Global Journal of Computer Science and Technology: H Information & Technology
Volume 17 Issue 2 Version 1.0 Year 2017
Type: Double Blind Peer Reviewed International Research Journal
Publisher: Global Journals Inc. (USA)
Online ISSN: 0975-4172 & Print ISSN: 0975-4350

Comparative Study of Symmetric Key Algorithms-Des, AES and Blowfish

By H. Fathima, K.S.R. Matriculation & K.S.R. Kalvi nagar
KSRMHSS

Abstract- This paper presents a peer analysis in the field of encryption algorithms, concentrating on private key block ciphers which are generally used for bulk data and link encryption. We have initially surveyed some of the popular and efficient algorithms currently in use. This paper focuses mainly on the different kinds of encryption techniques that are existing, and comparative study together as a literature survey. This study extends to the performance parameters used in encryption processes and analyzing on their security issues. Cryptography is the practice and study of hiding information. Prior to the modern age, cryptography was almost synonymous with encryption i.e. the conversion of information from a readable state to unreadable state. In order to avoid unwanted persons being able to read the information, senders retain the ability to decrypt the information. There are three types of Cryptography.

Keywords: encryption, decryption, cipher text, permutation, symmetric, subsitution bytes.

GJCST-H Classification: B.7.1, I.1.2

Strictly as per the compliance and regulations of:

Comparative Study of Symmetric Key Algorithms-Des, AES and Blowfish

H. Fathima [α], K.S.R. Matriculation [σ] & K.S.R. Kalvi nagar [ρ]

Abstract- This paper presents a peer analysis in the field of encryption algorithms, concentrating on private key block ciphers which are generally used for bulk data and link encryption. We have initially surveyed some of the popular and efficient algorithms currently in use. This paper focuses mainly on the different kinds of encryption techniques that are existing, and comparative study together as a literature survey. This study extends to the performance parameters used in encryption processes and analyzing on their security issues. Cryptography is the practice and study of hiding information. Prior to the modern age, cryptography was almost synonymous with encryption i.e. the conversion of information from a readable state to unreadable state. In order to avoid unwanted persons being able to read the information, senders retain the ability to decrypt the information. There are three types of Cryptography. They are Asymmetric-key cryptography, symmetric key cryptography and hashing. Encryption methods in which both the sender and receiver share the same key are referred to as symmetric key cryptography. This paper provides a comparison between symmetric key algorithms such as DES, AES, and Blowfish. The comparison is made on the basis of these parameters such as block size and key size.

Keywords: encryption, decryption, cipher text, permutation, symmetric, subsitution bytes.

I. Introduction

Symmetric-key algorithms [1] are algorithms that use the same cryptographic keys for both encryption of plaintext and decryption of cipher text. The keys may be identical or there may be a simple transformation to go between the two keys. The keys, in practice, represent a shared secret between two or more parties that can be used to maintain a private information link.[2] This requirement that both parties have access to the secret key is one of the main drawbacks of symmetric key encryption, in comparison to public-key encryption (also known as asymmetric key encryption).[3]Symmetric-key encryption can use either stream ciphers or block ciphers.[4]Stream ciphers encrypt the digits (typically bytes) of a message one at a time.

Block ciphers take a number of bits and encrypt them as a single unit, padding the plaintext so that it is a multiple of the block size. Blocks of 64 bits have been commonly used. The Advanced Encryption Standard (AES) algorithm approved by NIST in December 2001 uses 128-bit blocks.

Author α σ ρ: M.Sc (IT)., M.Phil (CS), Hss, Thokkavadi (p.o), Thiruchengode-637215.
e-mails: Fathimahussain_mscit07@rediffmail.com, Fathi.fathimahussain@gmail.com

II. Data Encryption Standard

Data Encryption standard (DES) adopted in 1997 by the National Bureau of Standards. For DES data are encrypted in 64 bit blocks using a 56- bit key. The algorithm transforms 64-bit input in a series of steps into a 64-bit output.

III. Des Encryption

There are two inputs in the encryption function: the plaintext to be encrypted and the key. In this case, the plaintext must be 64 bits in the length and the key is 56 bits in length. The 64-bit plaintext passes through an initial permutation (IP) that rearranges the bits to produce the permuted input. This is followed by a phase consisting of 16 rounds of the same function, which involves both permutation and substitution functions.

