Overview and Performance Analysis of Encryption Algorithms

Zahraa Ch. Oleiwi 1, Wasan A. Alawsi 1, Wisam. Ch. Alisawi 3, Ali S. Alfoudi 4, Liwa H. Alfarhani 5
1 College of Science, University of Al-Qadisiyah. Iraq
2 College of Science, University of Al-Qadisiyah. Iraq
3 College of Science, University of Al-Qadisiyah. Iraq
4 College of Computer Science and Information Technology, University of Al-Qadisiyah.
5 Academy Engineering, RUDN University, Russia.
zahraa.chaffat@qu.edu.iq

Abstract:
Data protection is a complex problem affecting many areas including computers and communications. To ensure the necessary protection of applications, cryptographic methods and various algorithms are used. In this paper general overview of cryptography, information security and the comparison of algorithms with symmetric and asymmetric keys is presented. Factors ensuring the achievement of efficiency, flexibility and security are the basis of this research. As a result, the best solution for symmetric and asymmetric encryption is produced.

Keywords: encryption; AES; Security model; DES; symmetric encryption; RSA; cryptography; asymmetric encryption.

1. Introduction
Cryptography is the coding science and coding of secure communication and is one of the most important process in the modern digital currencies industry. The encryption techniques used today are the result of a very long history of development[1]. Since ancient times, people have used encryption to transfer information securely. Cryptography began with the advent of writing art. With the civilizations development and the human organization beings into groups of countries, kingdoms, clans, etc., which led to the competition emergence among these groups for food, energy, drinking, and others, it became necessary to have a method and method in which each group would communicate safely and secretly away from the other group [2-5].
The cryptanalysis, the science by which the codes are decoded and resolved, has begun to catch up with the primitive sciences which are still relatively primitive in ciphering. Kennedy, a well-known mathematician of Arab advanced a technique known as frequency analysis around 800 AD that made the replacement code defenseless to decoding. For the first time, people trying to decode encrypted messages managed to come up with a systematic way to do so which made it necessary for encryption to go further so that it would still be useful[6].
There are a number of works devoted to the analysis of various methods and algorithms of encryption [7-16]. Let us briefly review cryptographic algorithms and classification of
encryption algorithm types and parameters that are verified for algorithms and protection problems.

2. Evolution of Cryptography

Historians conflict on the major source of encryption and its emergence. Some of them refer it to civilization of Phoenician, another to Roman civilization, and another to civilization of ancient Egyptian, but what does not differ is that all of these civilizations had special methods that they used to safety communicate by encrypting the messages[7].

It is known that primitive coding techniques existed in ancient times and it appears that most early civilizations used coding to some extent such as symbol substitution, which is the primary form of coding in both ancient Egyptian writings and Mesopotamia. The earliest known example of this type of encryption is found in the tomb of the Egyptian noble named second Khnumthab who lived about 3,900 years ago[17].

In later periods of antiquity, cryptography was widely used to protect important military information, a purpose that still serves to this day. In the city of Sparta, in the state of Greece, the messages were encrypted by writing them on parchment on a cylinder of a certain size, which makes the message unable to be divided until it is enveloped around a similar cylinder by the recipient. As well, spies in old India are known to have used coded messages as early as the 2nd century BC [17].

Hieroglyphics is the oldest coding technique, as it was used 4000 years ago and was used by ancient Egyptians to communicate by writing using this method. The written symbols in this technique were known only by copyist who sent telegrams and letters on behalf of the kings [17].

In the period between 500 BC and 600 BC some development occurred on coding techniques by using a primitive and simple technique by substituting letters with other letters and this command was used by the Romanians and was called Caesar Shift Cipher.

Cryptography and its technologies have spread widely in the Renaissance of the European continent, where many methods and research have emerged to analyze cryptographic techniques to decode the encrypted data. In the fifteenth century A.D. a new coding technology called Vigenere coding appeared[17].

The true development of cryptography at the end of the nineteenth century and in the twentieth century, after the invention of special machines for this matter, such as Enigma, which helped advance and increase the efficiency of cryptography.

