2nd International Conference on Current Research Trends in Engineering and Technology
© 2018 IJSRSET | Volume 4 | Issue 5 | Print ISSN: 2395-1990 | Online ISSN : 2394-4099
Themed Section: Engineering and Technology

A Comparative Study on Digital Encryption Algorithms

Harsh Shah[1], Vipul Sharma[2], Dharmik Panchal[3], Sumeet Patel[4], Dr. Sheshang Degadwala[5]

[1-4]U.G.Student Computer Engineering, Sigma Institute of Engineering, Bakrol, Gujarat, India
[5]Head of Department, Computer Engineering, Sigma Institute of Engineering, Bakrol, Gujarat, India

ABSTRACT

Cryptography is very essential in our life nowadays. Without this our useful information is very insecure. Nowadays our all the information is on the internet whether it is for education or any government sectors or privet sectors and we have to make sure that no one steals it or miss use it. What if we send the important and sensible information to particular person over a web, and there might be the chance that someone steals the information. The information is of any type, whether it can be video, audio, text or images. It has to be secure over the net. We can secure our data by using cryptographic algorithms, yet people are confused which algorithm should preferable for their data encryption, though there's multiple algorithms, after all it's all about their privacy and security of their information. So in this paper we explain you about the algorithms, how it works and which is the best one as of now. We also compare algorithms with respect to performance and the complexity.

Keywords: Security, Encryption, Decryption, Algorithm

I. INTRODUCTION

Cryptography is the methodology or science that uses mathematical function to encrypt or decrypt the data which enables you to convert your sensitive information into unreadable form i.e. ensuring that while sending over the network, no one can steal and read the information that you encrypt. The one who breaks this cryptographic method is called cryptanalytic sometime they are called as attacker.

Cryptography algorithms and also called as ciphers, uses mathematical function which is used in encryption as well as decryption technique. It works as the mixture of the two things. One is the key which is used to encrypt the data, and of course the actual data which we have to encrypt it or in cryptographic terminology it is also called as plain text. Key can be anything like a word or the number or the phrase depends upon the algorithm which we use. The actual security is all depend on the key length used for encrypting the data and the secrecy of that key. More secure the key, more security of our information.

Encryption is the way of hiding the information basically. Now, the information can be text or it can be image or it can be video. We are encrypting the files just because; the encrypted files are not readable by human. It's messy information. The characters might be substituted or rearranged or replaced by some other character and even some random characters can be added in order to make it more complex and hide the secret information. To do so, there are many algorithms out there to encrypt the data.

Basically the encryption techniques are categorized into two parts. One is the symmetric way and another is asymmetric way. Well symmetric key algorithm is the one way of hiding information that is cryptography where the same key is used for encryption and decryption as well. Let's say one person is encrypting the information with the particular key and then he sends it to the other person over the network. Now the other person, who receives the encrypted data, must have the same key in order to decrypt the information. So the sender of encrypted data needs to send that key to the receiver. Asymmetric key cryptography is harder to utilize. It is also called as public key cryptography. In this algorithm each user has one pair of cryptographic keys. One is public key and another is private key. The private key is kept secret, while public key is widely distributed and used by other users. Now we know that there are many algorithms are used in order to secure the information, but why we need such kind of algorithms. For privacy and confidentiality, ensuring that no one can read the message expect the intended receiver. For authentication, process of proving one's identity. For integrity, assuring the receiver that the received message has not been altered in any from the original. For non-repudiation, a mechanism to prove that the sender really sent this message. For key exchange, the method by which crypto keys are shared between sender and receiver.

In cryptography, we start with the unencrypted data, which is referred as the plain text. Then plain text is encrypted into cipher text i.e. perform encryption operation, which will be turned into decrypted form called as plain text i.e. readable text. For this, this process is something written as:

$$C = E_k(P)$$

$$P = D_k(C)$$

II. METHODS AND MATERIAL

1. Asymmetric cryptosystem:

Asymmetric cryptography is a technique that the secret key is divided into two parts, a public key and a private key. Public key is been given to anyone, whether the person is trusted or not, while for the private key it must be secret. Asymmetric cryptography has two primary functionalities the one is authentication and the other is confidentiality. Messages are signed with a private key, and then anyone with the public key is able to verify that the message was created by someone possessing the corresponding private key. Working is slightly different way from symmetric encryption. Someone with the public key is able to encrypt a message, providing confidentiality, and then only the person in possession of the private key is able to decrypt it.

Public key cryptography is said to be the most significant new research in cryptography since years. Modern PKC was first described publicly by Stanford University professor Martin Hellman and graduate student Whitfield Diffie in 1976. They researched the two-key crypto system in which two parties engage with each other in a secure communication over a non-secure communications channel without having to share a secret key.

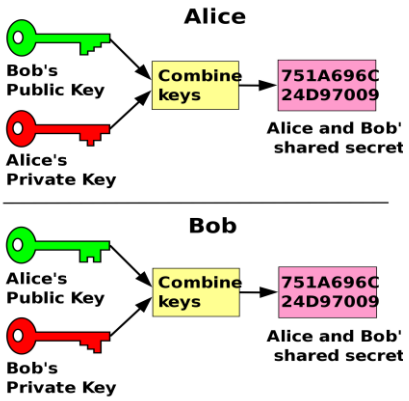

Figure I: Asymmetric key algorithm

1.1 RSA

RSA algorithm is a modern art encryption and decryption message. It's an asymmetric cryptographic

algorithm. There are two different keys, Public and Private. User creates and publishes product of two large prime number, along with value, as their public key. Everyone can use the public key to encrypt message, if the public key length is too large then the only person with knowledge of the prime factors can feasibly decrypt the entire message.

