Kirkuk University Journal /Scientific Studies (KUJSS)
Volume 13, Issue 3, September 2018 , pp. (64-74)
ISSN: 1992-0849 (Print), 2616-6801 (Online)

# A Compartive Study Between (AES) and (DES) Algorithms Based on the (SET) Protocol

Khattab O. Khorsheed
Ministry of Education / General Directorate of Education in Kirkuk, Kirkuk, Iraq.
komer592@gmail.com

## Abstract

Secure Electronic Transaction protocol is a very large protocol in securing electronic bargains in business online for the sake of privacy. The Data Encryption Standard (DES) cons are that it is slow and short key (56 Bits). The typical attack for this one is the key exhaustion, because of the progress in the computer devices. The goal of this paper is to offer a new perspective so the protocol is more secure and fast, by using (AES) Advanced Encryption Standard (128 Bits for 10 Round , 192 Bits for 12 Round, 256 Bits for 14 Round). Besides, it has a comparison between Data Encryption Standard & Advanced Encryption Standard.

**Keywords:** Encryption; Decryption; Cryptography; Data Encryption Standard (DES); Advanced Encryption Standard (AES); Symmetric Encryption; Asymmetric Encryption.

Kirkuk University Journal /Scientific Studies (KUJSS)
Volume 13, Issue 3, September 2018 , pp. (64-74)
ISSN: 1992-0849 (Print), 2616-6801 (Online)

# دراسة مقارنة بين (AES) و(DES) بالأعتماد على بروتوكول (SET) خوارزميات

خطاب عمر خورشيد
وزارة التربية / مديرية العامة لتربية كركوك، كركوك، العراق.
komer592@gmail.com

## الملخص

بروتوكول عملية التحويل الالكتروني، هو بروتوكول ضخم لحماية و حفظ خصوصية العمليات التجارية على الأنترنيت. خلل معيار تشفير البيانات (DES) هو أنه بطئ و قصير (56 بت). الهجوم النمطي على هذا الكود هو استنفاذ المفتاح بسبب التطور الحاصل في صناعة الحواسيب. والهدف من هذا البحث هو طرح منظور جديد مما يجعل البروتوكول أكثر أماناً و أسرع، باستخدام معيار التشفير المتقدم (AES) (128 بت لـ 10 دورات ، 192 بت لـ 12 دورة 256 بت لـ 14 دورة). كما وأن البحث يطرح مقارنة بين معيار تشفير البيانات و معيار التشفير المتقدم.

**الكلمات الدالة:** التشفير، فك التشفير، الترميز، معيار تشفير البيانات، معيار التشفير المتقدم، التشفير المتماثل، التشفير الغير المتماثل.

Kirkuk University Journal /Scientific Studies (KUJSS)
Volume 13, Issue 3, September 2018 , pp. (64-74)
ISSN: 1992-0849 (Print), 2616-6801 (Online)

## 1. Introduction

Online purchase is an essential part in e-business. E-commerce is one of most famous using in e-business part. That's to say you are selling and buying, but not in person, rather through the internet. Thus, you would pay online. Due to that, there is Secure Electronic Transaction protocol [1],[2]. This protocol is about security throughout the e-transaction. Secure Electronic Transaction strong save protocol, which encrypts to enhance the transactions safety [3]. The online bargain begins this way, first the customer set wanted. Second merchant answers by an order form that contains many relevant details, and overall an authorized certificate for him to show eligibility. Third, and as a result, the customer sends a buying a message, that contains payment related information [4]. Finally, the merchant verifies the customer and his credit card details to be shown, while the rest are encoded for the safety of the client. In Fig. 1 shown Participants in the SET system. This paper is organized as follows. In section 2: Secure Electronic Transaction Protocol, section 3: Data Encryption standard**,** section 4: Advanced Encryption Standard**,** section 5: valid secure electronic transaction protocol, section 6: security enhancement in secure electronic transaction protocol, section 7: comparative analysis of existing and enhanced secure electronic transaction. Finally, section 8: is the conclusion.