Cryptography has continued to progress gradually over the centuries. In the 1870s Thomas Jefferson described a major coding event although it was probably never built. His innovation known as the cipher wheel consisted of 36 letters of messages on moving wheels that could be used to achieve complex coding. This concept was largely progressed as it served as the standard for coding of American military until late in Second World War.

700 BC, the army of the Spartans of Scital used to send sensitive official messages in times of battles and wars, and both the sender and recipient of the message had a wooden rod of exactly the same diameter and length, and the message was encrypted by tightening a manuscript or piece of leather tightly around the wooden stick. And by writing the message to it, then the manuscript or leather is sent on its own to the recipient who can only read the content of the message after wrapping it on his piece of wood. Anyone else trying to read it will see scattered, meaningless letters[17].
1467, Leon Battista Alberti invented and published the first multi-alphabet, completely changing the course of cryptography throughout history. The Alberti cipher consists of two metal disks on the same axis, one within the other and relied on mixing the alphabet from the two disks By the possibility of rotating them[17][18].

1797, Thomas Jefferson invented this 26-piece wooden cylindrical wheel(known as Jefferson Wheel) mounted on an iron spindle, the letters of the alphabet are engraved randomly on the edge of each wheel, and by spinning these wheels the words can be produced, the recipient By spelling the coded message on his Jefferson cupboard, and then searching on the line that gives meaningful speech, the US military reused this encoder between 1923 and 1942[17][18].

In 1943, The Enigma consists of a series of rotating electromechanical encoders linked together, the machine was designed by a German engineer and used by the Nazi army, and was considered an impenetrable encoder, the British Bletchley Park facility - which was during Second World War responsible for decoding operations - to develop the work of a group of Polish crypto experts with the aim of breaking the code of the enigma machine, and the machine remained insensitive to penetration until the scientist Alan Turing, who was working at Bleachley Corporation, took advantage of the only vulnerability in the Ain However, it is not possible to encode each letter on its own, using this information in addition to the Bombe Machine, which reduced the time needed to penetrate the enigma, the Allies soon knew all the movements of the Nazi forces[17][18].

The proliferation of computers and communication systems in the 1960s brought a demand from the private sector for means to digitally protect information and provide security services. As computers spread, coding became much more advanced than in the analog era. 128-bit mathematical encryption is much more powerful than any ancient or medieval encoding and is now standard for many computer systems and sensitive devices.

In 1961, The first computer password was developed by the MIT Center for Computing Sciences using the Compitable Time-Sharing System at a time when the use of computers was rare and limited. On the research facility, CTSS first used the password and username as a verification method[17][18].

In 1970s, IBM created a team called the Crypto Group, which in turn worked on designing a cipher suite to protect corporate customer data. In 1973, the United States of America adopted the encryption algorithm to become a data encryption standard. The standard remained in effect for about 20 years until it was compromised in 1998 by the Electronic Freedom Foundation within 56 hours, and that period was reduced to 22 hours in the following year[17][18].

The most surprising development in cryptography history was in 1976 when Diffie and Hellman published new cryptographic trends. This paper presented the revolutionary concept of public key cryptography as well as presented a new and creative way.

In 1978, Rivest, Shamir, and Adleman discovered the first public key cryptography and signature system, now referred to as RSA. Another difficult mathematical problem in the RSA chart is the difficulty of analyzing large correct meters. This app has a tough mathematical problem for revitalizing blades efforts to find more effective ways for a factor[17][18].

The 1980s saw great developments in this area, but nothing made RSA unsafe. Another class of robust and practical public key charts was found by ElGamal in 1985. These are also
based on a separate logarithm problem. The digital signature is one of the most important contributions made by public key cryptography[17][18].

Beginning in 1990 computer scientists were developing a completely new form of coding, called quantum coding, and it hoped to raise the level of protection that modern coding provided once again. To process information in the United States to encode unclassified information, DES, the standard data encryption, is the most known encryption mechanism in history. It remains the standard way to secure e-commerce for many financial institutions around the world[17][18].

In 1994, the United States government adopted the ElGamal public key scheme based the Digital Signature Standard[17][18].

1997, AES Development: The Advanced Encryption Standard was developed by The National Institute of Standards and Technology and is still in use today. 128-bit encryption requires $2^{55}$ years to decode if a device capable of performing the necessary operations for that[17][18].

