# Text Encryption using Modified AES-2 Keys

Zahraa K. Taha
M.SC
Department of Network Engineering
College of engineering, Al-Iraqia University

## ABSTRACT
Data security is an essential component of an organization in order to keep the information safe from various competitors. This project includes the complete step by step implementation of Advanced Encryption Technique, i.e. encrypting 128 bit data using the modification AES-2Keys. The encryption process consists of the combination of various classical techniques such as substitution, rearrangement and transformation encoding techniques. Simulation results have been achieved using MATLAB R2015a; Results prove that the proposed algorithm resists different type of attacks. As a conclusion, the addition of an arithmetic operation and two keys don't effect on time of transmission data but makes the data more secure.

## General Terms
Security, Theory, Algorithm

## Keywords
Cryptography, Advance Encryption Standard, Cipher Text, Plain Text.

## 1. INTRODUCTION
The development of network technologies and digital devices makes the delivery of digital multimedia fast and easy. However, transmitting digital data over public networks such as the internet is not safe. Therefore, methods for protecting digital data, especially sensitive data, are highly essential[1]. There are a number of ways for securing data. The art and science of keeping messages secure is called cryptography [2]. The sender uses an encryption key to scramble the message, this scrambled message is transmitted through the insecure public channel, and the reconstruction of the original, unencrypted message is possible only if the receiver has the appropriate decryption key[3]. A cryptographic algorithm, or cipher, is a mathematical function used in the encryption and decryption process. A cryptographic algorithm works in combination with a key—a word, number, or phrase—to encrypt the plaintext. The same plaintext encrypts to different ciphertext with different keys. The length and strength of the Cryptography keys are considered an important mechanism. The keys used for encryption and decryption must be strong enough to produce strong encryption. They must be protected from unauthorized users and must be available when they are needed. Cryptography also contributes to computer science, particularly, in the techniques used in computer and network security for access control and information confidentiality. Cryptography is also used in many applications encountered in everyday life such as: computer passwords, ATM cards, and electronic commerce [4]. The symmetric encryption scheme has five ingredients (see Figure 1) [5]:

- Plaintext: This is the original intelligible message or data that is fed to the algorithm as input.
- Encryption algorithm: The encryption algorithm performs various substitutions and permutations on the plaintext
- Secret Key: The secret key is also input to the encryption algorithm. The exact substitutions and permutations performed depend on the key used, and the algorithm will produce a different output depending on the specific key being used at the time.
- Ciphertext: It is the encrypted text. The text obtain after encoding the data with the help of a key is known as cipher text.

Decryption Algorithm: This is essentially the encryption algorithm run in reverse. It takes the ciphertext and the secret key and produces the original plaintext.

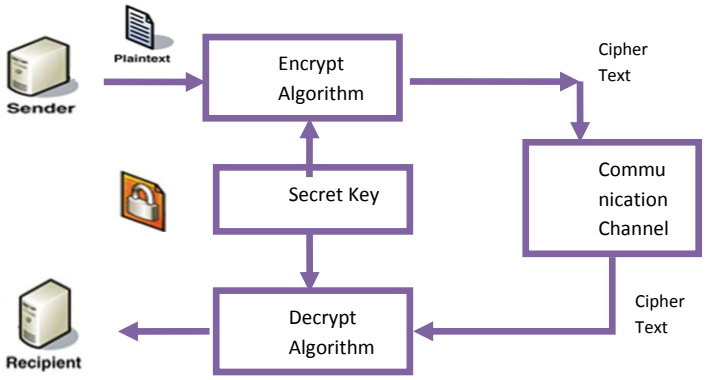


**Fig 1: Basic model of cryptography system**

## 2. METHOD
The proposed method includes the complete step by step implementation of Advanced Encryption Technique, i.e. encrypting 128 bit data using the AES and it's modification for enhanced reliability and security. The encryption process consists of the combination of various classical techniques such as substitution, rearrangement and transformation encoding techniques. The modifications include the addition of an arithmetic operation and use of two keys for data security. So in this paper, Advance Encryption Standard algorithm (AES) will be used as the base of the encryption. The next level of encryption is the use another key to encrypt the cipher text that can improve security of transmission data.