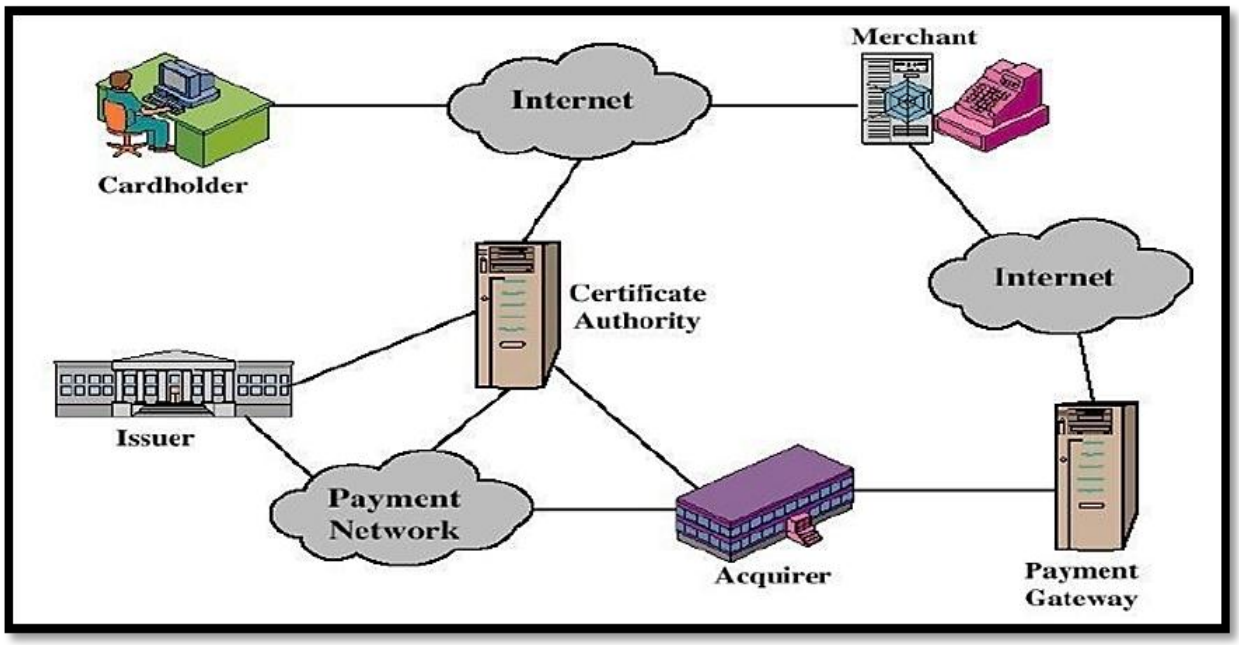



**Fig. 1:** Participants in the SET System.

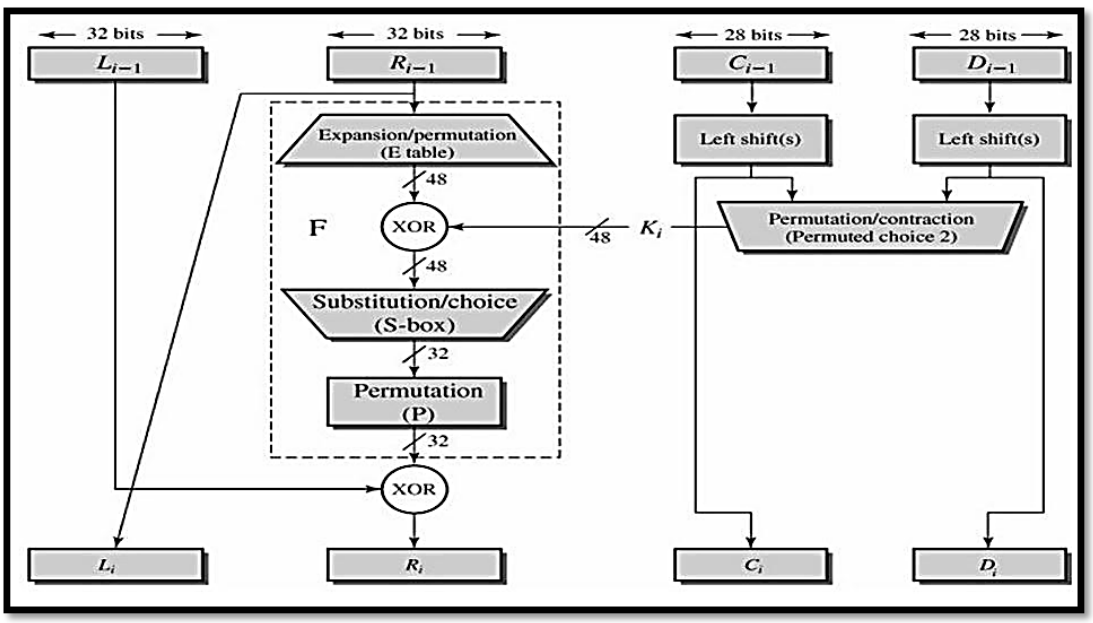
Kirkuk University Journal /Scientific Studies (KUJSS)
Volume 13, Issue 3, September 2018 , pp. (64-74)
ISSN: 1992-0849 (Print), 2616-6801 (Online)

