where Mi= M/mi and $yi_{\equiv} (Mi)^{-1}$ (mod mi) for $1 \le i \le r$.

AMSC2 takes the same input as AMSC1 to generate the cipher-text. Decrypts cipher-text to plain-text in both AMSC1 and AMSC2 use same algorithm. The attacker access one cipher-text a brute force attack is one way to crack the encryption. Because of security use primes and co-primes keys. Co-primes have better security because they will more computations to find key.

RC5 :

RC5 should have a variable-length cryptographic key. The user can choose the level of security appropriate for his application, or as required by external considerations such as export restriction. The key length b in thus a third parameter of RC5.One significant feature of the design of RC5 is its clarity; encryption is based on only three activity: addition, exclusive-or, and rotation. Thus, it makes RC5 both easy to implement, and very importantly, more amenable to analysis than many other block ciphers. The connection between easiness of design and simplicity of analysis, was indeed one of Rivest's goals.

The RC5 encryption algorithm is a block cipher that converts plain text data blocks of 16, 32, and 64 bits into cipher text blocks of the same length. The algorithm is organized as a set of iterations called rounds r that takes values. RC5 works with two 32 bit registers A and B which consist of the original input text or plain text as well as the output cipher at the end of encryption. First we load plain text into the registers A and B then encryption and decryption functions are utilized on it. In encryption procedure, Input text stored in two 32 bit input registers A and B where number of rounds for encryption are 2r+2and round keys will be S[0,1,2,….2r+1].Output text will be stored in A and B. After this process the datais encrypted and stored in registers A and B called cipher text.

The description of the encryption algorithm is given in the pseudo-code below. Assume that the input block is given in two w-bit registers A andB, and that the output is also placed in the registers A and B.

```
A = A + S [0]
B = B + S[1]
For i = 1 to r do
A = ((A _ B) <<<B) + S[2i]
B = ((B _ A) <<< A) + S[2i + 1]
```

The decryption normal is easily derived from the encryption normal.

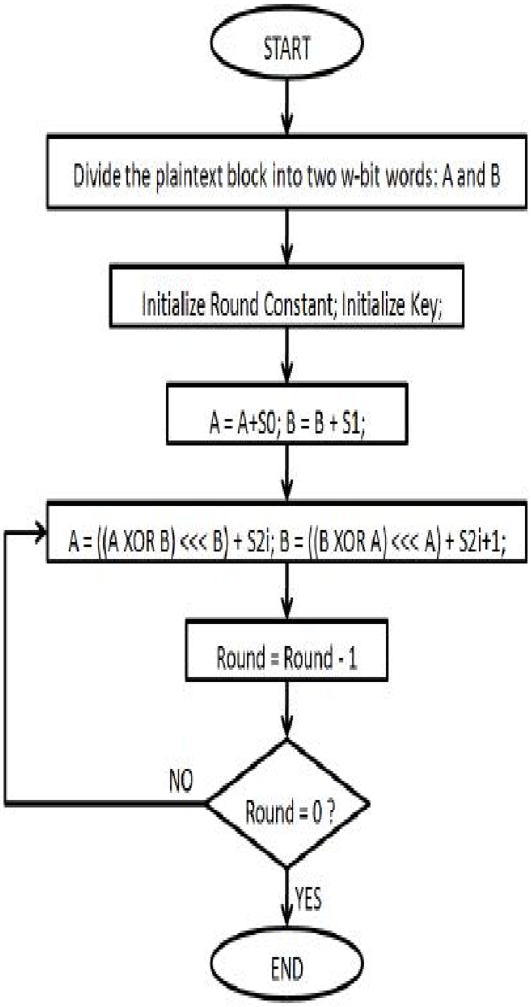
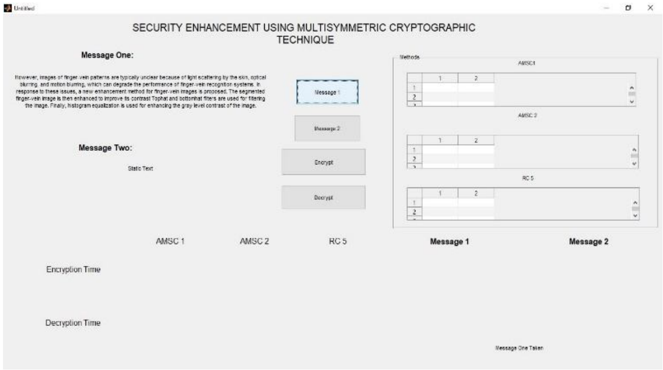