## 3. ADVANCE ENCRYPTION STANDARD (AES-128 BITS)
Advanced Encryption Standard (AES), also known as Rijindael is used for securing information. AES is a symmetric block cipher that has been analyzed extensively and is used widely now-a-days. AES, symmetric key encryption algorithm is used with key length of 128-bits for this purpose. High security, mathematical soundness,

resistance to all known attacks, high encryption speed, worldwide royalty free use, suitability across wide range of hardware and software are the characteristics of AES algorithm. The basic structure of AES is shown in Figure 2

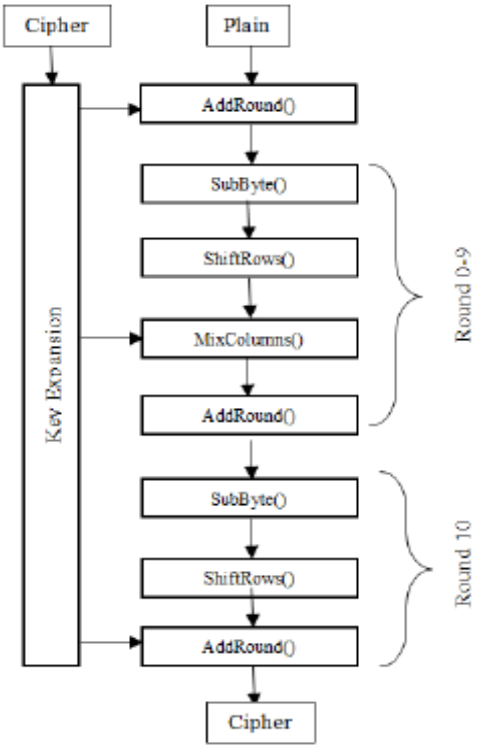


**Fig 2: Basic Structure of AES 128 Bit algorithm**

The algorithm begins with an Add round key stage followed by 9 rounds of four stages and a tenth round of three stages. The four stages are as follows [6]:

1. Substitute bytes
2. Shift rows
3. Mix Columns
4. Add Round Key

The tenth round simply leaves out the Mix Columns stage.

## 3.1 Substitute bytes

It is a table using 16*16 matrix of byte value called an S-box (as shown in Figure 3) the matrix consists of all the possible combinations of an 8bits sequence (256) each byte in matrix is mapped into a new byte. For example, the byte {95} selects row 9 columns 5 which turn out to contain the value {2A}. This is then used to update the state matrix.

| | 0 | 1 | 2 | 3 | 4 | 5 | 6 | 7 | 8 | 9 | A | B | C | D | E | F |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| 0 | 63 | 7C | 77 | 7B | F2 | 6B | 6F | C5 | 30 | 01 | 67 | 2B | FE | D7 | AB | 76 |
| 1 | CA | 82 | C9 | 7D | FA | 59 | 47 | F0 | AD | D4 | A2 | AF | 9C | A4 | 72 | C0 |
| 2 | B7 | FD | 93 | 26 | 36 | 3F | F7 | CC | 34 | A5 | E5 | F1 | 71 | D8 | 31 | 15 |
| 3 | 04 | C7 | 23 | C3 | 18 | 96 | 05 | 9A | 07 | 12 | 80 | E2 | EB | 27 | B2 | 75 |
| 4 | 09 | 83 | 2C | 1A | 1B | 6E | 5A | A0 | 52 | 3B | D6 | B3 | 29 | E3 | 2F | 84 |
| 5 | 53 | D1 | 00 | ED | 20 | FC | B1 | 5B | 6A | CB | BE | 39 | 4A | 4C | 58 | CF |
| 6 | D0 | EF | AA | FB | 43 | 4D | 33 | 85 | 45 | F9 | 02 | 7F | 50 | 3C | 9F | A8 |
| 7 | 51 | A3 | 40 | 8F | 92 | 9D | 38 | F5 | BC | B6 | DA | 21 | 10 | FF | F3 | D2 |
| 8 | CD | 0C | 13 | EC | 5F | 97 | 44 | 17 | C4 | A7 | 7E | 3D | 64 | 5D | 19 | 73 |
| 9 | 60 | 81 | 4F | DC | 22 | 2A | 90 | 88 | 46 | EE | B8 | 14 | DE | 5E | 0B | DB |
| A | E0 | 32 | 3A | 0A | 49 | 06 | 24 | 5C | C2 | D3 | AC | 62 | 91 | 95 | E4 | 79 |
| B | E7 | C8 | 37 | 6D | 8D | D5 | 4E | A9 | 6C | 56 | F4 | EA | 65 | 7A | AE | 08 |
| C | BA | 78 | 25 | 2E | 1C | A6 | B4 | C6 | E8 | DD | 74 | 1F | 4B | BD | 8B | 8A |
| D | 70 | 3E | B5 | 66 | 48 | 03 | F6 | 0E | 61 | 35 | 57 | B9 | 86 | C1 | 1D | 9E |
| E | E1 | F8 | 98 | 11 | 69 | D9 | 8E | 94 | 9B | 1E | 87 | E9 | CE | 55 | 28 | DF |
| F | 8C | A1 | 89 | 0D | BF | E6 | 42 | 68 | 41 | 99 | 2D | 0F | B0 | 54 | BB | 16 |

