Alert Message Creation based Advanced Encryption Standard Algorithm

M.Jayakumar
Ph. D Scholar (CS)
Dept. of Computer Science,
Government Arts College, Udumalpet-642126

T.Christopher, Ph.D
Assistant Professor & Head
Dept. of Computer Science,
Government Arts College, Udumalpet-642126

ABSTRACT
Today the worldwide activities of various organizations, enterprises and institutions, general agencies and individuals are done through Internet. The fast evolution of digital data exchange, security information becomes much important in data storage and transmission. The dramatic increase of data theft is a concern for the Internet community as a whole. Cryptography allows people to carry over the confidence found in the data transaction electronic world; Everyday thousands of people interact electronically, whether it is through e-mail, e-commerce, E-banking or overall data transformation using Internet. The perpetual increase of information transmitted electronically has led to an increased reliance on cryptography. Advanced Encryption Standard algorithm provides high security to information on networks. Further secure key mixing based Advanced Encryption Standard (KAES) algorithm is proposed by modifying the classical Advanced Encryption Standard algorithm. This algorithm is based on secure keys of 12 digit numeric key (Mobile Number). KAES algorithm using shift rows are cyclically shifted random generation values based and create new password sent to communicators mobile. KAES algorithms ensure the improved encryption performance, high secure and less encryption, decryption time. KAES algorithm is highly secure while improving the efficiency of cryptography algorithms.

Keyword
Secure key, Standard Encryption algorithm, Data security, Data integrity, privacy

1. INTRODUCTION
The Internet is a non-secure, potentially hostile environment for organizations to operate in. The challenge is for organizations to harness the benefits that the Internet provides while they maintain necessary levels of data and communication security [1][2].E-mail carries essential messages for the everyday workings of user business. Performing daily business transactions through electronic technologies is an accepted, reliable and necessary tool across the nation. Cryptography technologies have been developed to help organizations secure their systems and data against unauthorized access. Security of information transmitted over the network is becoming tougher in spite of the availability of many cryptographic algorithms [3]. The popular cryptographic algorithm is an Advanced Encryption Standard (AES).This algorithm each cipher uses several rounds of fixed operations and key generation, distributed to achieve desired security level [4]. Further improvement of secure key mixing based Advanced Encryption Standard algorithm is integrate the function of key using 12 digit numeric keys and Date & Time. This algorithm used 12 digit numeric keys as a Mobile Number. So every time encryption process is complete the stage alert message send to corresponding receiver. Last ten numbers is specifying Mobile Number then first two numbers are country code. KAES algorithm is maintaining success cryptography vital principle of data security, efficiency and flexibility.

2. CRYPTOGRAPHY AND NETWORK SECURITY ALGORITHM
Due to vast improvement in the fields of computation and network technology, in open networked systems, information is being received and misused by adversaries by means of facilitating attacks at various levels in the communication. Every concerned about keeping important data confidential, file, folder, or disk at encryption is a good solution. For secure data transmission via Internet or any public network, there is no alternative to cryptography. Many of us either knowingly or unknowingly using cryptic messages while doing online purchase and money transfer. And it is widely used by government and intelligence agencies around the world to safe transmission of any format of messages-online or offline. No data online is secure unless use any type of cryptography to send user messages. User might be thinking what about email user send daily- no email is secure until email system are using any kind of cryptography. So, whenever user sends some confidential business information to user clients, make sure user always use cryptography. Every crypto algorithm has its strength and weakness. A main challenge of data security in open network (Internet) is unauthorized access of data, duplicates, hacking of password, hacking of messages, data loss.

