A COMPARISON OF SYMMETRIC KEY ALGORITHMS DES, AES, BLOWFISH, RC4, RC6: A SURVEY

P. Princy

Research Scholar, School of Computer Science, Engineering and Applications,
Bharathidasan University, Trichy, India.
Princy0405@gmail.com

ABSTRACT - Cryptography or cryptology is a Greek word it means 'hidden'. It involves the blotting out of the specials meaning of letters, but not their existence. It is the one of the main categories of computer security that converts information from its normal form into an unreadable shape. The art of cryptography has turn more complex in order to make information more secure. The types of cryptography, one is symmetric and another one is asymmetric. Here we discuss about symmetric algorithms briefly. There are many symmetric algorithms are used now a day's like AES, DES, 3DES, BLOWFISH, RC4, RC6.In this survey we make the blowfish algorithm is more secure to compare other symmetric algorithms.

Keywords - Cryptography, symmetric, DES, AES, 3 DES, BLOWFISH

I. INTRODUCTION

The important type of the encryption is the symmetric key encryption. Symmetric key algorithms exist used the similar key for both the encryption and decryption. Hence the key is main applied secret. Symmetric algorithms have the rewards of not consuming too much of computing power and it works with richly speed in encryption. The Symmetric key algorithms are separating into two types: Block cipher and Stream cipher. The block cipher input is expressed as block of plaintext of constant size betting on the type of symmetric encryption algorithm, and the key of determined size is applied to block of plain text and then the output block of the same size as the block of plaintext is received.

II. Basic Terminology used in cryptography

A. *Plain Text*

The master copy message which is to be sent from sender to the recipient. This plain text is kept as an input at the time of encryption action. For example the sender wants to send a message “hello” to receiver then it is regard as a plaintext.

B. *Cipher Text:*

Cipher text is a text which is being sent from sender to receiver and it is not understandable by anybody. And it is the output of the encryption work. For example: “*#85K&” it is a cipher text produced for plain text “hello”.

C. *Encryption:*

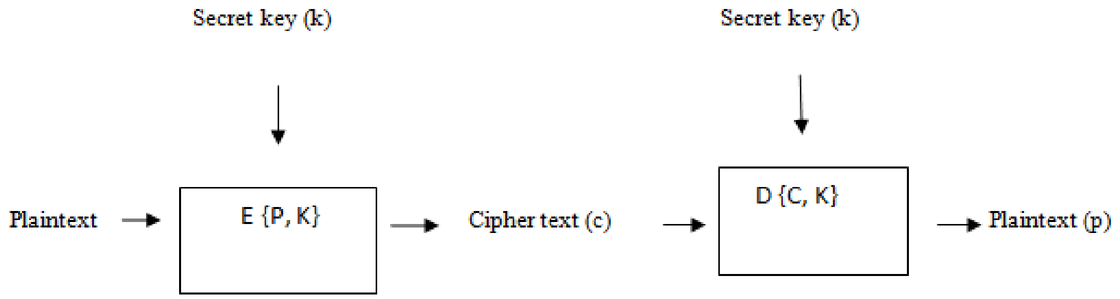
It is a process of converting a plain text into cipher text by using an encryption key and the algorithm is known as encryption algorithm.

D. *Decryption*:

It is a process of converting a cipher text into a plain text by applying a decryption key and an algorithm known as decryption algorithm.

D. *Keys:*

A Key is a numeric or alpha numeric text or may be a curious character. The Key is applied at the time of encryption carries a place on the plaintext and at the time of decryption takes a place on the cipher text. The choice of key in Cryptography is very important as the security of encryption algorithm depends directly on it [5].



Cryptography Security Algorithm

III. Goals of Cryptography

Cryptography serves following goals:

A. *Confidentiality*: It's defined as that only the sender and the prearranged receiver should be able to access the subjects of a message.

B. *Authentication*: In this mechanism helps to establishment proof of identities. This work defends that the source of the message is correctly identified.

C. *Integrity:* This mechanism assists that the contents of the message remain the same when it reaches the aimed recipient as sent by the sender.

