Volume 4, Issue 4, April 2014 ISSN: 2277 128X
International Journal of Advanced Research in Computer Science and Software Engineering
Research Paper
Available online at: www.ijarcsse.com

# Survey on Performance Analysis of Various Cryptographic Algorithms

**Bahar Saini**
*CSE& Kurukshetra University*
*Haryana, India*

***Abstract—Network security has gained huge prominence within the previous couple of years because it is that the key side of net based security mechanism. The simplest way to keep a message secret is to cover the actual fact of its existence which may be achieved by reworking the initial data into another type. This transformation will take place the shape of secret writing messages that create them non-readable. This art and science of achieving security is thought as cryptography. Cryptography encodes info in such a way that no-one will scan it , except the one who holds the key. Additional advanced crypto techniques make sure that the knowledge being transmitted has not been changed in transit. This paper offers a comparison of assorted cryptography algorithmic rules then finds best obtainable one algorithm for the network security***

***Keywords—Encryption, Cryptography, Symmetric Encryption, Advanced Encryption Standard (AES), Asymmetric Encryption, Decryption***

## I. INTRODUCTION

As we all know that demand of web is increasing day by day on transfer knowledge or alternative media types on the net. Currently it's the duty of the service provider to provide necessary security against the information thieves' attacks and providing the service under timely manner [3].

The quickly growing range of wireless communication users has led to increasing demand for security measures and devices to safeguard user knowledge transmitted over wireless channels. 2 sorts of cryptographic systems are developed for that purpose: symmetric (secret key) and asymmetric (public key) cryptosystems [9].

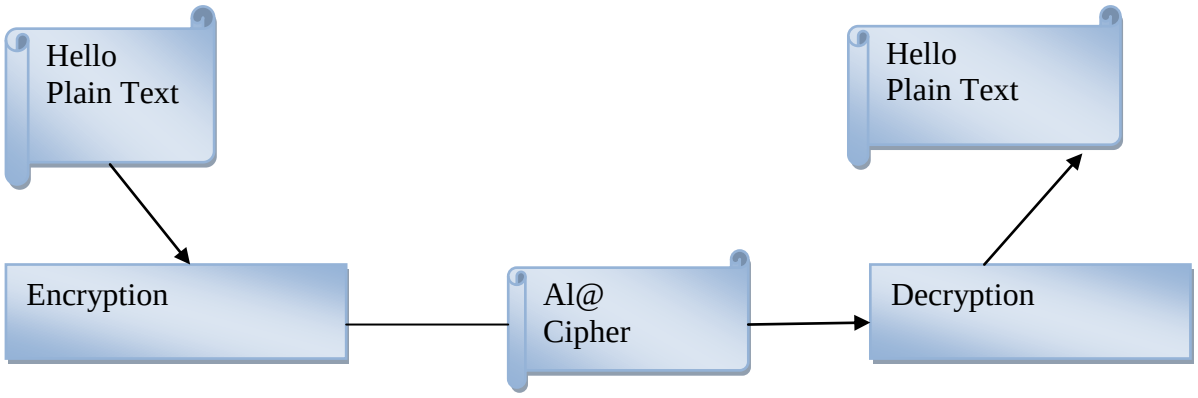
### 1.1 CRYPTOGRAPHY

Cryptography is that the study of Secret (crypto)-Writing (-graphy). It is the science or art of encompassing the principles and methods of transforming an intelligible message into coded type or unreadable type and that coded type then transforming the message back to its original type. Because the field of cryptography has advanced; cryptography these days is assumed as the study of techniques and applications of securing the integrity and authenticity of transfer of data under difficult circumstances [2].

Encryption is that the method of changing information to illegible type. Decryption is that the method of changing encrypted information into original type.