3. SECURE KEY BASED ADVANCED ENCRYPTION STANDARD
The Secure keys mixing based Advanced Encryption Standard have three operational stages:

- *SubBytes* takes the value of a word within a State Matrix and substitutes it with another value by a predefined S-box[5][6]
- *Shift Cells* circularly shifts each column in KAES value

KAES value

12 Digit numeric password1 = 919150282698 - Dispatcher Mobile Number

12 Digit numeric password2 = 919344820156 - Recipient Mobile Number

Date & time = 290920130941
- Encryption process data & time

State matrix decimal value = random generation

Protection Value

KAES value = Protection Value > Addition value of Mod 2^{16}

KAES value => create new password (96 to 192 bit key)

- *MixColumns* takes the value of a 4-word column within the State Matrix and changes the four values using a predefined mathematical function[7][8]

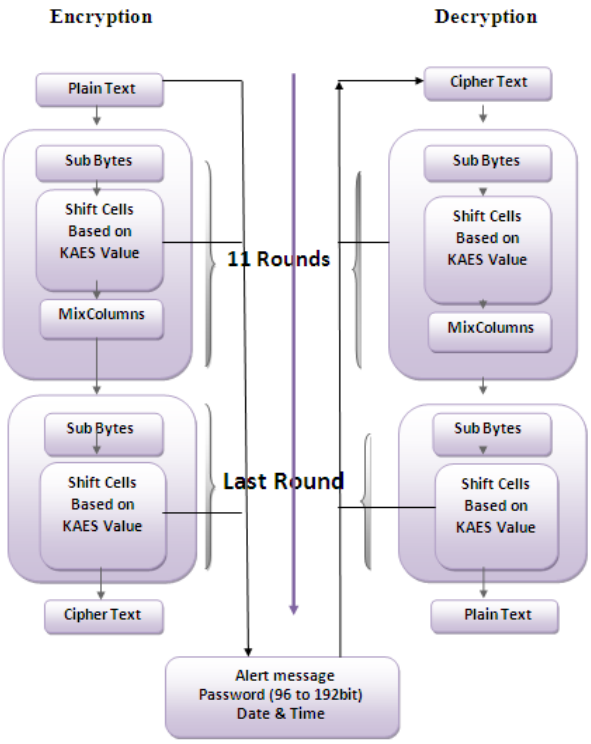

Figure-1 Secure Key based AES

KAES Algorithm

The proposed secure key mixing based Advanced Encryption Standard (KAES) algorithm require a plain text as input and 12 digit numeric keys (Mobile Numbers) and Date & Time as a key values. The main advantage of this proposed method is only can decrypt the encrypted text at the specific input of Date & Time and password. Further improvement of mobile alertness is new vital aspect of cryptographic world.

Encryption

Plain (byte in[4*Nb], byte out[4*Nb])

Key1 & Key2 (12 Digit numeric passwords)

(Date & Time)

Nb=4, 6, 8

Nr=11

Begin

Byte State Matrix [4, Nb]

State Matrix = in

For round = 1 step Nr

SubBytes (State Matrix)

Shift Cells Based on KAES value and password creation

MixColumns (State Matrix)

End for

SubBytes (State Matrix)

Shift Cells based on KAES value and password creation

Out = State Matrix

End

Alert message => Password (96bit to 192 bit) and Date & Time

Decryption

Cipher (byte in [4*Nb], byte out [4*Nb]])

Key1 & Key2 (96 to 192 bit key)

(Date & Time)

Key =true

Nb=4, 6, 8

Nr=11

Begin

Byte State Matrix [4, Nb]

State Matrix = in

For round = 1 step Nr

SubBytes (State Matrix)

Shift Cells based on KAES value and password checking

MixColumns (State Matrix)

End for

SubBytes (State Matrix)

Shift Cells based on KAES value and password checking

Out = State Matrix

Key=false

Out =State Matrix in

End

3 .1 The SubBytes transformation

The substitute bytes transformation operates on each of the State Matrix bytes independently and changes the byte value [9]. An S-box, or *substitution table*, controls the transformation. SubBytes transformation is that a given byte in State Matrix s is given a new value in State Matrix s' according to the S-box. The S-box is a function on a byte in State Matrix s so that:

$$s'_{i,j} = \text{S-box}\ (s_{i,j})$$

The general depiction of this transformation is shown Figure-2:

$s_{0,0}$	$s_{0,1}$	$s_{0,2}$	$s_{0,3}$		$s'_{0,0}$	$s'_{0,1}$	$s'_{0,2}$	$s'_{0,3}$
$s_{1,0}$	$s_{1,1}$	$s_{1,2}$	$s_{1,3}$	S-Box	$s'_{1,0}$	$s'_{1,1}$	$s'_{1,2}$	$s'_{1,3}$
$s_{2,0}$	$s_{2,1}$	$s_{2,2}$	$s_{2,3}$		$s'_{2,0}$	$s'_{2,1}$	$s'_{2,2}$	$s'_{2,3}$
$s_{3,0}$	$s_{3,1}$	$s_{3,2}$	$s_{3,3}$		$s'_{3,0}$	$s'_{3,1}$	$s'_{3,2}$	$s'_{3,3}$

43	75	20	65		1A	9D	B7	4D
6F	74	53	6E	S-Box	A8	92	ED	9F
6D	65	63	63		3C	4D	FB	FB
70	72	69	65		51	40	F9	4D

Figure-2 S-box substitution

3.2 The Shift Cells based on KAES value transformation

The shift cells transformation cyclically shifts the bytes based on KAES value. According to KAES value 11 then respectively as shown in Figure 3

SM = $\sum_{0(i,j)}^{n} \boldsymbol{M}$ Where $0 \leq I \leq 3$, $0 \leq j \leq 3$

SC = $\sum_{0}^{n(12)} \boldsymbol{K1} + \sum_{0}^{n(12)} \boldsymbol{K2} + \sum_{0}^{n(12)} \boldsymbol{DT}$ Modulo 2^{16}

Where $0 \leq SC \leq 15$

SM => State Matrix

K1&K2 => 12 Digit Numeric Values

DT => Date & Time

State S			
$s_{0,0}$	$s_{0,1}$	$s_{0,2}$	$s_{0,3}$
$s_{1,0}$	$s_{1,1}$	$s_{1,2}$	$s_{1,3}$
$s_{2,0}$	$s_{2,1}$	$s_{2,2}$	$s_{2,3}$
$s_{3,0}$	$s_{3,1}$	$s_{3,2}$	$s_{3,3}$

State S'			
$s_{0,0}$	$s_{0,1}$	$s_{0,2}$	$s_{0,3}$
$s_{1,2}$	$s_{1,3}$	$s_{1,0}$	$s_{1,1}$
$s_{2,0}$	$s_{2,1}$	$s_{2,3}$	$s_{3,0}$
$s_{3,1}$	$s_{3,2}$	$s_{3,3}$	$s_{2,2}$

A	9D	B7	4D
A8	92	ED	9F
3C	4D	FB	FB
51	40	F9	4D

1A	9D	B7	4D
A8	92	ED	9F
3C	4D	FB	51
40	F9	4D	FB

Figure-3 Secure Key based Shift cells

3.3 MixColumn () Transformation

The Mix Columns transformation operates on the State column-by-column, treating each column as a four-term polynomial [10]. The columns are considered as polynomials over GF (2^8) and multiplied modulo x^4+1 by a fixed polynomial a (x):

A (x) = (03) x^3 + (01) x2+ (01) x+ (02)

This can be written as a matrix multiplication as follows:

S'(x) =A(x) x S(x)

$$\begin{pmatrix} S'_{0,c} \\ S'_{1,c} \\ S'_{2,c} \\ S'_{3,c} \end{pmatrix} = \begin{pmatrix} 02\ 03\ 01\ 01 \\ 01\ 02\ 03\ 01 \\ 01\ 01\ 02\ 03 \\ 03\ 01\ 01\ 02 \end{pmatrix} \times \begin{pmatrix} S_{o,c} \\ S_{1,c} \\ S_{2,c} \\ S_{3,c} \end{pmatrix} \quad \text{for} \quad 0 \leq C \leq 4$$

As a result of this multiplication, the four bytes in a column are replaced as [11]