2012, Personal Data Locks: Personal Data Lockers has emerged as a way to use most of the capabilities of the Internet while maintaining security, the data is protected in the best possible way by working on centralization of storage, i.e. storing personal data such as money transfer statements, passwords, and ID numbers in one encrypted location that only the user can access, by keeping this data confidential under the user’s control, governments cannot decrypt it, not even the promoters of this technology themselves. In other words, personal data can only go where the user wants.

Recently, cryptographic techniques have also been used to make the creation of digital currencies possible. Cryptocurrencies benefit from advanced cryptographic technologies including hashtags, public key cryptography, and digital signatures. These technologies are used primarily to ensure the security of data stored on the blockchain and to validate transactions. A specialized form of encryption known as the Elliptical Curve Digital Signature algorithm (ECDSA) supports Bitcoin and other encryption systems as a way to provide additional security and ensure that funds can only be used by their rightful owners[19].

3. Information Security

It is the protection afforded to the automated information system in order to achieve the practical goals of maintaining the confidentiality, integrity, safety and availability of information system resources (including software, hardware, information / data firmware, and telecommunications)[6].

Science that is concerned with achieving the basic requirements of the security system (confidentiality, integrity, reliability, and availability of resources) is called cryptography, and cryptography is defined as:

It is a science that is interested in studying mathematical techniques related to the basic aspects of information security, and in particular, this science uses methods and algorithms to encode information, i.e. coding it and transforming it into an incomprehensible form that no person is not authorized to read. These methods or algorithms are called encryption algorithm[2].

4. Information Security Model

The term of information security refers to a technique used to achieve security requirements. The basic model of the information security system consists of the following basic components, as shown in Figure (1)[5]:


1- party (entity): A person or device that sends, receives or deals with information
• The sender: The party who wishes to send the message and is the entity that is considered the legal or licensed sender and authorized to send information.
Receiver: The entity intended to receive the transmitted information.
Adversary: It is a third party that tries to steal information, break the information security service, and penetrate the security system between the sender and the receiver. , Eavesdropper, intruder, and interloper.
2- Channels (channels \ transmission media): means (media) to transfer information from one entity to another through which data is transferred. The transmission channels can be classified according to their information security to:
• physically secure channel: It is the channel that the opponent cannot physically reach, such as trusted companies, personal contact between continuous parties and dedicated communication links….etc.
• An unsecured channel: It is the channel through which it is possible to rearrange, delete, insert or read information by parties other than the real sender (the opponent as mentioned previously).
• A secured channel: The channel through which the opponent cannot re-arrange, delete, enter or read the information. It differs from the physically secure channel in that it is secured by coding techniques.

![Fig.1. Model of Information Security](image_url)
Based on the foregoing, it becomes clear that the definition of information security is not limited to encryption and decryption and observance of privacy only, but it is much broader as it aims to achieve the following information security requirements[6]:

1- Confidentiality: it means keeping information content from everyone except those who are authorized to obtain it. There are many ways to provide confidentiality, ranging from physical protection to mathematical algorithms that make data incomprehensible. The concept of confidentiality covers the first two terms related to the term confidentiality of data, meaning that private or confidential information is not provided or disclosed to unauthorized individuals. The second is related to the term privacy, which refers to freedom from interference or infiltration. Privacy of information is the right to have some control over how your personal information is collected and used.

2- Data integrity: It is intended to address the unauthorized change of data with the aim of ensuring data integrity, i.e. full data access without deletion, addition or replacement. The concept of integration also refers to the integrity of the system, which confirms that the system performs its intended function in an impeccable manner, and free from unintended or unintended manipulation of the system.

3- Availability: confirms that the systems are operating quickly and that the service is not rejected for authorized users. In other words, ensuring timely access to and use of information, as loss of availability is the disruption of access to or use of information or the information system.

5. Security Architecture

Security Architecture is known as a framework that produces a systematic technique to define security requirements and to describe methods that satisfy those requirements. It defines attacks, security mechanisms and services, and the relationships between these categories[6].

5.1 Security Mechanism

It is any process (or device that contributes to this process) designed to detect or prevent any security attack or recover from it. These mechanisms are encryption algorithms, signatures and authentication protocols, which we will look at in other chapters in detail.