1.2 Deffie Hellman Key Exchange

Deffie hellman key exchange tactic to exchange data or information securely over internet. It's the first public key protocols. Vintage example of public key exchange implementation within the cryptographic fields. This algorithm is used to secure a variety of internet services. Secure encryption communication between two parties required to exchange data and communication.

1.3. Digital Signature

Based on public key cryptography and it is also known as asymmetric cryptography. One can generate two keys using public key algorithm like RSA and that keys are mathematically linked. One key is public and the other one is private. Now to create DS, signing software (such as an email program) creates a one-way hash of the electronic data to be signed in and private key is used to encrypt the hash. Thereafter encrypted hash along with other information such as hashing algorithm is the digital signature. The difference between encrypting the hash and not encrypting the whole document is because hash can convert an arbitrary input into fixed length value, which is usually much shorter. Time consumption is less since hashing is much faster to sign in.

1.4. Elgamal

Elgamal Encryption is an asymmetric key encryption algorithm used for public key cryptographic system. This system is based on Diffie-Hellman key exchange and provides an additive layer of security with asymmetrically encrypting keys which is previously used for symmetric message encryption. Usually used in hybrid cryptosystem. Encrypting the message itself using symmetric cryptosystem and Elgamal and then used to encrypt the key used for symmetric cryptosystem. System is slower than symmetric ones, so it is faster to encrypt the symmetric key with Elgamal and the message with symmetric cipher.

2. Symmetric cryptosystem:

Symmetric key cryptography methods employ a single key for both encryption and decryption. The sender uses the key to encrypt the plaintext and sends the cipher text to the receiver. The receiver applies the same key to decrypt the message and recover the plaintext. Single key is used for both functions, encryption and decryption is also called *symmetric encryption*. With this cryptographic algorithm, it is obvious that the key must be known to both the sender and the receiver; that, in fact, it s the secret. The biggest issue with this algorithm, of course, is the distribution of the key. Secret key cryptography schemes are generally categorized as being either *stream ciphers* or *block ciphers*.

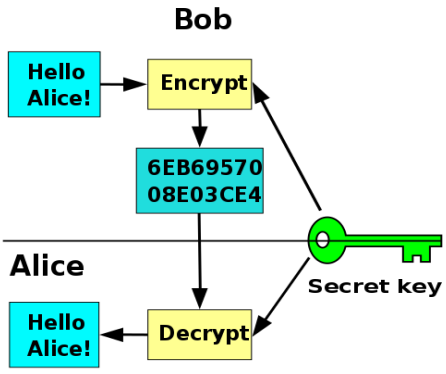

Figure I: Symmetric key algorithm

2.1 AES

The advanced encryption standard is the algorithm, which is widely adopted and it is very popular symmetric algorithm. It is six time faster than triple data encryption standard. It is an iterative algorithm in which substitution and permutation operation performs. It uses three sizes of keys, 128, 192 and 256 bits based on rounds.

2.2 DES

The DES is again the symmetric key algorithm that uses block cipher mechanism and it was published by National Institute of Standards and Technology. It is the implementation of the pure festal cipher which performs 16 rounds. There's the key generator so once we use the 56 bit key for the DES, it generates 48 bits of key for every feistel round. But around few years ago the cryptanalytic found that the algorithm is weak because of the weak key.

2.3 Twofish

Two fish is the symmetric key block cipher algorithm which uses the block size of 128 bits and key sizes up to 256 bits. The algorithm was one of the five finalist's algorithms of the Advanced Encryption Standard contest, but it was not selected for standardisation.

III. PERFORMANCE

Methods	AES	DES	RSA
Key Size	128,192,256 Bits	56 Bits	>1024 Bits
Block Size	128 Bits	64 Bits	Minimum 512 Bits
Encryption	Faster	Moderate	Slower
Decryption	Faster	Moderate	Slower
Scalability	Not Scalable	Scalable, Due to varying the key size and block size	Not Scalable
Algorithm	Symmetric	Symmetric	Asymmetric
Power Consumption	Low	Low	High
Inherent Vulnerabilities	Brute Force attack	Brute forced, Linear and differential cryptanalysis attack	Brute forced and oracle attack
Key Used	Same key used for Encryption & Decryption	Same Key used for Encryption & Decryption	Different key used for Encryption & Decryption
Rounds	10/12/14	16	1
Simulation Speed	Faster	Faster	Faster
Hardware & Software implementations	Faster	Better in Hardware	Not efficient

IV. CONCLUSION

So we conclude that to achieve any kind of digital security in the Sense of the information, you can select as per your requirement. This paper approach you to find your best algorithm keep in mind that which is faster than others to secure your information and sending it via insecure channel.

IV.REFERENCES

[1] K. Sekar and M. Padmavathamma, "Comparative study of encryption algorithm over big data in cloud system," in IEEE 2016 ed. New Delhi, India.

[2] Abdullah Al Mamun, Khaled Salah and Somaya Al-Maadeed", BigCrypt for big data encryption", in IEEE 2017th ed. Valencia, Spain.

[3] A. Nadeem and M. Y. Javed, "A performance comparison of data encryption algorithms", in IEEE 2006th ed. Karachi, Pakistan.

[4] Madhumita Panda "Performance analysis of encryption algorithms for security" in IEEE 2017th ed. Paralakhemundi, India.