$S'_{0,c} = ([02].S_{0,c}) \times ([03].S_{1,c}) \times S_{2,c} \times S_{3,c}$

$S'_{0,c} = S_{0,c} \times ([02].S_{1,c}) \times ([03].S_{2,c}) \times S_{3,c}$

$S'_{0,c} = S_{0,c} \times S_{1,c} \times ([02].S_{2,c}) \times ([03].S_{3,c})$

$S'_{0,c} = ([03].S_{0,c}) \times S_{1,c} \times S_{2,c} \times ([02].S_{3,c})$

State S			
$s_{0,0}$	$s_{0,1}$	$s_{0,2}$	$s_{0,3}$
$s_{1,0}$	$s_{1,1}$	$s_{1,2}$	$s_{1,3}$
$s_{2,0}$	$s_{2,1}$	$s_{2,2}$	$s_{2,3}$
$s_{3,0}$	$s_{3,1}$	$s_{3,2}$	$s_{3,3}$

x

State P			
02	03	01	01
01	02	03	01
01	01	02	03
03	01	01	02

State SP			
$sp_{0,0}$	$sp_{0,1}$	$sp_{0,2}$	$sp_{0,3}$
$sp_{1,0}$	$sp_{1,1}$	$sp_{1,2}$	$sp_{1,3}$
$sp_{2,0}$	$sp_{2,1}$	$sp_{2,2}$	$sp_{2,3}$
$sp_{3,0}$	$sp_{3,1}$	$sp_{3,2}$	$sp_{3,3}$

1A	9D	B7	4D
A8	92	ED	9F
3C	4D	FB	51
40	F9	4D	FB

x

02	03	01	01
01	02	03	01
01	01	02	03
03	01	01	02

AB	38	EF	8A
55	8C	2D	60
0A	85	60	66
3A	8A	4E	F4

Figure-4 Mixcolumn multiplication

Finally after 12 rounds we get chipper text as shown in Figure-5

FF	**E7**	**DD**	**F7**
B1	**7D**	**5C**	**F4**
AC	**68**	**AC**	**C6**
00	**C3**	**14**	**2C**

Figure-5 KAES Output

For the plain text "436F6D70757465722053636965 6E6365", Secure key 12 digit password key1"919150282698", key2 "919344820156"and Date & Time "29/09/2013 09:41", the KAES algorithm generate the following output value

"FFB1AC00E77D68C3DD5CAC14F7F4C62C"

Password: "01410259731410611"

4. PROTECTION IMPROVEMENT OF AES

The most important security to be given during communication is "unauthorized access". Main challenge of data security in open network (Internet) is unauthorized access of data, duplicates, hacking of password, hacking of messages, data

loss. This algorithm is inbuilt communicators Mobile Number (initially collected regarding communicators Mobile Number) like a numeric 12 digit passwords, Date & time also including. So any doubt for message is wrong then easy to check Date & Time stamp and alert message status. It's through double protection is created.

I. Alert Message & password: Only authorized holder access the text, this algorithm protect encryption time automatically message (Password and Date & Time) are send to receiver and decryption time message send to sender. Suppose unauthorized access is attempt in decryption process then the message status and structure automatically changed and alert message send to dispatcher.

II. Date & Time: Since encryption process status are integrated in this algorithm, so it is easily identified wrong and faked messages received the receiver then the message originality easily checked. This stage alert message and Date & Time is verify then captures the message status.

III. KAES Algorithm: Security improvement purpose this algorithm is initiate add four security factor

- 12 Digit numeric password (Sender Mobile Number)
- 12 Digit numeric password (Receiver Mobile Number)
- Date & time
- Create new password different sizes (96 bit to 192 bit)

Encryption time given value is receiver Mobile number except Date & Time automatically captures the machine. Decryption time is checking two keys of password and Date & Time. Protection improvement of Advanced Encryption Standard algorithm is inbuilt the part of numeric password (Mobile Number). KAES value based on Shift cells process are increases the security. KAES Encryption process is inbuilt on dispatcher and recipient Mobile Number; it's through automatically create the message is reach to receiver and sender. So hackers, unauthorized access is not possible.