START
Divide the plaintext block into two w-bit words: A and B
Initialize Round Constant; Initialize Key;
A = A+S0; B = B + S1;
A = ((A XOR B) <<< B) + S2i; B = ((B XOR A) <<< A) + S2i+1;
Round = Round - 1
Round = 0 ?
NO
YES
END

Fig.2:- RC5 Flow chart

III. RESULT

The three algorithms in MATLAB gui. Compare these algorithms with encryption and decryption time.

In gui click on message 1 then select the message. The selected message is given.



SECURITY ENHANCEMENT USING MULTISYMMETRIC CRYPTOGRAPHIC TECHNIQUE

Message One:

However, images of finger-vein patterns are typically unclear because of light scattering by the skin, optical blurring, and motion blurring, which can degrade the performance of finger-vein recognition systems. In response to these issues, a new enhancement method for finger-vein images is proposed. The segmented finger-vein image is then enhanced to improve its contrast Tophat and bottomhat filters are used for filtering the image. Finally, histogram equalization is used for enhancing the gray level contrast of the image.

Message Two:

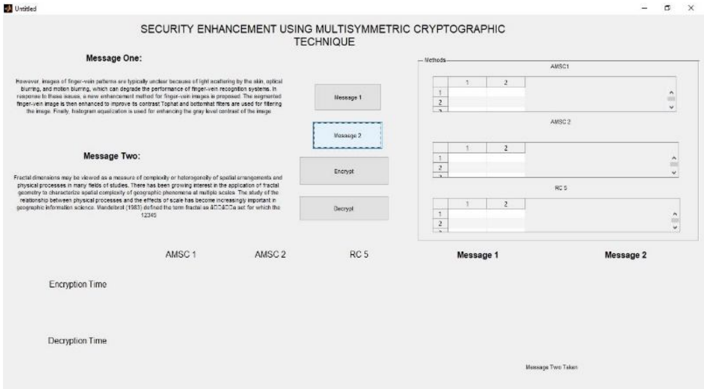
Static Text

	AMSC 1	AMSC 2	RC 5	Message 1	Message 2
Encryption Time					
Decryption Time					

Message One Taken

Fig.3:- first message given

In gui click on message 2 then select the message. The selected message is given.



SECURITY ENHANCEMENT USING MULTISYMMETRIC CRYPTOGRAPHIC TECHNIQUE

Message One:

However, images of finger-vein patterns are typically unclear because of light scattering by the skin, optical blurring, and motion blurring, which can degrade the performance of finger-vein recognition systems. In response to these issues, a new enhancement method for finger-vein images is proposed. The segmented finger-vein image is then enhanced to improve its contrast Tophat and bottomhat filters are used for filtering the image. Finally, histogram equalization is used for enhancing the gray level contrast of the image.

Message Two:

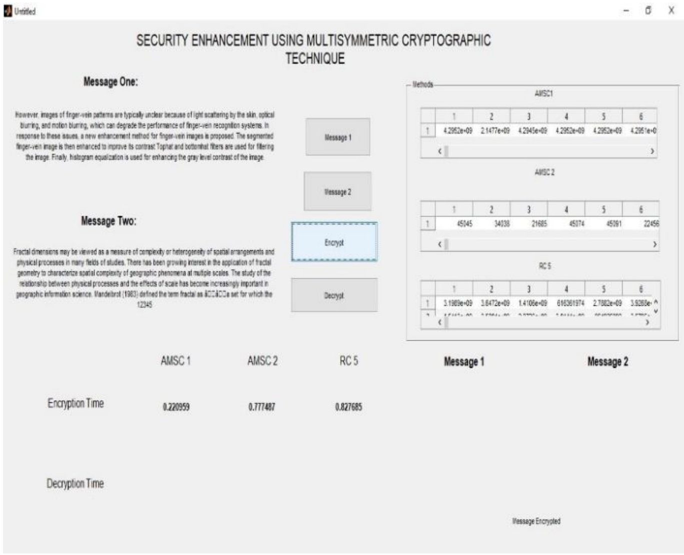
Fractal dimensions may be viewed as a measure of complexity or heterogeneity of spatial arrangements and physical processes in many fields of studies. There has been growing interest in the application of fractal geometry to characterize spatial complexity of geographic phenomena at multiple scales. The study of the relationship between physical processes and the effects of scale has become increasingly important in geographic information science. Mandelbrot (1983) defined the term fractal as â□□â□□a set for which the 12345