The output of the last (sixteenth) round consists of 64 bits that there are a function of the input plaintext and the key. The left and right halves of the output are swapped to produce the preoutput. Finally the preoutput is passed through a permutation (IP^{-1}) that is the inverse of the initial permutation function, to produce the 64-bit cipher text.

IV. Initial Permutation

The input to a table consists of 64 bits numbered from 1 to 64. The 64 entries in the permutation table contain a permutation of the numbers from 1 to 64. Each entry in the permutation table indicates the position of a numbered input bit in the output which also consists of 64 bits.

V. Details of Single Round

The round key Ki is 48 bits. The R input is 32 bits. This R input is first expanded to 48 bits by using a table that defines a permutation plus an expansion that involves duplication of 16 of the R bits. The resulting 48 bits are XORed with Ki. This 48 bit result passes through a substitution function that produces a 32-bit output.

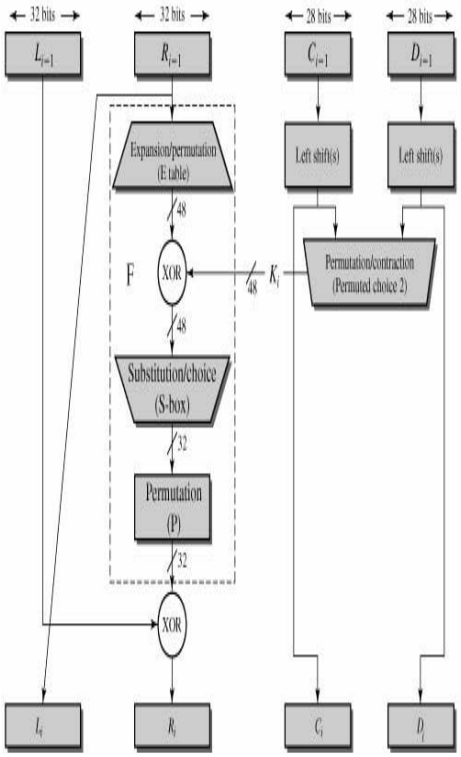


Figure 1: Single Round DES

The substitution consists of a set of eight S_ boxes, each of which accepts 6 bits as input and produces 4 bits as output. The first and last bits of the input to box Si from a 2-bit binary number to select one of four substitutions defined by the four rows in the table for Si the middle four bits select one of the sixteen columns.

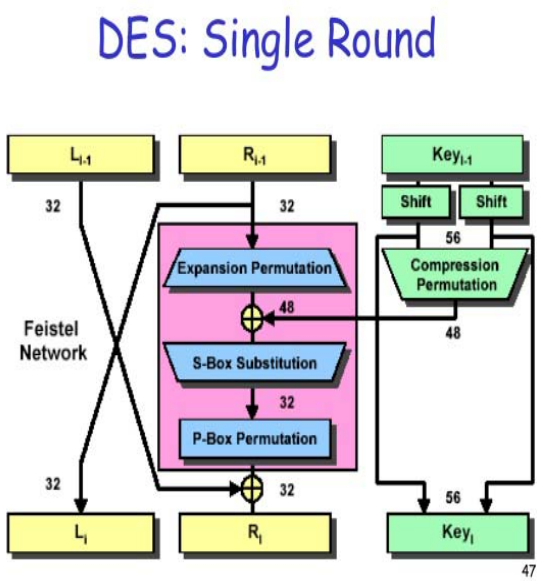


Fig 2: Single Round DES

The decimal value in the cell selected by the row and column is then converted to its 4-bit representation to produce the output. The outer two bits of each group select one of four possible substitutions (one row of an s- box). Then a 4 bit output value is substituted for the particular 4-bit input (the middle four input bits). The 32-bit output from the eight S-boxes is then permuted.

VI. Avalanche Effect

A desirable property of any encryption algorithm is that a small change in either the plaintext or the key should produce a significant change in the cipher text. I particular, a change in one bit of the plain text or one bit of the key should produce a change in many bits of the cipher text. If the change were small, this might provide a way to reduce the size of the plaintext or key space to be searched.

VII. Advanced Encryption Standard

NIST in 1997 issued a call for proposals for a new Advanced Encryption Standard (AES). NIST specified that AES must be a symmetric block cipher with a block length of 128 bits and support for key lengths of 128, 192, and 256 bits. The AES specification uses the same three key size alternatives but limits the block length to 128 bits. A number of AES parameters depend on key length. Substitute byte uses an S-box to perform a byte-by-byte substitution of the block.