## 2. Secure Electronic Transaction Protocol

SET is a very efficient security protocol, which uses encryption to supply secure information, guarantees payment safety, and authorize identity. In order to authenticate cardholders, merchants will be given digital certificates by certain institutions. It depends on encryption and digital certificate to confirm the security and authentication of the message, namely and commonly by the digital envelope. Using a randomly generated key, the message data is encoded by recipient's public key. This is known as digital envelope, where it is sent to the receiver's message encryption. The receiver uses a private key to decrypt the digital envelope, and it depends on reversing the original message by the symmetric key [5].

## 3. Data Encryption Standard

DES is actually the most used block cipher in the world. DES, it is a symmetric key algorithm for both sender and recipient secret key. There are many fields for DES; the most important of them is the banking industry. It is for this use that the DES was initially standardized, and ANSI ensures that it will be used in the next years and it will substitute DES with AES algorithms in the future. Although there is by whom over the design DES being used 56 bits key. DES is public standard; the design criteria used are categorized [6]. The block diagram of DES algorithm is shown in Fig. 2.




(a) Encryption/Decryption (b) Key Generation

**Fig. 1:** The Block Diagram of DES Algorithm.

Kirkuk University Journal /Scientific Studies (KUJSS)
Volume 13, Issue 3, September 2018 , pp. (64-74)
ISSN: 1992-0849 (Print), 2616-6801 (Online)

## 4. Advanced Encryption Standard

AES presents one of the most essential algorithm which uses one symmetric key in both the processes of encryption and decryption. Said key could be one of three options, 128 bits, 192 bits or 256 bits. According to the key length, the speed of the AES algorithm is fast and secret for encryption and decryption [7]. This makes it one of the most common standard symmetric 7key cryptographic algorithms employed. The Advanced Encryption Standard algorithm uses 128 bits for the original 16-byte text which are used to combine the 4x4 matrix. Overall, the algorithm depends mostly on the key length, an example of that is in the 10 rounds which takes a 128-bit key and the 12 rounds takes a 192 bit key and so on. Each round uses different key of 128-bit the 128-bit original key has probable keys of **2^128 = 3.4x 10^38** The 192-bit main key has probable keys **2^192 = 6.2x 10^57** probable keys and the 256 bit original key has probable keys **2^256 = 1.1x 10^77** probable keys. [8],[9].The block diagram of AES algorithm shown in Fig. 3.