	AMSC 1	AMSC 2	RC 5	Message 1	Message 2
Encryption Time					
Decryption Time					

Message Two Taken

Fig.3:- Second message given

Select the two message then click on encryption. Display encryption time of methods.



SECURITY ENHANCEMENT USING MULTISYMMETRIC CRYPTOGRAPHIC TECHNIQUE

Message One:

However, images of finger-vein patterns are typically unclear because of light scattering by the skin, optical blurring, and motion blurring, which can degrade the performance of finger-vein recognition systems. In response to these issues, a new enhancement method for finger-vein images is proposed. The segmented finger-vein image is then enhanced to improve its contrast Tophat and bottomhat filters are used for filtering the image. Finally, histogram equalization is used for enhancing the gray level contrast of the image.

Message Two:

Fractal dimensions may be viewed as a measure of complexity or heterogeneity of spatial arrangements and physical processes in many fields of studies. There has been growing interest in the application of fractal geometry to characterize spatial complexity of geographic phenomena at multiple scales. The study of the relationship between physical processes and the effects of scale has become increasingly important in geographic information science. Mandelbrot (1983) defined the term fractal as â□□â□□a set for which the 12345

AMSC1

	1	2	3	4	5	6
1	4.2952e+09	2.1477e+09	4.2945e+09	4.2952e+09	4.2952e+09	4.2951e+0

AMSC 2

	1	2	3	4	5	6
1	45045	34038	21685	45074	45091	22456

RC 5

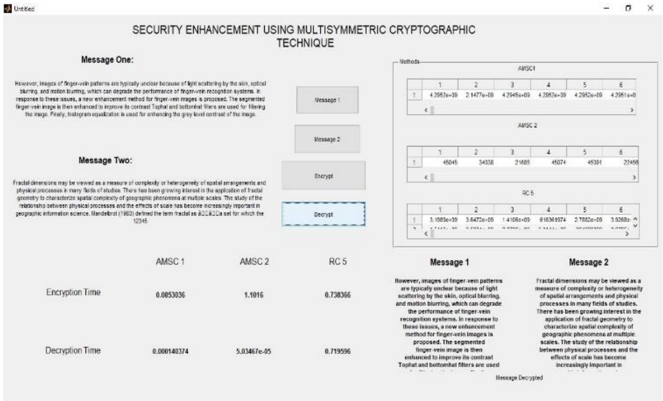
	1	2	3	4	5	6
1	3.1989e+09	3.8472e+09	1.4106e+09	616361974	2.7882e+09	3.9268e+

	AMSC 1	AMSC 2	RC 5	Message 1	Message 2
Encryption Time	0.220959	0.777487	0.827685		
Decryption Time					

Message Encrypted

Fig.5:- Encryption time

Select the decryption then messages have decrypted and display decryption time of methods.



Untitled

SECURITY ENHANCEMENT USING MULTISYMMETRIC CRYPTOGRAPHIC TECHNIQUE

Message One:

However, images of finger-vein patterns are typically unclear because of light scattering by the skin, optical blurring, and motion blurring, which can degrade the performance of finger-vein recognition systems. In response to these issues, a new enhancement method for finger-vein images is proposed. The segmented finger-vein image is then enhanced to improve its contrast Tophat and bottomhat filters are used for filtering the image. Finally, histogram equalization is used for enhancing the grey level contrast of the image.

