Volume 5, Issue 4, April 2015 ISSN: 2277 128X
International Journal of Advanced Research in Computer Science and Software Engineering
Research Paper
Available online at: www.ijarcsse.com

A Review on: Network Security and Cryptographic Algorithm

Swati Kashyap, Er. Neeraj Madan
Student, Haryana Engineering College,
Haryana, India

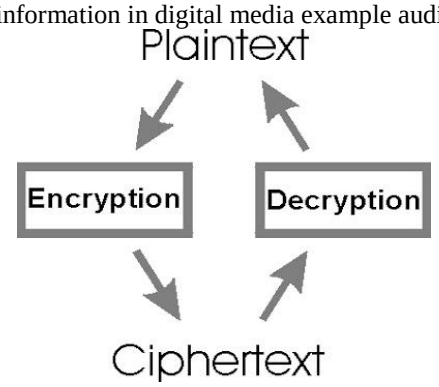
Abstract: Security is the most challenging aspects in the internet and network application. These days the applications like Internet and networks are growing very fast, thereby the importance and the value of the exchanged data over the internet or other media types are increasing. for secure communication the cryptography is essential. in information security, Cryptography algorithms is very important. Cryptography is subdivided into two - Symmetric and Asymmetric key cryptography Cryptography has come up as a solution in information security system against various attacks. The comparision of various encryption algorithms DES, 3DES, AES & RSA on the basis of key size, rounds and block size is the objective .

Keywords: – Advanced Encryption Standard, Data Encryption Standard, Rivest –Shamir-Adlemen ,Triple Data Encryption Standard ,encryption,decryption.

I. INTRODUCTION

CRYPTOGRAPHY

Cryptography means "Hidden Secrets", now-a-day concerned with encryption.cryptography,the study of techniques for secure communication. It is useful for analyzing those protocols, that are related to various aspects in information security such as authentication, confidentiality of data, non-repudiation and data integrity. It is a part of information security. Both cryptography and Steganography have a secure method – AES algorithm is a very secure technique for cryptography and the Steganography methods, which are useful for frequency domain, are highly secured. A technique named Data hiding that is used to hide information in digital media example audio, images, video etc.



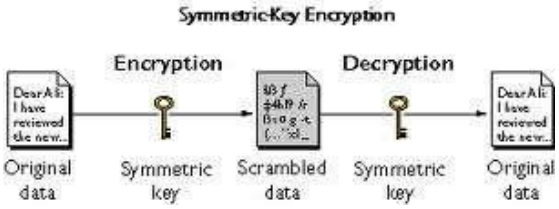
The goals behind using cryptography are discuss as follow:
Authentication of data: The data sender and receiver must be authenticated before sending and receiving data.
Confidentiality of data: It means that the user who is authenticates, can only access the messages or data of other authenticated users.
Integrity: integrity of data means that the data is free from any kind of modification between sender and receiver.
Non-Repudiation: it is defined as neither the receiver nor the sender can falsely deny that they have sent a certain message.
Service Reliability: secured system can be attacked by intruders, which may affect the service that is provided to the user.

Symmetric and Asymmetric encryptions

There are commonly two types of techniques that are used for encrypt/decrypt the secured data like Asymmetric and Symmetric encryption techniques.

Symmetric Encryption

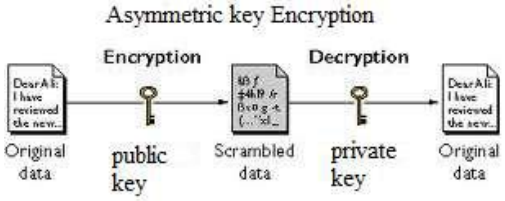
In case of Symmetric Encryption, same cryptography keys are used for encryption of plaintext and decryption of cipher text . Symmetric key encryption is faster and simpler but their main drawback is that both the users need to transfer their keys in a secure way.



As shown in the figure , there is only one key used both for encryption and decryption of data. So the main problem over this system is, users key should be transfered in a safe manner.

Asymmetric Encryption

Asymmetric encryption uses two keys and also known as Public Key Cryptography, because user uses two keys: public key, which is known to public and a private key which is only known to user.



In Asymmetric key Encryption, the different keys that are used for encryption and decryption of data that is Public key and Private key.

AES (Advanced Encryption Algorithm)

AES is an iterated symmetric block cipher, which is describe as:

- working of AES is done by repeting a similar outlined steps multiple times.
- AES can be a secret key encryption algorithm.
- AES operates on a predetermined bytes

AES in addition as most encryption algorithms is reversible. This means that a similar steps are performed to finish both encryption and decryption in reverse order. The AES algorithm operation using bytes that make it easier to implement and justify.

This key is expanded into individual sub keys, which is for every process round. This methodology is termed KEY EXPANSION. As AES is associate iterated block cipher .means the similar operations are performed many times on a fixed number of bytes.

