International Journal of Emerging Engineering Research and Technology
Volume 3, Issue 10, October 2015, PP 48-49
ISSN 2349-4395 (Print) & ISSN 2349-4409 (Online)

Study of Symmetric Cryptography Algorithms

Ms.Snehalata D.Ulhe*, Ms.Nilima D. Bobade, Mr.Amit J. Pimprikar

Department of MCA, Prof. Ram Meghe Institute of Technology & Research, Badnera, India

ABSTRACT

Security of data over the network is very important issue. Cryptography is a word with Greek origins, means "secret writing". Cryptography ensures us the data security. Cryptography is used to ensure confidentiality, integrity and availability of data by cryptographic algorithms. Encryption methods in which both the sender and receiver share the same key is referred to as symmetric key cryptography. Symmetric algorithms are again of two types block ciphers and stream ciphers. Block ciphers are commonly used. Performance of different algorithms is different according to the inputs. In this paper I have defined and analyzed various cryptographic symmetric algorithms like DES, Triple DES, AES.

Keywords: Cryptography, Symmetric key cryptography, DES, AES, Triple DES.

INTRODUCTION

Cryptography is the study of information hiding and verification. The aim of cryptography is to make it possible for two people to exchange a message in such a way that other people cannot understand the message. Encryption is the process of converting normal text to unreadable form while decryption is process of converting encrypted text in readable format. Cryptography maintains information securities such as data confidentiality, data integrity, authentication, and non-repudiation. The cryptographic systems are classified along three independent dimensions:

1. Type of operation used for transforming message.(Substitution or transposition)
2. The number of keys used.(Symmetric or asymmetric)
3. The way in which message is processed.(block or stream cipher)

The most commonly used symmetric encryption algorithms are block ciphers[1]. Block Cipher processes the plaintext input in fixed sized blocks and produces a block of cipher text of equal size for each plaintext block. In this paper three most commonly used and important block ciphers: Data Encryption Standard (DES),Triple DES(3-DES) and Advance Encryption Standard AES.

DES

DES was issued in 1977 as FIPS 46 by NIST. The algorithm is called as Data Encryption algorithm (DEA). It is a Feistel-type Substitution-Permutation Network cipher. The plaintext is divided into 64-bit blocks. The key size is 56-bits. Total 16 rounds of Feistel system is used, with an overall 56-bit key permuted into 16 48-bit subkeys, one for each round. To decrypt, the identical algorithm is used, but the order of subkeys is reversed. The 64-bit block is divided into two halves left and right each is of 32 bits. The hash function "f", specified by the standard.

Using the so-called "S-boxes", takes a 32-bit data block and one of the 48-bit subkeys as input and produces 32 bits of output. Sometimes DES is said to use a 64-bit key, but 8 of the 64 bits are used only for parity checking, so the effective key size is 56 bits.

Concerns about the strength of DES fall in two categories: about the algorithm itself and about the use of small size key. The more serious concern is key length.DES finally and definitively proved insecure in 1998.

Triple DES

Triple DES was first standardized for financial application in ANSI standard X9.17 in 1985.Triple DES was incorporated as part of the DES in 1999 with publication of FIPS 46-3. This algorithm uses

Address for correspondence:

Snehal.ulhe9@gmail.com

3 keys and 3 executions of DES. So the effective key length for 3 DES become 168 bits.It can be also performed with 2 keys in which first and third key will be same and then key length become 112 bits.

The principle drawback of 3DES is that algorithm is slow in software.

AES

The Advance Encryption Standard was developed by two researchers Dr. Vincent Rijmen and Dr. Joan Daemen and previously called as Rijndael.AES uses block size of 128 bits. The key length can be 128,192 0r 256.The input to the encryption and decryption is 128 bit block. The block is taken as square matrix of bytes. The contents are the copied into state array and this array is modified at each stage. After all operation state array is copied to output matrix. The ordering of bytes within matrix is by column. The four stages are used one of substitution and three of permutation. The stages are substitute bytes, shift rows, mix columns and add round key.[2]

COMPARISON BETWEEN AES, 3DES AND DES

Advance Encryption Standard (AES) and Triple DES are commonly used block ciphers. Whether we choose AES or 3DES depend on our needs.DES was developed to work better on hardware than software. We can compare them on basis of security and performance. For DES there are 2^{56} keys are possible, which is approximately 7.2* 10^{16} .But still it is vulnerable to brute-force attack. Therefore, DES could not keep up with advancement in technology and it is no longer appropriate for security. 3DES is a construction of applying DES three times in sequence. Two-key 3DES is widely used in electronic payments industry. 3DES takes three times as much CPU power than compare with its predecessor which is significant performance hit. AES outperforms 3DESboth in software and in hardware AES is faster in software and works efficiently in hardware[3]e. It works fast even on small devices such as smart phones; smart cards etc.AES provides more security due to larger block size and longer keys. AES is replacement for 3DES according to NIST both ciphers will coexist until the year2030 allowing for gradual transition to AES. Even though AES has theoretical advantage over 3DES for speed and efficiency in some hardware implementation3DES may be faster where support for 3DES is better. We can compare these three algorithms as follows:

Table1. *Comparison between AES,Triple DES and DES*

Criteria	DES	Triple DES	AES
Developed in	1977	1978	2000
Block Size	64-bit	64-bit	128-bit,192-bit,256-bit
Key Length	56-bit	168-bit or 112-bit	128-bit,192-bit,256-bit
Possible keys	2^{56}	2^{168} or 2^{112}	2^{128} or 2^{192} or 2^{256}
Security	Proven weak	Weak only if exit in DES	Secure
Cryptanalysis resistance	Vulnerable to differential, linear and weak substitution tables	Vulnerable to differential, Brute force attack is possible with differential cryptanalysis	Strong against differential, linear, interpolation and square attacks

CONCLUSION

In this paper a new comparative study between DES, 3DES and AES were presented according to six criteria, which are Developed year, block size, key length, possible keys, security, cryptanalysis resistance. From all these AES is better than DES and 3DES.

REFERENCES

[1] Atul Kahte "Cryptography and Network Security",2nd Ed".

[2] Gabriela Moise "A survey on the usage of substitution Tables in DES and AES algorithms" Vol.LXI No.2/2009

[3] A.A.Zaidan, B.B.Zaidan, Anas Majeed, "High Securing Cover-File of Hidden Data Using Statistical Technique and AES Encryption Algorithm", World Academy of Science Engineering and Technology (WASET), Vol.54, ISSN: 2070-3724, P.P 468-479.

[4] Gunjan Gupta , Rama Chawla " Review on Encryption Ciphers of Cryptography in Network Security" , International Journal of Advanced Research in Computer Science and Software Engineering , Volume 2, Issue 7, July 2012