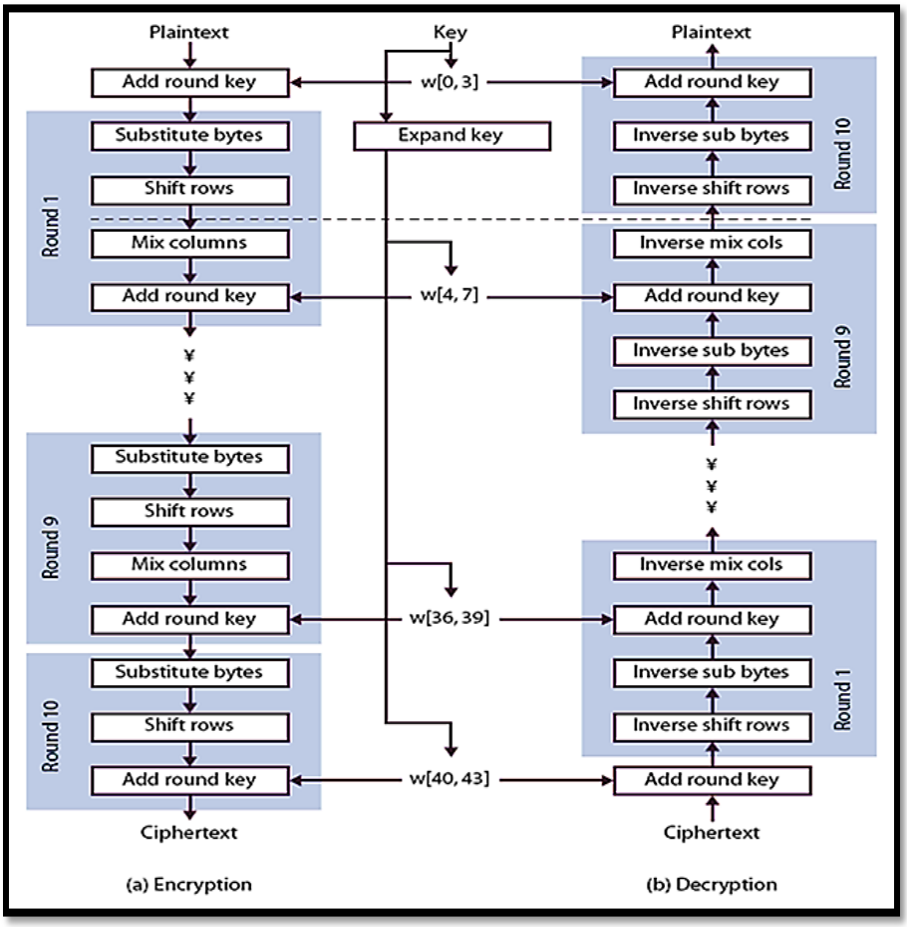



**Fig. 3:** Overall Structure of the AES Algorithm.

Kirkuk University Journal /Scientific Studies (KUJSS)
Volume 13, Issue 3, September 2018 , pp. (64-74)
ISSN: 1992-0849 (Print), 2616-6801 (Online)

## 5. The Four Steps in Each Round of Processing (AES)

### 5.1 Substitution (Sub Bytes):

In the substitution steps uses a 16x16 lookup table in order to replace bytes with other given ones in the input state array. The creation of the table's entries is done through the notion of multiplicative inverses in GF ($2^8$) and bit scrambling to destroy the bit-level correlations within each byte [7].

### 5.2 Shift Rows:

Every one of the four rows of the matrix is removed to the left. An entry that 'fall off' is re-inserted on the right side of row. The shifting is performed as the following list indicates:

- First row does not shift,
- Second row is shifted one (byte) position to the left,
- Third row is shifted two positions to the left,
- Fourth row is shifted three positions to the left,
- The result is a new matrix consisting of the same 16 bytes but shifted with respect to each other.

### 5.3 Mix Columns:

Every one of the said columns is treated as a polynomial over {\display style \ operator name {GF} (2^{8})} {\display style \operator name {GF} (2^{8})} and is then multiplied modulo {\display style z^{4}+1} {\display style z^{4}+1} with a fixed polynomial {\display style c(z)={03}_{16}\cdot z^{3}+z^{2}+z+{02}_{16}} {\display style c(z)={03}_{16}\cdot z^{3}+z^{2}+z+{02}_{16}}. The coefficients are shown in their hexadecimal correspondent of the binary demonstration of bit polynomials from {\display style \operator name {GF} (2)[x]} {\display style \operator name {GF} (2)[x]}. The Mix Columns stage can also be regarded as a multiplication as shown in particular MDS matrix in the finite field {\display style \operator name {GF} (2^{8})} {\display style \operator name {GF} (2^{8})}. This process is designated further in the article presented by Rijndael Mix Columns.

### 5.4 Add Round Key:

The 16 bytes of the matrix are currently measured as 128 bits and are XORed to the 128 bits of the round key. In the final round, then the output becomes the cipher text. Other than

Kirkuk University Journal /Scientific Studies (KUJSS)
Volume 13, Issue 3, September 2018 , pp. (64-74)
ISSN: 1992-0849 (Print), 2616-6801 (Online)

that, the 128 bits outcome is taken as 16 bytes and begin another round similar to the round before. The course of decryption of an AES cipher text is similar to the encryption process in the reverse order. Each round is comprised of the four processes that are taken in the reverse order:

- Add round key
- Mix columns
- Shift rows
- Byte substitution.

## 6. Steps Valid Secure Electronic Transaction Protocol

1. Order information (OI) and Payment Information (PI) are hashed by SHA-1 and their relevant message. And hashed again with SHA-1.
2. The new payment order message digest is encoded again with the private key of the client.
3. Dual Signature, orders data of the agent's license that has the agent public key. In Fig. 4 shown Construction Dual Signature.
4. Payment information message digest (PIMD) is enciphered with Advanced Encryption standard (AES) using 128bits.
5. The 128-bit key is sent to the merchant, enhancing the public key of the salesperson.
6. Eventually, the process is done the other way around to secure the client's confidentiality.