DES (Data Encryption Standard)

DES is a block encryption algorithm. DES is a symmetric algorithm, means same key is used for encryption and decryption . one of 64-bit key is used. From 64 bits, independent key is made by 56 bits, which determine the exact cryptography transformation, for error detection DES, 8 bits are used.

Six different permutation operations are used both in key expansion part and cipher part. Decryption is same as encryption in DES algorithm, in reverse order , the round keys are applied. The DES weaknesses is recorded by many attacks and methods, which implies that it is an insecure block cipher.

3-DES(Triple – Data Encryption Standard)

It uses 64 bit block size with 192 bits of key size. The method of encryption is same as to the one in the original DES but applied 3 times to increase the encryption level and the average safe time. The disadvantage regarding 3DES is that it is slower than other block cipher methods .

RSA(Rivest –Shamir-Adlemen)

This is public key encryption algorithm developed by Adi Shamir, Ron Rivest and Len Adlemen in 1977. It is most popular asymmetric key cryptographic algorithm. RSA may use to provide both secrecy and digital signature. It uses the prime no. to generate the public and private key based on mathematical fact and multiplying large numbers together. the block size data is used in which plaintext and cipher text are integers between 0and n1 for some n values. Consider the Size of n is 1024bits or 309 decimal digits. In this two different keys are used for encryption and decryption purpose. And also the sender knows encryption key and receiver knows decryption key.

Basic Terms

Plain Text

The original message that the person wishes to communicate with the other is defined as Plain Text. For example, a person named alice wishes to send “Hello Friend how are you” message to the person Bob. Here “Hellow Friend how are you” is a plain text message.

Cipher Text

The message that cannot be understood by any one or a meaningless message is what we call as Cipher text. Suppose, "Ajd672#@91ukl8*^5%" is a Cipher Text produced for "Hello Friend how are you".

Encryption

A process of converting plain text into cipher text is called as Encryption. This process requires two things- an encryption algorithm and a key. algorithm means the technique that has been used in encryption. Encryption of data takes place at the sender side.

Decryption

A reverse process of encryption is called as Decryption. In this process Cipher text is converted into Plain text. decryption process requires two things- a decryption algorithm and a key. algorithm means the technique that has been used in Decryption. Generally the both algorithms are same.

Key

A key is a numeric or alpha numeric text or may be a special symbol. the key is used when encryption takes place on the plain text and at the time of decryption takes place on the cipher text. For example, if key of 3 is uses by the Alice to encrypt the plain text "President" then cipher text produced will be "Suhylghqw".

Input data size- Different algorithm required different memory space to perform the operation. The memory space required by any algorithm is determined on the basis of input data size, number of rounds etc. The algorithm is considered best which use small memory and perform best task.

Time- The time required by algorithm to complete the operation depends on processor speed, algorithm complexity. Less the time algorithm takes to complete its operation better it is.

Throughput- the encryption algorithms having Throughput is calculated by dividing the total plaintext in Megabytes encrypted on total encryption time for each algorithm.

II. LITERATURE SURVEY

A. Implementation of AES Using S-Box Rotation

AES algorithm is considered as a secured algorithm. S-box and key used have some security issue . In this paper focus is on the S-box rotation so that we get highly secured information .earlier the standard AES consists of four stages while in the new design, their is a five stages and the extra stage is known as S-box rotation .Implementation of proposed work and Experimental results are to be discuss.[1]

B. FPGA Implementation of Reconfigurable Parameters AES Algorithm

In this paper, a novel method of using customized (AES) variable parameters is introduced. This method depends on a continuous parameters reconfiguration and a customization of each internal block. The customization depends on varying the four transformations (polynomial and affine transformations for S-Box (SB), Shift Rows (SR) transformation, and Mix Column (MC) transformation). Internal AES blocks (SB, SR, and
MC) are varied each round. Furthermore, these blocks are randomly interconnected during each session. The ciphered output was tested using avalanche, strict avalanche, and other NIST tests. This method overcomes (ECB) mode problems which appear when there is high redundancy in the plain data and also increasing strength against brute force attacks. The proposed AES is implemented on Field programmable Gate Arrays (FPGAs**) [2].**

C. An Overview of Cryptanalysis Research for the Advanced Encryption Standard

Since its released in November 2001, the Advanced Encryption Standard (NIST FIPS-197) has been the subject of extensive cryptanalysis research. This research importance has intensified since AES was named as a Type-1 Suite B Encryption Algorithm (CNSSP-15), in 2003, by NSA. As such, AES is now authorized to protect classified and unclassified national security systems and information. an overview of current cryptanalysis research on the AES cryptographic algorithmis provided by the paper on the impact discussion is provided by each technique to the strength of the algorithm in national security applications. The conclusion of paper with an attempt at a forecast of the usable life of AES in these applications[3]. A Review on Various Most Common Symmetric Encryptions Algorithms. Security is the most challenging aspects in the internet and network application. In applications like internet and network are growing very fast, so the importance of the exchanged data over the internet or other media types are increasing. In data communication ,information security is utmost issue. A great loss to the organization can be cause by loss or threat to information . A main role is played by Encryption technique in information security system. A comparison of various encryption algorithms is given by this paper and then finds best available one algorithm for the network security[7]. A Study of 3DES, DES, RSA and AES. In today world importance of exchange of data over internet and other media type is eminent; the search for best data protection against security attacks and a method to timely deliver the data without much delay is the matter of discussion among security related communities. Cryptography is a method which provides the security mechanism within timely driven fashion. Usually, Cryptography is attached to the definition of encryption ,referred to as "the study of secret",. characteristic that identified and differentiated encryption algorithm from another are