5.2 Encryption Algorithms

Encryption is the process of coding a message so that it is incomprehensible or interpretable, and there are three terms for coding[8]:

1- Encoding means the coding of entire words or phrases and their conversion into other phrases and words.
2- **Enciphering** means the translation of letters or symbols individually.

3- **Encryption** is the broadest term covering the terms Encoding and Enciphering.

And with coding, there must be a decryption process that performs the opposite process of coding as it converts encrypted words into understandable words that the authorized recipient of the message can understand and read.

The explicit message, which is still on the sender’s side, is called the original or explicit message, plaintext, and after encoding it with the encryption process, it is called ciphertext and it is sent via the transmission channel to the recipient as in the equations (1) and (2).

\[
C = E(P) \text{ ..........(1)}
\]
\[
P = D(C) \text{ ..........(2)}
\]

Where, \( P \) is the explicit text, plaintext, and \( C \) is the ciphertext, \( E \) stands for encryption, and \( D \) stands for decryption.

Based on the foregoing, the term cryptography is defined as the process of using cryptography to hide real text.

The encryption algorithm requires the key. If the attacker knows the algorithm or the encrypted text, the encrypted messages will remain secret and unknown because the attacker does not know the value of the key.

The encryption key is denoted by \( K_E \), and the decryption key is denoted by \( K_D \), thus, the cipher equations (3) and(4) is as follows:

\[
C = E(K_E, P) \text{ ..........(3)}
\]

And the decipher equation is:

\[
P = D(K_D, C) \text{ ..........(4)}
\]

6. **Security Attack**

It is any process that threatens the information security of the institution. The person making the attempt is called the opponent and there are two types of it[2][6]:

A passive adversary is an opponent who is able to read information from an insecure channel as well as analyze traffic.

An active adversary is the opponent who transfers, changes or deletes information on an unsafe channel.

Among the opponent's actions is cryptanalysis, where he is defined as studying mathematical techniques trying to break cryptographic techniques and more generally information security services. The person involved in code analysis is called cryptanalyst. The science that is concerned with the study of cryptography and cryptanalysis is called cryptology.

To try to analyze cipher, the cipher analyzer performs any of the following attempts:

- Try to break one message.
- Trying to recognize patterns in encrypted messages in order to be able to break codes by applying decryption algorithms.
- Trying to find general weaknesses in cryptographic algorithms without the necessity of intercepting any message.

Figure (3) shows the most elements of network security model.
Cryptanalytic attacks are classified as in below table(1):

**TABLE 1: Types of Cryptanalytic Attack**

| Type of Cryptanalytic Attack | Information Known to Attacker |
|------------------------------|-------------------------------|
| Cipher text only             | • Cipher algorithm            |
|                              | • part of the encrypted text  |
| Known-plaintext              | • Cipher algorithm            |
|                              | • Encrypted text              |
|                              | • Samples of each plaintext and encrypted text |
| Chosen-plaintext             | • Cipher algorithm            |
|                              | • Encrypted text              |
|                              | • Pair of plaintext and its cipher text chosen by attacker |
| Chosen-ciphertext            | • Cipher algorithm            |
|                              | • Encrypted text              |
|                              | • Pair of chosen ciphertext and its encrypted plaintext |
| Chosen text                  | • Cipher algorithm            |
|                              | • Encrypted text              |
|                              | • Pair of plaintext and its ciphertext chosen by attacker |
|                              | • Pair of chosen ciphertext and its encrypted plaintext |
| brute-force attack (passive attack) | • Tries all the possible keys |
| dictionary attack            | • Tries dictionary of the most common words |
| man in middle attack (active attack) | • Tries to exchange the keys between |

![Fig.3. Network Security Model](image-url)
two parities of connection channel in security system

| timing attack | • Analyzes the time spent on implementing cryptographic algorithms |

7. **Classification of Cipher Algorithms**

Cryptographic algorithms are classified according to several considerations[6]:

1. **Number of keys**
   - According to the value of the used key, the cipher algorithms are divided into:
     - **Symmetric cipher algorithms**: in this algorithm, there is one key used for encryption and decryption process so,
       
       \[ K_E = K_D \]

     - **Asymmetric cipher algorithms**: in this algorithm, there are two keys, one of them used for encryption and called public key, and the other used for decryption.
       
       \[ K_E \neq K_D \]

2. **Process of data**
   - Cipher algorithms are divided according to how they process the data into:
     - **Block encryption algorithms**: In this algorithm, the entire block of plain text is processed resulting in an encoded block of equal length.
     - **Stream encryption algorithms**: In this algorithm, the plain text is processed bit or byte by byte as streaming form.