5. CPU TIME COMPARISON

Time taken for encryption and decryption process is significantly less in KAES algorithm than AES algorithm. The Figure-6 shows time taken for encryption and decryption process of AES algorithm and KAES algorithm

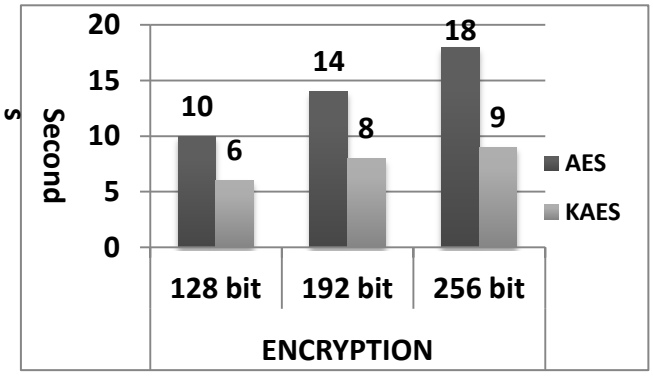

Figure-6 Encryption Time management of AES vs. KAES

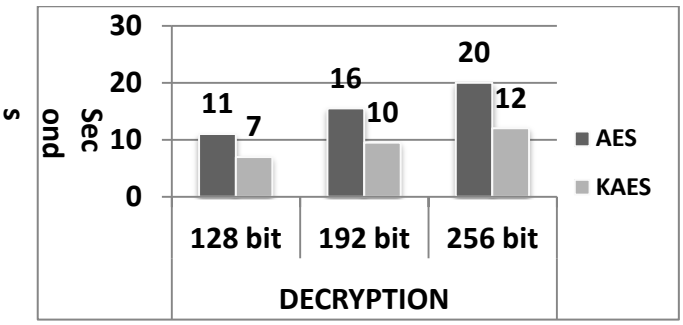

Figure-7 Decryption Time management of AES vs. KAES

6. ADVANTAGES OF SECURE KEY BASED AES

The proposed KAES algorithm is effectively stops their known attack resistance than the AES algorithm. As 6th figure shows in 256 bit encryption process, KAES algorithm takes 9 sec to encrypt plain text which is almost 50% of time while comparing AES algorithm. This algorithm designed using simplified 35 modules used and at the same time high data security of encryption and decryption process maintained. KAES algorithm Protection of inbuilt numeric key based algorithm to execute the process is high level security in cryptography. Every time process is complete stage alert message send to corresponding key value holder. So unauthorized access is attempt easily identifying chance available.

Secure key based AES algorithm ensure to met the standard cryptography goals such as

- Information in computer is transmitted and has to be accessed only by the authorized holder and not by anyone else.
- The information received by any system has to check the identity of the sender that whether the information is arriving from a authorized address or a false identity
- Only the authorized party is allowed to decryption process, otherwise easily identify message originality.
- Date & time as a key is used confidence to message originality.

6.1 Protection of Security attacks

The development of computer networks has lead to a world full of connected computational resource. The most important factor is to secure the information store by a user. Information can be easily copied or erased or modified. This stage secure the information of secure key (Mobile Number) may be attached to each user, while configuring and sending may be a properly. Security review shown Figure-8

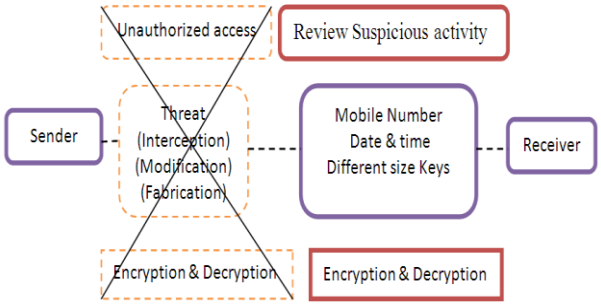

Figure-8 Security review

Brute –force and side channel attacks: A brute force attack systematically attempts every possible key. It is most often used in a known plaintext or cipher text-only attack. A side channel attack leverages additional information, such as time taken or CPU cycles used, to perform a calculation, voltage used. Side channel attack is hacker observes time/power and cracks cipher without trying each key. CPU cycle analysis shown Figure-9