their capability to secure the protected data against attacks and their speed and effectiveness in securing the data. comparative study is provided by this paper between four such widely used encryption algorithms 3DES,AES,RSA & DES on the basis of their ability to secure and protect data against attacks and speed of encryption and decryption[4].

D. Efficient Implementation of AES

With the fast progression of digital data exchange in electronic way, in data storage and transmission, information security is becoming much more important. A solution is present for cryptography which plays a vital role in information security system against various attacks. some algorithms is used in this security mechanism uses to scramble data into unreadable text which can be only being decoded or decrypted by party those possesses the associated key. Two types of cryptographic techniques are being used: symmetric and asymmetric. In this paper we have used symmetric cryptographic technique AES (Advance encryption standard) having 200 bit block as well as key size. And the same conventional 128 bit conventional. using 5*5 Matrix AES algorithm is implemented for 200 bit. On implementing, the proposed work is compared with 256 bit, 192 bits & 128 bits AES techniques on two points. These points are encryption and decryption time and throughput at both encryption and decryption sides[5].

E. Efficient Data Hiding By Using AES & Advance Hill Cipher Algorithm.

In this paper we propose a data hiding technique using AES algorithm.The two popular ways of sending vital information in a secret way is Steganography and Cryptography. For making data secured cryptography was introduced. cryptography cannot provide a better security approach because the scrambled message is still available to the eavesdropper. a need of data hiding arises. So, by combining the steganography and cryptography , the security can be improved . many cryptography techniques are available here; among them AES is one of the most useful techniques .In Cryptography, use of AES algorithm to encrypt a message using 128 bit key the message is hidden . In this proposed technique, use of advance hill cipher and AES to enhance the security level which can be measured by some measuring factors. The result shown by this work is advance hybrid scheme gives better results than previous[6].

SUMMARY OF COMPARISION OF VARIOUS ENCRYPTION ALGORITHM

In the following Table, Comparative study of various encryption algorithm on the basis of their ability to secure and protect data against attacks and speed of encryption and decryption.

Algorithms	BASED ON	Key Size	Block Size	Rounds
Data Encryption Standard	Block Encryption algorithm	56 bits	64 bits	16
Triple- Data Encryption Standard	Block Encryption algorithm	112 bits or 168 bits	64 bits	48
Advanced Encryption Standard	Secret key Encryption algorithm	128 bits,192 bits,256 bits	128 bits	10,12or 14
Rivest-Shamir-Adlemen	Public key Encryption algorithm	1024 or 2048 bits	512 bits	

III. CONCLUSION

By reviewing the papers we finally conclude that the performance evaluation of cryptography algorithm depends on throughput of encryption scheme, CPU time taken & packet size. The throughput of the encryption scheme is calculated by dividing the total plaintext in MB by total encryption time in Second for each algorithm. If the throughput value increases, the power consumption by this encryption technique is decreased. AES is the far better algorithm in terms of performance and security but its power consumption is on high.

REFERENCES

[1] Bahar Saini," Implementation of AES using S-BOX rotation", International journal of advanced research in computer science and software engineering, May 2014.

[2] A.E.Rohiem, F.M.Ahmed and A.M.Mustafa, "FPGA Implementation of reconfigurable parameters AES algorithm", 13th international conference on AEROSPACESCIENCE AND AVIATION TECHNOLOGY, ASAT-13, May 26-29, 2009.

[3] Alan Kaminsky, Michael Kurdziel, Stanislaw Radziszowski,"An overview of cryptanalysis research for the advanced encryption standard", Rochester institute of Technology , NY,Horris corp, RF communication Div.,Rochester,NY.

[4] Amritpal Singh, Mohit Marwaha, Baljinder Singh, Sandeep Singh," Comparative study of DES, 3DES, AES and RSA".

[5] Ritu Pahal, Vikas Kumar,"Efficient implementation of AES", International journal of advanced research in computer science and software engineering, volume3, issue 7, july2013.

[6] N.Lalitha,P.Manimegalai,V.P.Muthu kumar,M.Santha,"Efficient data hiding by using AES and advance Hill cipher algorithm ", International journal of research in computer applications and Robotics, volume 2, issue 1 ,January 2014.

[7] Sweta K.Parnar,Prof. K.C.Dave,"A review on various most common symmetric encryption algorithm", International journal for scientific research and development ,volume 1,issue 4,2013.