**Fig 3: S-box substitution values for the byte (in hexadecimal format)**

## 3.2 Shift rows Transformation

This stage is known as Shift rows. This is a simple permutation an nothing more. It works as follow:

The first row of state is not altered.

The second row is shifted 1 bytes to the left in a circular manner.

The third row is shifted 2 bytes to the left in a circular manner.

The fourth row is shifted 2 bytes to the left in a circular manner.

## 3.3 Mix Columns

This stage (known as MixColumn) is basically a substitution but it makes use of arithmetic of GF (28). Each column is operated on individually. Each byte of a column is mapped into a new value that is a function of all four bytes in the column. The transformation can be determined by the following matrix multiplication on state Each element of the product matrix is the sum of products of elements of one row and one column.

## 3.4 Add Round Key

In this stage (known as AddRoundKey) the 128 bits of state are bitwise XORed with the 128 bits of the round key. The operation is viewed as a columnwise operation between the 4 bytes of a state column and one word of the round key. This transformation is as simple as possible which helps in efficiency but it also affects every bit of state.

## 3.5 The AES key expansion algorithm

The AES key expansion algorithm takes as input a 4-word key and produces a linear array of 44 words. The function consists of the following subfunctions:

1. RotWord performs a one-byte circular left shift on a word. This means that an input word [b0, b1, b2, b3] is transformed into [b1, b2, b3, b0].
2. SubWord performs a byte substitution on each byte of its input word, using the s-box described earlier.
3. The result of steps 1 and 2 is XORed with round constant, Rcon[j] shown in table 1.

**Table 1. Round constant values**

| j | RC[j] |
|---|---|
| 1 | 01 |
| 2 | 02 |
| 3 | 04 |
| 4 | 08 |
| 5 | 10 |
| 6 | 20 |
| 7 | 40 |
| 8 | 80 |
| 9 | 1B |
| 10 | 36 |
| 11 | 6C |
| 12 | d8 |
| 13 | A6 |
| 14 | 4d |

## 4. THE PROPOSED METHOD

The proposed algorithm is modifying symmetric block cipher cryptography (AES) with different keys that are simple and more efficient for sending hidden message. The modifications include the addition of an arithmetic operation and use of two keys for data security. AES is fast in both software and hardware and is used to prevent sensitive data from being available in readable format. The steps of the proposed algorithm are shown in figure. The second key is used to hide an encrypted text (text is encrypted by AES). Figure 4 shows an example of applying the proposed algorithm AES.

Algorithm of the proposed system AES-2key

Step1: Determine the set of round keys from the cipher key.

Step2: Initialize the state array with the block data (plaintext).

Step3: Add the initial round key to the starting state array.

Step4: Perform nine rounds of state manipulation.

Step5: Perform the tenth and final round of state manipulation.

Step6: Copy the final state array out as the encrypted data (ciphertext).