#### 1.1.1 Symmetric Encryption

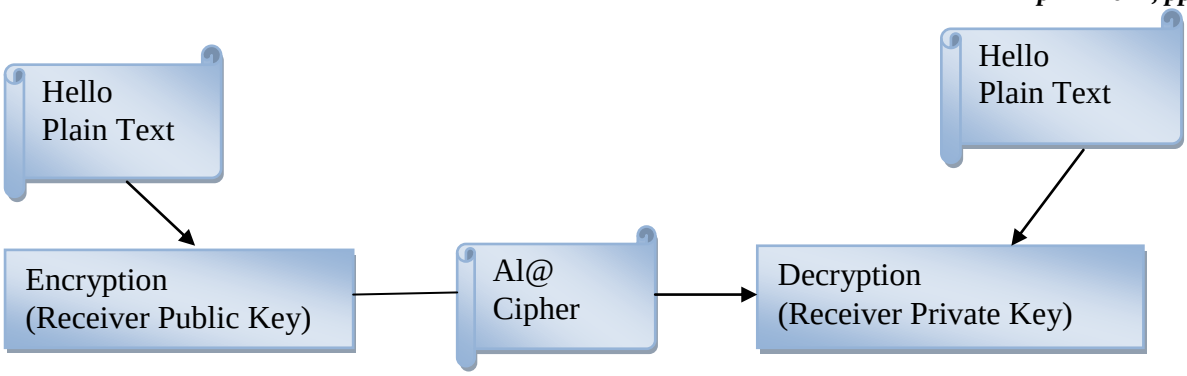
In case of Symmetric Encryption, same cryptography keys are used for coding of plaintext and decryption of cipher text. Symmetric key encryption is less complicated and quicker however their main negative aspect is that both the users need to transfer their keys during a secure approach.




#### 1.1.2 Asymmetric Encryption

In the Asymmetric encryption, a couple of keys are used. It's additionally called Public Key Cryptography (PKC), as users tend to use a couple of keys: public key, which is known to public and a personal key that is purely known to user.




Steganography is a branch of data hiding during which secret data is camouflaged within other information. Steganography is a word with Greek origins means that "covered writing" (Greek words "stegos" which means "cover" and "grafia" which means "writing"). To communicate securely in such a way that the true message isn't visible to the observer is that the main objective of steganography [8].

### 1.2 CRYPTOGRAPHY GOALS

The goals behind using cryptography. They're as follow:

- *Authentication*: It implies that the information sender and information receiver should be genuine before causing and receiving data.
- *Confidentiality:* It implies that the user who is authenticates, can only access the messages or knowledge of other authenticated users.
- *Integrity:* It implies that the information is free from any kind of modification between sender and receiver.
- *Non-Repudiation:* This perform implies that neither the sender nor the receiver will incorrectly deny that they have sent an explicit message.
- *Access control:* Only the approved parties are able to access the given data. [2]

### 1.3 AES (Advanced Encryption Standard)

The Advanced Encryption Standard is outlined by the National Institute of Standards and Technology (NIST) of the United State Government standard for symmetric encryption[9].
AES is the strongest and best cryptology algorithm because of 3 areas: cost, implementation and security.AES also proved that it secure against large number of attacks.
AES could be a block cipher that encrypts a 128-bit block (plaintext) to a 128-bit block (cipher text), or decrypts a 128-bit block (cipher text) to a 128-bit block (plaintext).
The length of cipher key used by AES can be 128, 192, or 256 bits. The encryption/decryption with a key (cipher key) is denoted AES-128, AES-192, AES-256 severally. AES-128, AES-192, AES-256 process the information block in, respectively, 10, 12, or fourteen iterations of a pre-defined sequence of transformations, that are also referred to as "rounds" (AES rounds) for short.
The rounds are identical apart from the last one that slightly differs from the others (by skipping one of the transformations). The rounds work on two 128-bit inputs: "State" and "Round key". Every round from one to 10/12/14 uses a distinct Round key. The 10/12/14 round keys are derived from the cipher key by the "Key Expansion" Algorithm program .This algorithm is independent of the processed information, and may be applied independently of the encryption/decryption phase[4].