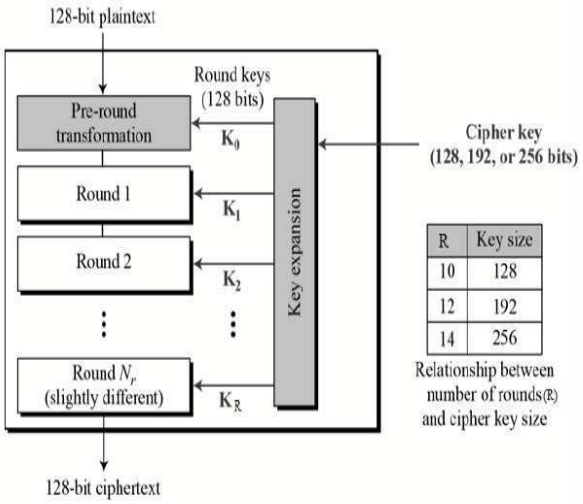


Fig 3: AES

VIII. Substitute Bytes Transformation

AES defines a 16×16 matrix of byte values called an S-box that contains a permutation of all possible 256 8-bit values. The leftmost 4 bits of the byte are used as a row value and the rightmost 4 bits are used as a column value serve as indexes into the S-box to select a unique 8-bit output value.

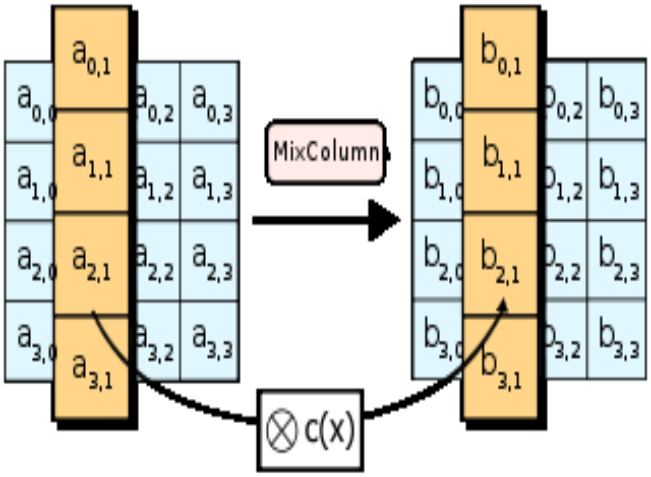


Figure 4: substitute bytes transformation

IX. Shift Row Transformation

a) Forward and Inverse transformations

The forward shift row transformation, called shift rows. The Inverse shift row transformation called Inv shift Rows, Perform the circular shifts in the opposite direction for each of the last three rows, with one- byte circular right shift for the second row.

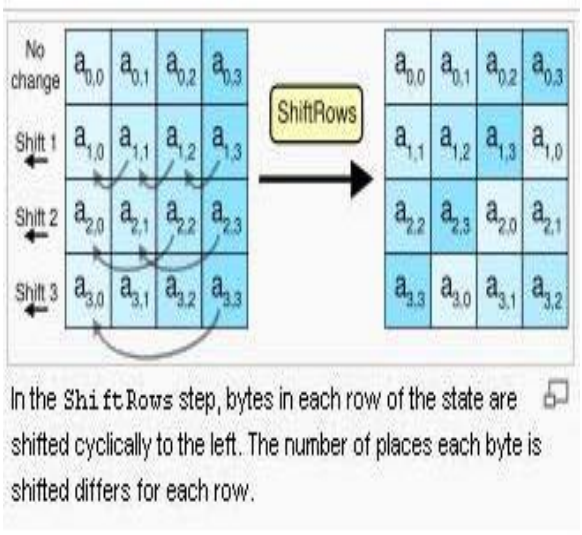


Figure 5: shift row transformation

The Forward mix column transformation, called Mix columns, operates on each column individually. Each byte of a column is a mapped into a new value that is a function of all four bytes in the column. The Inverse add round key transformation is identical to the forward add round key transformation, because the XOR operations its own inverse.

X. Blow Fish

Blowfish is a symmetric cipher developed by Bruce Schneier [SCHM93, SCHN94]. Blowfish was designed to have the following characteristics such as Fast, Compact, Simple and variably secure. The key length is variable and can be as long as 48 bits. This allows a tradeoff between higher speed and higher security.