D. *Non- repudiation*: It does not allow the sender of a message to rebut the claim of not posting the message.

E. *Access Control:* It's depicted and control who can access what.

F. *Availability*: It states that intends should be usable to authorized parties all the times.

IV. TYPES OF CRYPTOGRAPHY

There are two types of cryptography algorithms. That is symmetric and asymmetric. Here the most important type of the encryption is the symmetric key encryption. Symmetric key algorithms are widely used the only one key for both encryption and decryption process. Hence the key is in the sense of mystery. Symmetric algorithms have the pros of not taking too much of computing power and it works with high level of speed in encryption. Symmetric key algorithms are dividing into two types: Block cipher and Stream cipher. In this block cipher input is caught as a block of plaintext of fixed size look upon the type of a symmetric encryption algorithm, key of lasting size is applied on to block of plain text and then the output block of the same size as the block of plaintext is received. In stream cipher at a time one bit is encrypted. Some most usable Symmetric-key algorithms are described here: Data Encryption Standard, 3DES, and Advanced Encryption Standard.

A. Data Encryption Standard (DES)

Data Encryption Standard (DES) is a symmetric- key block cipher. It is released as FIPS-46 in the Federal Register in 1977 by the National Institute of Standards and Technology (NIST). In the encryption site, DES carries a 64-bit plaintext and makes same 64-bit cipher text, at the decryption site, it capture a 64-bit cipher text and produces a 64-bit plaintext, and also the same 56 bit cipher key is applied for the pair encryption and decryption. The encryption build up is made of two permutations (P-boxes), it is called the initial and final permutation, and it has a 16 Feistel rounds. For each one uses a different 48-bit round key yielded from the cipher key granting to a predefined algorithm.

The function of the DES algorithm is made up of four sections:

- Expansion P-box
- A whitener (that adds key)
- A group of S-boxes
- A straight P-box.

B. Advanced Encryption Standard (AES)

In Advanced Encryption Standard is a symmetric- key block cipher issued as FIPS-197 in the Federal Register in December 2001 by the National Institute of Standards and Technology (NIST). The AES is a non-Feistel cipher. AES encrypts a data with the block size of 128-bits. It applies 10, 12, or fourteen rounds. To depending on the number of rounds, the key size may be in 128, 192, or 256 bits. AES works on a 4×4 column-major order matrix of bytes, it's known as the state.

C. Triple-DES

A quiet and simple way of heightening, the key size of DES is to use Triple DES, to hold it versus attacks without the requirement to design an entirely new block cipher algorithm. In case of DES, Encryption key size was only 56 bits, this key size of 56 bits was usually enough when that algorithm was designed, because of enhancing the computational quality brute force attack is Triple DES supplies a comparatively simple method of increasing the key size of DES to defend against such attacks, without the required to design a completely new block cipher algorithm. Triple DES is the simple modification of DES. It executes DES thrice. It is also a block cipher causing three keys each of 56 bits and all the keys are independent.

D. Blowfish Algorithm

Blowfish is defined as a symmetric block cipher algorithm. Basically it uses the same secret key to both the encryption and decryption process of messages. Here the block size for Blowfish is 64 bits; messages that aren't a product of 64-bits in size have to be trudged. It uses a variable –length key value, from 32 bits to 448 bits. It is reserve for applications where the key is not varied frequently. It is substantially faster than most encryption algorithms when performed in 32-bit microprocessors with huge data caches.

E. RC4

RC4 algorithm is a stream cipher symmetric key algorithm. As the data stream is merely XOR with generated key sequence. It uses a variable length key value is 256 bits to initialize a 256-bit state table. A state table is widely used for generation of pseudo-random bits which is XOR with the plaintext to give the cipher text [3].

F.RC6

RC6 extends good operation in terms of security and compatibility. RC6 is a Feistel Structured private key algorithm that causes use a 128 bit plain text with the 20 rounds and a variable Key Length of 128, 192, and 256 bit. As RC6 operates on the principle of RC that can maintain an extensive range of key sizes, word-lengths and number of rounds, RC6 does not comprise S- boxes and same algorithm is used in turned for decryption [3].

Faster Transfer of AES Encrypted Data over Network

Advanced Encryption Standard (AES) is a NIST (National Institute of Standards and Technology) stipulation of the encryption and decryption electronic data. AES tolerated the drawback of slow processing and it takes the large time of data transferring, so to increase the speed of the process of the AES algorithm, we apply AES algorithm in parallel. There is a file of 5 megabit (5242880 bits) which requires to be sent from sender to receiver. Here using a 128 bit AES algorithm the number of steps expected will be 5242880/128=40960. This means 40960 data blocks will be made on which AES will be used individually. But using the parallel approach of AES algorithm, the number of steps required will be 40960/64=640 where 64 is number of processors. The total time expect to process the data will be reduced by number of processor time’s uniprocessor time.