   Figure(6) shows flowchart of all the types of cipher algorithms divided as in considerations above.
8. Symmetric Ciphers Algorithms

As we knew in the previous chapter that cipher algorithms are mathematical processes and techniques aimed to coding data and converting it to an incomprehensible form and it is one of the aspects of information security architecture that contributes to achieving information security requirements and information security system services[14].

An input to the encryption algorithm is the text to be encrypted and the key. The key is one of the most important inputs to the encryption algorithm, and it is a value independent of the plain text and the algorithm, as each algorithm produces a different output each time depending on the specific key value used at that time[14][15].

Symmetric cipher algorithms, known as traditional or single-key encryption, it is used the same key to both cipher and decipher process. Symmetric cipher algorithms is the encryption used before Asymmetric (public-key) was developed in the 1970s. It remains by far the most widely used type of encoder[8][11].

The strength of the encryption algorithm that is identical to its resistance to the attack depends on the strength and confidentiality of the key and its transmission through secure channels, so there is no need for the confidentiality of the encryption algorithm. Where the encryption system is computationally secure whenever the time and cost of code breaking exceed the time and cost used for encryption[6].

Symmetric algorithms can be distinguished according to the type of reversible operations used to convert plain text to cipher text into: Substitution where each element in plain text is set in another
element, and transposition where the elements are rearranged in the unusual text, without loss of information. Efficiency factors are evaluation for the following algorithms[6][15]: The Data Encryption Standard (DES) is a symmetric-key block cipher meaning it processed plaintext as blocks, each block with 64-bits to return ciphertext block with same size(64-bit). Each block has been divided into two 32-bits blocks (left block of 32-bits and right block of 32-bits). The encryption process is made of two permutations (P-boxes) and sixteen Feistel round. There are initial and final permutation process of rearranges the bits in each block of plaintext according to lookup tables. The function used in DES which consider the heard of DES implements key of 48-bit size on right most block of 32-bit size. Where the function contain expansion (P-box), XOR operation and confusion using S-boxes. P-boxes and S-boxes are defined according bit-selection table. Key generation in DES for each round of 16 round implies permutation, shift operation and compression operations in order to produced key of 48-bits[6][15].

The Advanced Encryption Standard (AES) is a symmetric-key block cipher algorithm. It is non Feistel cipher. The size of encrypted and decrypted block is 128-bits. It uses 10, 12, 14 round with key of 128, 192, 256-bits respectively. Size of key depend on number of rounds but the size of each round keys are 128 bits always[6].

| No. of round | Size of keys |
|--------------|--------------|
| 12           | 128          |
| 14           | 192          |
| 16           | 256          |

TABLE 2: Round vs size of key in AES algorithm

AES implement encryption process using four types of transformations: substitution, permutation, mixing, and key-adding. Substitution transformation includes two invertible transformations: sub-byte involves 16 independent byte to byte transformations using sub-byte transformation table. Permutation involves shift process denotes by shiftRows. The next transformation that change bits inside the byte to provide diffusion level is called MixColumns. mixColumns implement mathematical operation in GF(2^8). The last function of encryption process of AES is key adding that includes adding key word with each state column matrix where the operation in this process is matrix addition[6][15].