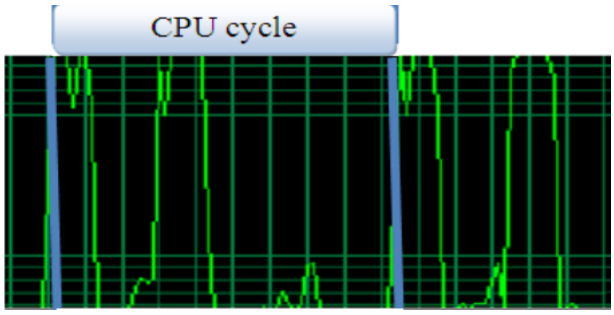

Figure-9 Power analysis of Side-Channel attack

KAES algorithm is using three different type of keys .So key guessing and possible key checking is not possible. This algorithm is using one key automatically capture the machine and other key create different sizes. Uses for time and power analysis are not potential. Further maximum of unauthorized message modification is identifying or stop of this method using properly. Still inbuilt 12 digit passwords and Date & Time keys using the algorithm and creation different size of password are increase the security. Key size is similar but additional keys using this algorithm, so hackers attack is not possible. Shift cells transformation is 128 bit circulation based on random generating value. But AES algorithm shift row process is constant.

Table-1 Comparison of AES & KAES

Advanced encryption Standard	**Secure key using Advanced encryption standard**
Key size =128,192,256 bit	Key Size = **192** Bit
Encryption Rounds =Initial Round +(10 ,12,14)	Encryption rounds =**12** Rounds
Modules =50	Modules =**35**
Single key	Different type of **three** keys
Shift rows Constant	Random number generation
Possible Side-Channel Attack	Not possible
Not possible for Alert messages	Possible alert messages

7. CONCLUSION

This approach also provides more security, confidentiality, and authentication as KAES algorithm is strong enough to Encryption and decryption process. The basic design of an encryption algorithm is based upon the strength of mathematical calculations, cryptanalytic resistance; randomness. This procedure explores efficiency of time/space, hardware and software and flexibility of keys. This proposed a revised Advanced Encryption Standard algorithm using Key mix using numeric keys and Date & Time key instead of conventional key addition which increases the security of KAES. Secure key mixing based advanced encryption standard is stronger and Date & Time include the processes increase the security. Unauthorized access is not possible for this algorithm because alert messages every process completed stage create and send to communicators mobile. The proposed secure key mixing based advanced encryption standard algorithm is very effective, efficient performance in terms of effect than other encryption algorithms. Security analysis and experimental results the proposed encryption and decryption scheme is fast and on the other hand it provides good security on the data.

8. REFERENCES

[1] Stallings W. Cryptography and Network Security. Prentice Hall, Upper Saddle River,New Jersey, USA, second edition, 1999.

[2] U.S. Department of Commerce / National Institute of Standard and Technology. FIPS PUB 197, Specification for the Advanced Encryption Standard (AES), November 2001. Available at http://csrc.nist.gov/encryption/aes.

[3] William Stallings,"Network Security Essentials(Applications and Standards)"*Pearson Education*, 2004,pp.2-80.

[4] National Institute of Standards and Technology (US), Advanced Encryption Standard, Http://csrc.nist.gov/publication/drafts/dfips-AES.pdf.

[5] Charles P. Pfleeger, Shari Lawrence Pfleeger. "Security in Computing", *Pearson Education* 2004 pp. 642-666.

[6] William Stallings, *Cryptography and Network Security*, Pearson Education, 2009.

[7] Behrouz A. Forouzan, De Anza College *Cryptography and Network Security* (McGraw-Hill,2007)

[8] W. Mao, Modern Cryptography: Theory and Practice. Prentice Hall, 2003

[9] Trenholme, S. "S-box." *AES*. 2010. http://www.samiam.org/s-box.html

[10] *Wolfram MathWorld: The Web's Most Extensive Mathematics Resource*. March 3, 2010. http://mathworld.wolfram.com/FiniteField.html

[11] Trenholme, S. "Rijndael's MixColumn Stage." *AES*. 2010. http://www.samiam.org/mix- column.html.