Message Two:

Fractal dimensions may be viewed as a measure of complexity or heterogeneity of spatial arrangements and physical processes in many fields of studies. There has been growing interest in the application of fractal geometry to characterize spatial complexity of geographic phenomena at multiple scales. The study of the relationship between physical processes and the effects of scale has become increasingly important in geographic information science. Mandelbrot (1983) defined the term fractal as â□□â□□a set for which the 12345

Methods

AMSC1

	1	2	3	4	5	6
1	4.2952e+09	2.1477e+09	4.2945e+09	4.2952e+09	4.2952e+09	4.2951e+0

AMSC 2

	1	2	3	4	5	6
1	45045	34038	21685	45074	45391	22458

RC 5

	1	2	3	4	5	6
1	3.1089e+09	3.6472e+09	1.4106e+09	616361974	2.7882e+09	3.9268e

	AMSC 1	AMSC 2	RC 5
Encryption Time	0.0853036	1.1016	0.738366
Decryption Time	0.000140374	5.03467e-05	0.719596

Message 1

However, images of finger-vein patterns are typically unclear because of light scattering by the skin, optical blurring, and motion blurring, which can degrade the performance of finger-vein recognition systems. In response to these issues, a new enhancement method for finger-vein images is proposed. The segmented finger-vein image is then enhanced to improve its contrast Tophat and bottomhat filters are used

Message 2

Fractal dimensions may be viewed as a measure of complexity or heterogeneity of spatial arrangements and physical processes in many fields of studies. There has been growing interest in the application of fractal geometry to characterize spatial complexity of geographic phenomena at multiple scales. The study of the relationship between physical processes and the effects of scale has become increasingly important in

Message Decrypted

Fig.6:- Decryption time and messages are decrypted

Compare these three methods in a graph. Compare encryption and decryption time in milliseconds with different messages. The messages will text, symbol, alphanumeric. In this graph decide which method require less time.

In fig.7 messages are text messages.

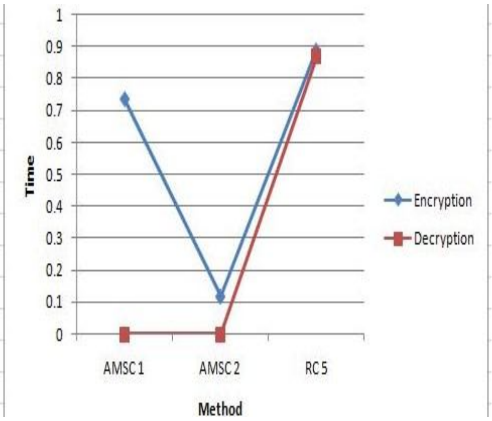


Fig.7:- Graph of Text

In fig.8 messages are numbers.

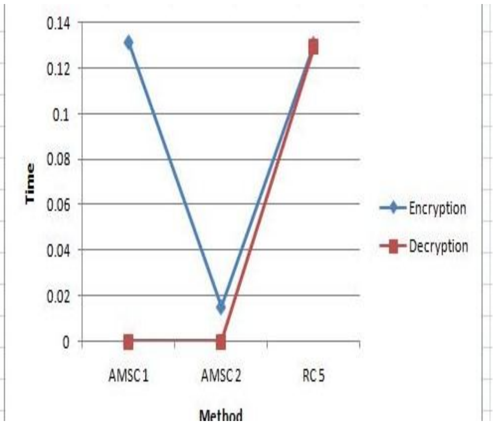


Fig.8:- Graph of Number

In fig.9 messages are alphanumeric.

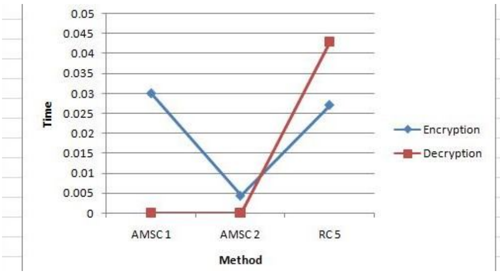


Fig.9:- Graph of Alphanumeric

In fig.10 messages are Symbol.

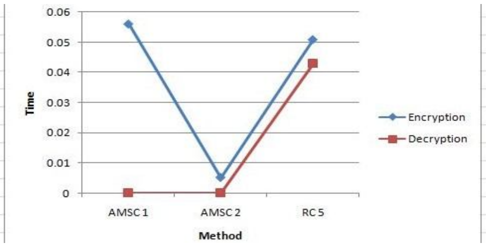


Fig.9:- Graph of Symbol

The above graph shows AMSC2 require less time for encryption and decryption.