9. Asymmetric Ciphers Algorithms

Encryption with an asymmetric key represents a method in which the key used for encryption are differed from the key used for decryption processes. One of the keys is published denoted by public key and the second one called private key. This system is also called a cryptographic system with a public key. When the key of the encryption is published firstly, the system allows the user of the public key to openly transmit the message [7, 11]. If the decryption key is published, the system verifies the signature of documents, blocked by the part own the private key. Public key methods are important because they can be used to securely transfer encryption keys or other data, even if both users do not have the ability to negotiate a private key in a private algorithm. The keys used in public key cryptography algorithms are usually much longer, which increases the security of transmitted data. Two well-known asymmetric (public key) encryption methods have been discussed below:
RSA best known & widely used public-key encryption algorithm produced by Rivest, Shamir & Adleman of MIT in 1977. RSA algorithm based on a finite (Galois) field exponentiation over integers modulo a prime and uses large integers of 1024 bits where security of RSA due to cost of factoring large numbers[10].

Algorithm 1 RSA key generation

//input: p,q  
//output: public encryption key: PU={e,n}  
//secret private decryption key: PR={d,n}  
{
Randomly select two large primes: p, q
computing n=p.q where ø(n)=(p-1)(q-1)
Randomly select the encryption key e where 1<e<ø(n), gcd(e,ø(n))=1
solve following equation to find decryption key d
where e.d=1 mod ø(n) and 0≤d≤n
}

Algorithm 2 RSA encryption algorithm

// Notation Description:
// M: original message
//C: encryption message
//PU: public key
{
the sender encrypts M with public key of recipient
PU={e,n}
calculates: C = M^e mod n, where 0≤M<n
}

Another most common public-key encryption algorithm is ElGamal related to Diffie-Hellman (D-H) key exchange. ElGamal uses exponentiation in finite Galois field[10]. Below scheme explain the ElGemal in details:

10. Performance Analysis Measurement Factors
In this work the following factors are used as encryption efficiency criteria[16][20]:
1- Security robustness: this factor related to the achievement of the encryption protected from brute force, timing attack and various plaintext cryptanalysts.
2- Length and type of used key: is an factor that related to security of method and determined the type of encryption method.
3- Algorithm structure: if the algorithm has a Feistel structure where the permutation and substitution operation implement on half block in each round.
4- Implementation time and algorithm speed: this factor determined the time required to implement all operations of algorithms and related to algorithm complexity and speed of processor.
5- Complexity and cost: this factor related to type of process and size of memory used to implement encryption algorithm.
6- Avalanche effect: is the property of algorithm such that a small change in either the plain text or the key produced significant change in the ciphertext.

11. Performance analysis and comparative study
Let's consider comparison results for efficiency estimations of symmetric and asymmetric encryption algorithms by various parameters – factors for a choice of security product. The time factor is measured as high, low. Speed is defined in such terms as fast, slow and moderate. We define algorithm structure in “Feistel” and “non Feistel”. The key length is measured in terms of the used bits. Avalanche is measured as strong, power consumption (used memory) is defined as high and low. The results of the analysis are shown in the following table (3):

**TABLE 3: Measurement factors or Symmetric and Asymmetric**

| Factor                          | Asymmetric encryption | Symmetric encryption |
|--------------------------------|-----------------------|----------------------|
|                                | ElGamal               | AES                  | DES                  | 3DES                  |
| Security robustness against attack | vulnerable Man-in-the-middle attack | Brute force, statistical attack, differential and linear attack | Brute force, vulnerable to linear attack | Brute force, Man-in-the-middle attack |
| Length of key                  | Large prime number> 1024 bits | Large prime number> 1024 bits | 128, 192 or 256 bits | 64 bits | 129 bits |
| Type of key                    | Different keys according to DH exchange | public key and private key one for encryption and one for decryption | one private key for encryption and decryption | one private key for encryption and decryption | one private key for cipher and decipher |
| Structure of Algorithm         | Non Feistel No rounds | Non Feistel No rounds | Non Feistel 10,12,14 rounds | Feistel 16 rounds | Feistel 16 rounds |
| Algorithm speed                | High                  | High                 | High                 | High                 | High                 |
| Memory consumption             | Less than RSA         | High                 | less than DES        | Higher than AES      | Higher than DES      |
| Avalanche effect               | less than that for AES | less than that for AES | Strong than that for DES | Strong, less than that for | Strong, less than that for AES |
It is clear from above table that the AES is more secure than DES according to the large size of key and complexity of encryption operation in each round as well as the complexity of key generation. Also number of rounds increase the security of encryption algorithm. As memory consumption reduced the speed of implement the algorithm increase, so AES consider best solution among symmetric encryption algorithm since it characterized by simplicity where it can be easily implemented using cheap processors and minimum amount of memory. Among asymmetric encryption algorithms, the RSA algorithm provides greater security, because it uses factorization of a large prime number to generate keys. Therefore, the RSA algorithm is found to be the best solution among asymmetric encryption algorithms.