### 1.4 APPLICATION OF CRYPTOGRAPHY

#### 1.4.1 Secure Data Transmission Using Proxy-Signcryption

The signcryption could be a public-key primitive that simultaneously performs the functions of both cryptography and digital signature. Integration of signcryption and proxy signature public key paradigms provides secure transmission .It is economical in computation and communication costs [4].

#### 1.4.2 Monitoring Communication

Cryptography will offer staggeringly robust encryption; it will impede the government's efforts to legitimately perform electronic reconnaissance So as to fulfil this would like, key is escrowed via entrusted third party .This technology permits the use of robust cryptography, however additionally permits the government when legally authorized to get decryption keys held by escrow agents[4].

**1.4.3 Transferring Files on Network**

Files that are to be exchanged between users got to be protected against malicious users and attackers. Symmetric Key cryptographic uses solely single key for both encryption and decipherment. During this technology symmetric key is then encrypted with public key that is related to sender of file to get encrypted file and this encrypted file is then send to receiver. To decrypt the file, encrypted file system component driver uses private key that is related to receiver to decrypt the symmetric key used to encrypt file. The encrypted file system component driver is then uses symmetric key to decrypt the file [4].

**1.4.4 Certificates and Authentication**

A certificate is an electronic document that identifies an individual, a server, a company, or another entity and to associate that identity with a public key. Certificate authorities (CAs) issued certificate that binds a specific public key to the name of the entity that the certificate identifies (the name of an employee or a server). In addition to it, a certificate includes a serial number, name of certificate authority who issued it. And also it includes digital signatures of the issuing CA. Certificates help prevent the use of fake public keys for impersonation. . Solely the general public key certified by the certificate can work with the corresponding private key possessed by the entity known by the certificate [4].

## II. RELATED STUDY

Shivangi Goyal et.al [1], the author gave a short outline of cryptography, whenever it's applied and its usage in numerous forms. It provides knowledge, integrity, electronic signatures, confidentiality and advanced user authentication. The ways of cryptography use mathematics for securing the info (encryption and decryption).

Sweta K.Parmar et.al [2], the author gave a comparison of varied encryption algorithms and so finds best offered one algorithm for the network security.

Amritpal Singh et.al [3], the author projected the two main characteristics that identify and differentiate encryption algorithm from another are their speed and effectiveness in securing the info and their capability to secure the protected knowledge against attacks. This paper provides a comparative study between four such wide used encryption algorithms DES, of DES, 3DES, AES and RSA on the idea of their ability to secure and protect knowledge against attacks and speed of encryption and decryption.

Shaaban Sahmoud et.al [4], the author developed a additional powerful algorithm for cryptography. This algorithm is based on AES to get competely different sub keys from the initial key and using each sub key to encrypt.Author used AES to safegaurd their style from structural analysis.

Mohammad Soltani et.al [5], the author suggested a new robust cryptography algorithm to extend security within the Symmetric-key manufacturing algorithm. The ability to encrypt the secret file in consecutive stages, no limitation for the quantity of keys, changing the physical structure of the secret file, a part of secret file at one of the keys at each stage of cryptography, storing Interdependence of all keys in all stages of encrypting and decrypting making five keys at every stage of cryptography are the main features of defined cryptography algorithm. To make the keys interdependent and to encrypt the secret file by each of them, there are two independent algorithms to pick out the kind of algorithm needed to make the keys interdependent by the user, large changes within the body of the encrypted file In case of wrong decryption and to form the resulting keys and encrypted file unique after the cryptography method.