Step7: generate second key

Step8: rearrange the second key

Step9: Xor between encrypted data and the second key

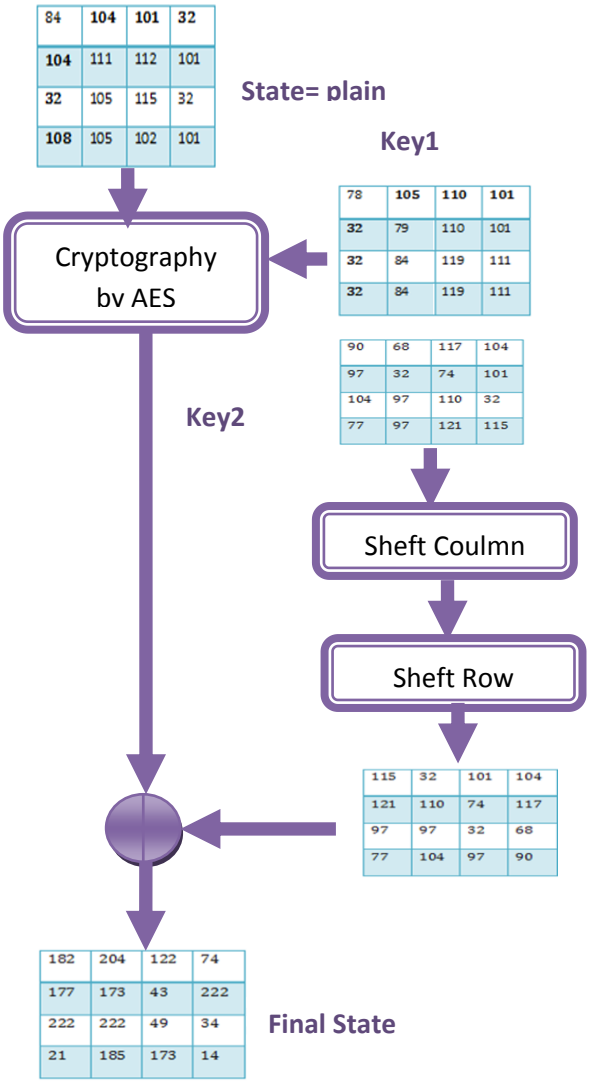


**Fig.4. Example of applying the proposed algorithm AES-2 Key**

## 5. RESULTS

In this section, the experimental result shows the evaluation of our proposed technique. The modification of AES-2 Keys can be used to protect text

The suggestion method (AES-2keys) code was tested using two keys. Simulation results have also been drawn using MATLAB R2015a. Following example shows the transmission of encrypted text. To implement proposed algorithm we have to focus on two parts which are a) key generation, and b) encryption process. One of the results is given below.

Plain text is encrypted by AES-2 keys

Plain text: 'The hope is life'

Plaintext in Hex (128 bits): 84 104 101 32 104 111 112 101 32 105 115 32 108 105 102 101

Key1: 'Nine One Two Two'

Key1 in Hex (128 bits): 78 105 110 101 32 79 110 101 32 84 119 111 32 84 119 111

**AES-2Keys Example - The 1st Roundkey**

W[0]=[ 4e 69 6e 65], W[1]=[ 20 4f 6e 65], W[2]=[ 20 54 77 6f], W[3]=[20 54 77 6f]

Circular byte left shift of w[3]: [54 77 6f 20]

Byte Substitution (S-Box):[20 f5 a8 b7]

Adding round constant (01; 00; 00; 00) gives: g(w[3])=[ 21 f5 a8 b7]

w[4] = w[0] XOR g(w[3]) =[7f 9c c6 d2]

w[5] = w[4] XOR w[1] =[5f d3 a8 b7]

w[6] = w[5] XOR w[2] =[7f 87 df d8]

w[7] = w[6] XOR w[3] = [5f d3 a8 b7]

**AES Example - All RoundKeys**

| Round 0 | | | | Round 1 | | | |
|---|---|---|---|---|---|---|---|
| 4E | 69 | 6E | 65 | 6F | 9C | C6 | D2 |
| 20 | 4F | 6E | 65 | 4F | D3 | A8 | B7 |
| 20 | 54 | 77 | 6F | 6F | 87 | DF | D8 |
| 20 | 54 | 77 | 6F | 4F | D3 | A8 | B7 |
| Round 2 | | | | Round 3 | | | |
| 0B | 5E | 6F | 56 | 3A | B9 | 76 | 15 |
| 44 | 8D | C7 | E1 | 7E | 34 | B1 | F4 |
| 2B | 0A | 18 | 39 | 55 | 3E | A9 | CD |
| 64 | D9 | B0 | 8F | 31 | E7 | 19 | 43 |
| Round 4 | | | | Round 5 | | | |
| A6 | 6D | 6C | D2 | 7B | 51 | AE | B7 |
| D8 | 59 | DD | 26 | A3 | 8 | 73 | 91 |
| 8D | 67 | 74 | EB | 2E | 6F | 7 | 7A |
| BC | 80 | 6D | A8 | 92 | EF | 6A | D2 |
| Round 6 | | | | Round 7 | | | |
| 84 | 53 | 1B | F8 | 7D | 38 | 63 | EC |
| 27 | 5B | 68 | 69 | 5A | 63 | 0B | 85 |
| 9 | 34 | 6F | 13 | 53 | 57 | 64 | 96 |
| 9B | DB | 5 | C1 | C8 | 8C | 61 | 57 |
| Round 8 | | | | Round9 | | | |
| 99 | D7 | 38 | 4 | 2A | D2 | 31 | 6E |
| C3 | B4 | 33 | 81 | E9 | 66 | 2 | EF |
| 90 | E3 | 57 | 17 | 79 | 85 | 55 | F8 |
| 58 | 6F | 36 | 40 | 21 | EA | 63 | B8 |
| Round10 | | | | | | | |
| 9B | 29 | 5D | 93 | | | | |
| 72 | 4F | 5F | 7C | | | | |
| 0B | CA | 0A | 84 | | | | |
| 2A | 20 | 69 | 3C | | | | |