12. Conclusion

This paper investigates the performance of security product according to most effective, flexibility, security factors as comparative and analysis study between symmetric and asymmetric encryption algorithms. As a result, the AES algorithm is indicated as the best solution among symmetric key encryption algorithms. Among symmetric encryption algorithms, the RSA algorithm provides greater security.

REFERENCES

1. Wisam. Ch. et.al.(2019), " Improvement of Classical Cipher Algorithm based on a New Model of Timed-Released Encryption ", International Journal of Applied Engineering Research, Vol. (14), No. (16), pp. (3531-3536).
2. Shangin V.(2014), " Information security and data protection", DMK Press
3. Vasilenko O.N.(2006), Theoretical-numerical algorithms in cryptography, Moscow Center for Continuous Mathematical Education.
4. Chandler J.(1999), "Introduction to cryptography", BYTE-Russia, Vol.(12), No.(12), pp.(18-31).
5. Biryukova O.V.(2015), Information Security, Ryazan.
6. William S.(2011), Cryptography And Network Security Principles And Practice.
7. Biryukova O.V.(2015), Information Security, Ryazan.
8. Shemet V.S.(2016), "Overview of encryption methods ", Symbol of Science.
9. Kumar S. et al.(2016), " A Survey on Various Asymmetric Algorithms ", International Research 7. Journal of Advanced Engineering and Science, Vol. (1), No.( 4), pp. (117-119).
10. Shetty A. et al.(2014), "A Review on Asymmetric Cryptography – RSA and ElGamal Algorithm", *International Journal of Innovative Research in Computer and Communication Engineering*, Vol.(2), Special Issue 5, pp. (98-105).

11. Tripathi R., Sanjay A.(2014),"Comparative Study of Symmetric and Asymmetric Cryptography Techniques :Comparative Study of Symmetric and Asymmetric Cryptography Techniques", *International Journal of Advance Foundation and Research in Computer*, Vol.(1), No. (6), pp. (68-76).

12. Mittal M.(2012), "Performance Evaluation of Cryptographic Algorithms", *International Journal of Computer Applications*, Vol. (41), No.(7), pp. (1-6).

13. Kumar Y. et al.(2011)," Comparison of Symmetric and Asymmetric Cryptography with Existing Vulnerabilities and Countermeasures", *International Journal of Computer Science and Management Studies*, Vol.(11), No.( 03), pp. (60-63).

14. Thambiraja E. et al(2012), " A Survey on Various Most Common Encryption Techniques", *International Journal of Advanced Research in Computer Science and Software Engineering*, Vol.(2), No.( 7), pp.( 226-233).

15. Alanazi H. et al.(2010), " New Comparative Study Between DES, 3DES and AES within Nine Factors ", *Journal of Computer*, Vol.(2), No.( 3), pp.(152-157).

16. Marwaha M. et al.(2013)," Comparative Analysis of Cryptographic Algorithms" *International Journal of Advanced Engineering Technology*, pp. (16-18).

17. Tony M. D.(2009)," A Brief History of Cryptography", *Inquiries Journal*, Vol. (1), No. (11).

18. John F. Dooley (2018), *History of Cryptography and Cryptanalysis, Springer.*

19. W. Ch. Alisawi, Alaa A. Hussain, Wasan A. Alawi (2018), "Estimate new model of system management for database security", *Indonesian Journal of Electrical Engineering and Computer Science*,Vol.(14), No.(3), pp.(1391-1394).

20. Priyadarshini P.(2016)." A Comprehensive Evaluation of Cryptographic Algorithms: DES, 3DES, AES, RSA and Blowfish", *ELSEVIER*, pp.( 617 – 624).

21. Study The Current Density-Voltage (J-V) Characteristics of α-Fe2O3 Thin Film Prepared by Spray Pyrolysis Technique