**Comparison table for assorted cryptographic algorithms**

| Cryptography Algorithm | Time Consumed (MilliSecond) | Throughput (MegaBytes/Second | Power Consumption (Micro Joule/Byte) | %Battery Consumption | Key Size(s) Speed | Speed | Security |
|---|---|---|---|---|---|---|---|
| AES | 350 | 4 | 2.6 | 0.0047 | 128, 192, 256 bits | Fast | Secure |
| DES | 370 | 4 | 2.7 | 0.005 | 56 bits | Slow | Insecure |
| 3DES | 440 | 3 | 3.1 | 0.0058 | 112/168 bits | Very Slow | Moderately Secure |
| RC2 | 470 | 3 | 3.5 | 0.0062 | …… | …… | …… |
| BlowFish | 50 | 25 | 0.8 | 0.0005 | 32-448 bits | Fast | Believed secured, but less attempted cryptanalysis than other algorithms |
| RC6 | 200 | 6 | 2.3 | 0.0028 | …… | …… | …… |

Akanksha Mathur et.al [6], the author presented an algorithm for encryption and decryption which is based on ASCII values of characters within the plaintext. This algorithm is employed to encrypt knowledge by using ASCII values of the info to be encrypted. The key used are going to be modifying o another string which string is employed as a key to encrypt or decrypt the info. So, it may be aforesaid that it's a form of isosceles encoding algorithmic rule as a result of it uses same key for encoding and coding however by slightly modifying it.. This algorithm operates once the length of input and therefore the length of key are same.

N.Lalitha et.al [7], the authors propose a data hiding technique using AES algorithm. The author used a combination of steganography and cryptography for improving the security**.**

## III. CONCLUSIONS

This paper presents a survey of performance analysis of various algorithms.DES, AES, RC2, Blowfish, 3DES and RC6 are some well-known cryptographic algorithms have been analysed. Numerous points can be concluded from the simulation outcome. Measurement of performance of various algorithms is quantified in terms of Time consumed (Millisecond), Throughput (Megabytes/Second), Power Consumption (Micro Joule/Byte), %Battery Consumption, Key size(s) Speed, Speed, Security. The best algorithm are those that are well-known and well-documented because they are well-tested and well studied. A good cryptographic system strikes a balance between what is possible and what is acceptable.

## REFERENCES

[1] Shivangi Goyal International Journal of Science and Technology Volume 1 No. 3, March, 2012 IJST.
[2] Sweta K.Parmar ,prof K.C.Dave2 IJSRD - International Journal for Scientific Research & Development| Vol. 1, Issue 4, 2013
[3] Amritpal Singh, Mohit Marwaha, Baljinder Singh, Sandeep Singh, International Journal of computer & technology, Vol 9, No 3.
[4] Shaaban Sahmoud, Wiram Elmasy, Shadi Abudalfa, International Arab Journal of e-Technology., Vol.3, No.1, Jan2013.
[5] Mohammad Soltani,Young Researchers Society, Department of Computer Engineering, Shahid Bahonar, Journal of Basic and Applied Scientific Research**.,**3(7).
[6] Akanksha Mathur / International Journal on Computer Science and Engineering (IJCSE), Vol. 4 No. 09 Sep 2012.
[7] N.Lalitha, ,P.Manimegalai, V.P.Muthukumar, M.Santha, INTERNATIONAL JOURNAL OF RESEARCH IN COMPUTER APPLICATIONS AND ROBOTICS Vol 2,issue.1 ,JANUARY 2014.
[8] Amitava Nag, Sushanta Biswas, Debasree Sarkar & Partha Pratim Sarkar, International Journal of Computer Science and Security, (IJCSS), Volume (4): Issue (6) 562.
[9] Ritu et al., International Journal of Advanced Research in Computer Science and Software Engineering 3(7), July – 2013.
[10] Kritika Acharya, Manisha Sajwan, Sanjay Bhargava International Journal of Computer Applications Technology and Research Volume 3– Issue 2.
[11] Diaa Salama Abdul. Elminaam, Hatem M. Abdul Kader and Mohie M. Hadhoud,International Journal of Computer Theory and Engineering, Vol. 1, No. 4,