**AES Example - Add Roundkey, Round 0**

State Matrix and Roundkey No.0 Matrix:

**State**

| | | | |
|---|---|---|---|
| 54 | 68 | 65 | 20 |
| 68 | 6F | 70 | 65 |
| 20 | 69 | 73 | 20 |
| 6C | 69 | 66 | 65 |

**Round Key**

| | | | |
|---|---|---|---|
| 4E | 69 | 6E | 65 |
| 20 | 4F | 6E | 65 |
| 20 | 54 | 77 | 6F |
| 20 | 54 | 77 | 6F |

XOR the corresponding entries, e.g., 54 Xor 4E=1A

0101 0100

Xor 0100 1110

---

0001 1010 = 1A

**The new State Matrix is**

| | | | |
|---|---|---|---|
| 1A | 1 | 4E | 9 |
| 48 | 20 | 7 | 0C |
| 45 | 24 | 4 | 9 |
| 0 | 31 | 57 | 0A |

**AES-2 Keys Example - Round 10**

Cipher text: is the message after encrypted with key1

| | | | |
|---|---|---|---|
| 64 | DB | 79 | 37 |
| 5C | FA | BC | 99 |
| 8F | 69 | 83 | 9D |
| C1 | 1C | 3 | 5A |

Key2='ZDuha Jehan Mays'

| | | | |
|---|---|---|---|
| 5A | 61 | 68 | 4D |
| 44 | 20 | 61 | 61 |
| 75 | 4A | 6E | 79 |
| 68 | 65 | 20 | 73 |

Shift Row key2

| | | | |
|---|---|---|---|
| 68 | 65 | 20 | 73 |
| 75 | 4A | 6E | 79 |
| 44 | 20 | 61 | 61 |
| 5A | 61 | 68 | 4D |

Shift column key2

**Final State: XOR between the ciphertext and key2**

| | | | |
|---|---|---|---|
| 17 | FB | 1C | 5F |
| 25 | 94 | F6 | EC |
| EE | 8 | A3 | D9 |
| 8C | 74 | 62 | 0 |

# 6. CONCLUSION

In this paper the modification of AES have been proposed and investigated to encrypt the text. The Advanced Encryption Technique was implemented successfully using 'Matlab' language. The modifications brought about in the code was tested and proved to be accurately encrypting of the data messages with even higher security and immunity against the unauthorized users. Applying the idea of another key to encrypt the cipher text provides a better performance than standard AES. The suggestion method (AES-2Keys) to encrypt text provides more efficient for sending text because it is fast in both software and hardware. The advantage of the proposed coded system is the ability to use more than one key to make it more security without effect on time of transmission.

# 7. REFERENCES

[1] A. Thesis, "IMAGE STEGANOGRAPHY WITH FORWARD ERROR CORRECTING CODES STRATEGY of Nahrain University in Partial Fulfillment of the Requirements for the Degree of by," 2011.

[2] "IMPLEMENTATION OF HYBRID ENCRYPTION METHOD USING CAESAR ' CHAROMIE AlL TAT WI A thesis submitted in partially fulfillment of the requirements for the award of degree of Bachelor of Computer Science ( Computer Systems & Networking ) Faculty of Computer System & Software Engineering Universiti Malaysia Pahang ( UMP )," no. April, 2010.

[3] B. Vijay and J. Swathi, "Implementation of digital Steganography using image files-a Computational approach," vol. 10, no. 5, pp. 6–10, 2014.

[4] M. A. Alia, A. A. Tamimi, and O. N. A. Al-allaf, "Cryptography Based Authentication Methods," vol. I, pp. 22–24, 2014.

[5] C. Security, "Symmetric Key cryptosystem," pp. 1–19, 2004.

[6] C. Hall and N. Ferguson, "Chapter 7 The Advanced Encryption Standard ( AES )," no. November, pp. 58–73, 2001.