A Study of Encryption Algorithms (RSA, DES, 3DES and AES) for Information Security

In this survey we used avalanche effect to bear AES algorithm is supply more security to other symmetric algorithms. AES algorithm is most effective in the terms of speed, time, throughput, and avalanche effect. The Security furnished by these algorithms can be enhanced further, if more than one algorithm is applied to data.

A Modified Crypto Scheme for Enhancing Data Security

Here we propose a Software tool which involves cryptographic enciphering and deciphering on with File separating and joining mechanisms. And also we have to use modified Blowfish algorithm for encryption and decryption of data. While we use only one algorithm, we discriminate the cryptographic scheme by changing the key for varying file slices. Our results this proposed system is clearly explain that our tool serves as a better solution both in the terms of performance as well as security. It also gives a high end data security when transporting over any insecure medium. The Intruders don’t have any idea about our modification both in terms of algorithm as well as in our design, so breaking this system is highly impossible. We are sure that is, this proposed software tool is unique of its kind and it can also be tuned in terms of higher performance and security in near future by adding or replacing cryptographic part because of its modularity in design.

A Survey on Cryptographic Algorithms

Compare the block size, key size and encryption and decryption time, CPU processor time in the form of throughput and power expenditure to the symmetric algorithms DES, AES, 3DES, BLOWFISH. The blowfish algorithm is better than the other algorithms. Compare to other algorithm the BLOWFISH algorithm is more secure and fast process algorithm. It reduces the execution time and it gives more security and also it consumes less memory usage compared to any other algorithms.

Table 1. Comparison of symmetric algorithms

Algorithms	**Key size**	**Block size**	**Round**	**Structure**	**Flexible**	**Features**
DES	64 bits	64 bits	16	Feistel	No	Not structure, Enough
3DES	112 or 118 bits	64 bits	48	Feistel	Yes	Adequate security
AES	128,192,256 bits	128 bits	10,12,14	Substitution, Permutation	Yes	Replacement for DES, Excellent security
RC4	Variable	40-2048 bits	256	Feistel	Yes	Fast cipher in SSL
RC6	128-256 bits	128 bits	20	Feistel	Yes	Good security
BLOW FISH	32-448 bits	64 bits	16	Feistel	Yes	Excellent security

V. CONCLUSION

From this survey we can conclude the blow fish algorithm is more secure to compare other symmetric key algorithms, and produce best result for less processing time and rounds. To increase the key size of blowfish algorithm 128 to 448, it gives more privacy to the messages and provides high end data security when transmitting over any unsafe medium. Table.1shows the blowfish algorithm is provides excellent security to compare symmetric algorithms.

REFERENCES

[1] G. Manikandan , G. Krishnan and Dr.N.Sairam A Unified Block And Stream Cipher Based File Encryption Journal of Global Research in Computer Science Volume 2, No. 7, July 2011.

[2] Krishnamurthy G.N, Dr. V. Ramaswamy, Leela G.H and Ashalatha M.E Blow-CAST-Fish: A New 64-bit Block Cipher IJCSNS International Journal of Computer Science and Network 282 Security, VOL.8 No.4, April 2008.

[3] Anjula Gupta1 Navpreet Kaur Walia Cryptography Algorithms: A Review International Journal of Engineering Development and Research IJEDR Volume 2, Issue2 2014.

[4] Maulik P. chaudhari, Sanjay R.patel, A Survey on Cryptography Algorithms, International Journal of Advance Research in Computer Science and Management Studies, Volume 2, Issue 3, March 2014.

[5] Mohsin Khan, Sadaf Hussain, Malik Imran Performance Evaluation of Symmetric Cryptography Algorithms: A Survey, International Journal of Information Technology and Electrical Engineering ,Volume 2, Issue 2 April 2013.

[6] Maulik P. Chaudhari, Neha Parmar Blowfish Algorithm by Modify Randomness for S-Boxes using Fuzzy Value and Apply Encryption or Decryption on Image International Journal of Science and Research (IJSR) Volume 3 Issue 6, June 2014

[7] Gurpreet Singh and Supriya A Study of Encryption Algorithms (RSA, DES, 3DES and AES) for Information Security International Journal of Computer Applications Volume 67– No.19, April 2013.