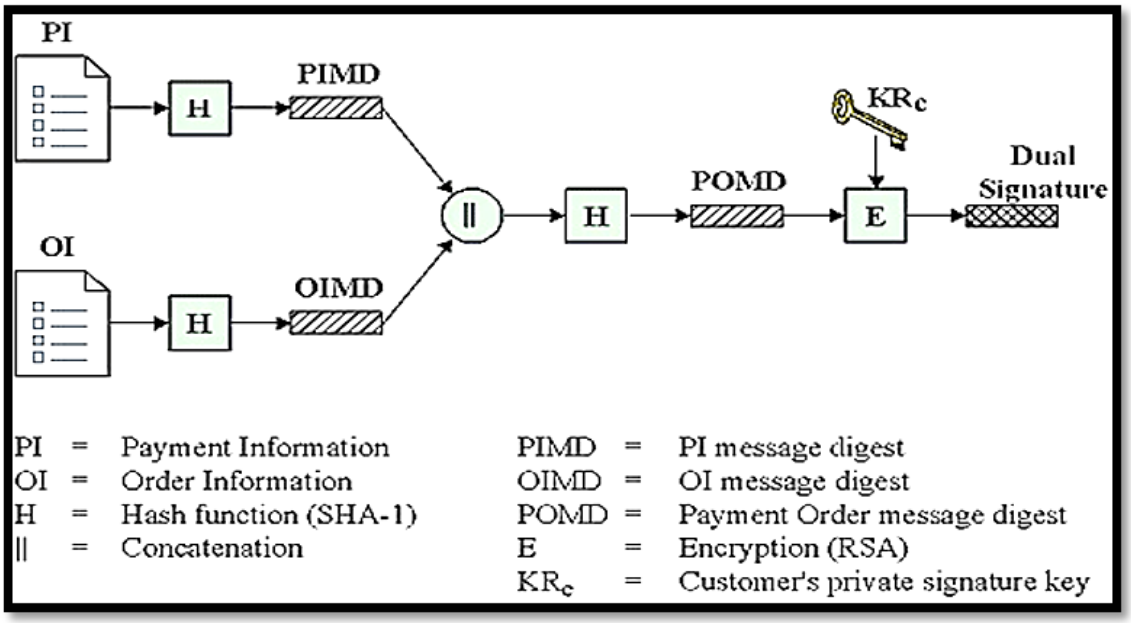



**Fig. 4:** Construction Dual Signature.

Kirkuk University Journal /Scientific Studies (KUJSS)
Volume 13, Issue 3, September 2018 , pp. (64-74)
ISSN: 1992-0849 (Print), 2616-6801 (Online)

## 7. Security Enhancement in SET Protocol

As for the SET currently used, it uses the bilateral key7 cryptography DES-56 to cipher biclique signatures, messages, fee massages, briefs as well as the agent's public key license. Due to the unreliability of DES-56-bit key space, it has been replaced with the AES-128-bit key size. Similarly, the SET protocol was shown to have more security and to be faster during the encoding/decoding processes. SET Protocol may consist of many interesting features such as:

- The model is rare as it possesses no digital proof of identity in the registration protocols. It rather permits itself through filing a registration form which the format is not specified. The authentication process takes place outside the protocol, when the cardholder's bank inspects the completed form.
- The dual signature is a new construction where the partial sharing of information among three peers leads to unusual protocol goals.
- SET makes use of many kinds of digital envelopes. A digital envelope contains two parts: the first of which is encrypted using a public key, contains a fresh symmetric key K and identifying information; the other, encrypted using K, transfers the full message text. Digital envelopes manage to keep the public-key encryption lowest; however, the many symmetric keys complicate the reasoning. Most verified protocols distribute just one or two secrets.

## 8. Comparative Analysis of Existing and Enhanced SET

An effective bilateral key cipher algorithm like AES, whose essential security target to defend opposing to cryptanalytic attack, is key exhaustion. The key exhaustion decides the potentiality of the symmetric key algorithm. It is on average to have n-bit key. And it is vital to attempt (2n-1) keys, however, if n was large enough, it will be significantly not virtual. To decrypt the 56-bit DES, using key exhaustion is possible. Whereas, it is not valid to do the same with AES that uses 128,192, 256 bit key. The implementation of AES helps dramatically to speed up encryption and decryption processes. All byte values in the AES algorithm will be presented as the concatenation of its individual bit values (0 or 1) between braces in the order {b7, b6, b5, b4, b3, b2, b1, b0}. These bytes are interpreted as finite field elements using a polynomial representation:

Kirkuk University Journal /Scientific Studies (KUJSS)
Volume 13, Issue 3, September 2018 , pp. (64-74)
ISSN: 1992-0849 (Print), 2616-6801 (Online)

$$b_7x^7 + b_6x^6 + b_5x^5 + b_4x^4 + b_3x^3 + b_2x^2 + b_1x + b_0 = \sum_{1=0}^{7} b_i\ x^i \quad 8.1$$

Uses arithmetic in the finite field GF ($2^8$) with irreducible polynomial:

$$m(x) = x^8 + x^4 + x^3 + x + 1 \quad 8.2$$

In Table 1 shows the compare between DES-56 Bits & AES-128 Bits processing time in min.

**Table 1:** Compare between DES-56 Bits & AES-128 Bits Processing Time in Min.

| Size of file | DES-56 Bits | | AES-128 Bits | |
|---|---|---|---|---|
| | Encryption | Decryption | Encryption | Decryption |
| 5 KB | 0.022396 min | 0.00234375 min | 00.13802 min | 0.00206042 min |
| 15 KB | 0.063017 min | 0.013802 min | 0.052083 min | 0.00755208 min |
| 20 KB | 0.069531 min | 0.01849 min | 0.061198 min | 0.017969 min |
| 25 KB | 0.071234min | 0.025343 min | 0.064118min | 0.02121 min |
| 50 KB | 0.245677 min | 0.165788 min | 0.145685 min | 0.118769 min |

## 9. Conclusion

The Secure Electronic Transaction (SET) is a very vital procedure which is why it needs a strong defensive system is required. Thus the AES was designed after the development of the DES. AES uses (128 bits for 10 round, 192 bits for 12 round and 256 bits for 14 round); however, DES uses a 56-bit key. The confidentiality and authentication are more guaranteed with AES than it was with DES, additionally, the pace of encryption and decryption. Selected as AES finalist it has the following attributes:

1. 128-bit block size.
2. 128, 192, or 256 bit key size.
3. An iterative rather than a Feistal cipher (like IDEA).
4. Treats data as 4 groups of 4 bytes
5. Has 9, 11, or 13 rounds, where each round consists of:
   - A byte substitution step (1 S-box used on every byte)
   - A shift rows step (shuffle the bytes between groups)
   - A mix columns step (matrix multiplication of groups with each other) An add round key step

**6.** All operations can be combined into x or and table lookups – hence implementation can be very fast and efficient Resistance against all known attacks and code compactness on a wide range of platforms design simplicity from DES it is possible to say that AES algorithm is strong and will remain for several decades.

## References:

**[1]** R. Hunt, "**PKI and Digital Certification Infrastructure**", 9th International Conference on Networks, Thailand, IEEE, 1531(2001).

**[2]** Lawrence C. Paulson,"**Verifying the SET protocol: Overview**", International Journal of Advanced Manufacturing Technology, 25(5) ,4 (2003).

**[3]** Douglas H. Steves, Chris E. Yurkanan and M. Gouda, "**Properties of Secure Transaction Protocols",** Computer Networks and ISDN Systems, 29(4), 1809 (1997).

**[4]** D. Eastlake and P. Jones, **"US secure hash algorithm 1 (SHA1)"**, 3rd Edition , RFC – Informational, USA (2001).

**[5]** G.Agnew **"Secure Electronic Transaction (SET protocol)"**, International Journal of Computer Vision-Springer, 11(2), 334 (2003).

**[6]** A.Nadeem, and M.Y.Javed,"**A performance comparison of data encryption algorithms",** 1st International Conference on Information and Communication Technologies, Pakistan, IEEE, 84 (2005).

**[7]** Soumya, K Ramesha and Guruprasad, **"A Survey on Cryptography Algorithms for Network Communication"**, International Journal of Engineering Science and Computing, 6(5), 6188 (2016).

**[8]** Mao Y. Wang, Chih P. Su, Chia L. Horng**, "Single- and Multi-Core Configurable AES Architectures for Flexible Security"**, IEEE Transactions on Very Large-Scale Integration (VLSI) Systems, 18(4) , 541(2010).

Kirkuk University Journal /Scientific Studies (KUJSS)
Volume 13, Issue 3, September 2018 , pp. (64-74)
ISSN: 1992-0849 (Print), 2616-6801 (Online)

**[9]** W. Stallings, "**The advanced encryption standard",** Cryptologia, 26(3), 165(2002).