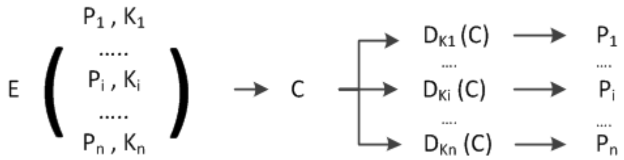
Performance Parameter:

The performance of proposed work is evaluated with following parameters:

- Speed
- Size
- Security
- Time

Transmitter Side:

This method encrypts multiple variable size plain-texts using multiple variable size keys into one cipher-text, hence the name Multi-Symmetric. Fig. shows the system model where P1; P2; :: Pn are the plain texts, K1;K2; ::Kn are the keys respectively, E is the encryption algorithm, D is the decryption algorithm and C is the cipher-text.



Definition 1: Let P1; P2 ;:: Pn be plain-texts, K1;K2; :: Kn be keys accordingly.

Transmitter generates cipher-text:

C = EAMSC ([K1;K2; :::Kn]; [P1; P2; :::Pn])

Cipher-text C represents all plain-texts, and can be decrypted by any key Ki to plain-textPi.

Receiver Side:

At the receiver side decrypts cipher-text C using his key Ki,
Where Pi = C mod Ki.

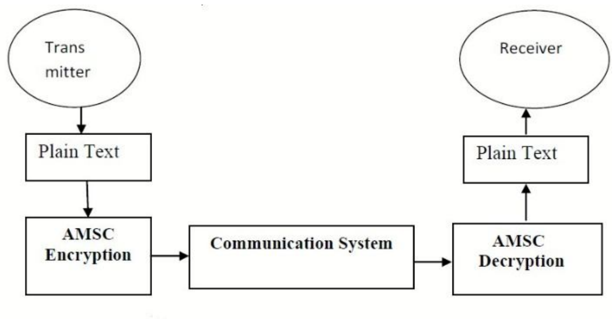


Fig.10:- Standardized Communication Diagram For Transmitter and Receiver

IV. CONCLUSION

This paper, hide multiple plain-texts in cipher-text. The AMSC can be Used in different applications like TCP/IP multicast, secure Communications, etc. Moreover, it presented AMSC as a Method for enigmatic secure communication, where in all Applications, regardless of the knowledge of the adversary, AMSC endures different security attacks. Compared AMSC and RC5 symmetric key algorithm to other approaches such as concatenating cipher-texts and showed the security and overhead advantages. Compare to asymmetric algorithm, symmetric algorithms are faster and provide more security. Normal new encryption technique is deriving hence quick and protected ordinary encryption techniques will ever come out with high rate of security. The result shows the AMSC2 require low encryption and decryption time. AMSC2 is better than other algorithm.

REFERENCES

[1] Dhenakaran S.S, Naganathan E.R, “A New Approach toMultiple symmetric keys” International journal of computer science and network security, vol.7, issue 6, pp 254-259, 2007.

[2] H. Bojinov, E. Bursztein, X. Boyen, and D. Boneh., “Kamouflage: lossresistant password Management.” ESORICS, pp 286-302, 2010.

[3] A. Juels and T. Ristenpart., “Honey encryption: Securitybeyond the brute-force bound.” EUROCRYPT 2014, pp.293-310, 2014.

[4] Bidisha Mandal, Sourabh Chandra, SK Safikul Aalam,subhendu Sekhar Patra, “A Comparative and AnalyticalStudy on Symmetric key cryptography, pp 131-136, 2014.

[5] N. Ruangchaijatupon and P. Krishnamurthy, “Encryptionand power consumption in wireless LANs-N, "The Third IEEE Workshop on Wireless LANs, pp. 148-152, Newton, Massachusetts, 2001.

[6] D. Salama, A. Elminaam and etal, "Evaluating The Performance of Symmetric Encryption Algorithms", International Journal of Network Security, Vo1.10, issue 3, pp 216-222, 2010.

[7] Stallings, W.: Cryptography and Network Security:Principles and Practice, 6e, Pearson Prentice Hall,978-0-13-335469-0, 2014.