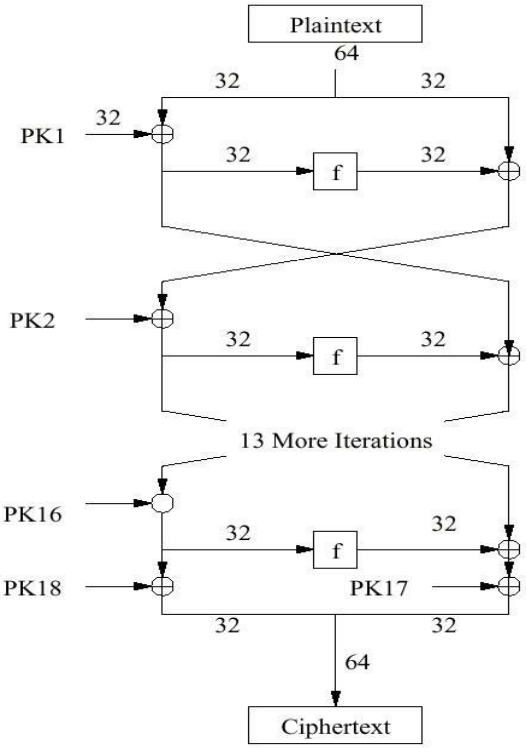


Figure 6: Blow fish

Blow fish encrypts 64-bit blocks of plaintext into 64-bit blocks of cipher text. Blowfish is implemented in numerous products and has received a fair amount of scrutiny.

XI. Encryption and Decryption

a) Blowfish uses two primitive operations

Addition: Addition of words, denoted by +, is performed by modulo 2 ^{32} .Blowfish decryption involves using the sub keys in reverse order. However, unlike most block ciphers, Blowfish decryption occurs in the same algorithmic directions as encryption, rather than the reverse.

Blowfish is a formidable symmetric cipher. Unlike DES, the S-boxes in Blowfish are key dependent. The blowfish design is that operations are performed on both halves of the data in each round, compared to performing an operation on just half the data in each round in the classic Feistel cipher. This should provide greater cryptographic strength, even though the additional operation is linear (XOR).

XII. Experimental Results

Table1: Block Size

ALGORITHM	BLOCK SIZE
DES	64
AES	128
BLOW FISH	64

Graph1: Block size

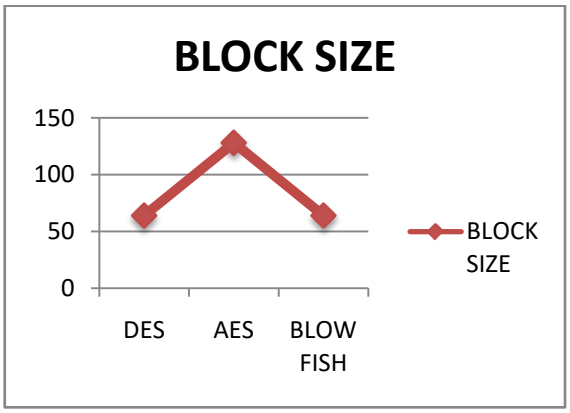
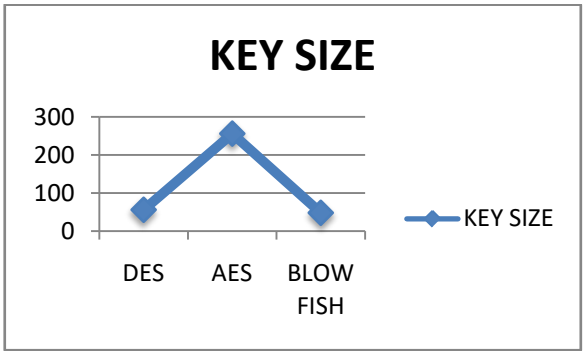


Table 1: Key Size

ALGORITHM	KEY SIZE
DES	56
AES	256
BLOW FISH	48

Graph 2: Key Size



XIII. Conclusion

This paper gives a detailed study of the popular symmetric key encryption algorithms such as DES, AES and Blowfish. Further, symmetric key encryption provides more security. This paper presents the performance evaluation of selected symmetric algorithms. From the presented simulation we can conclude that AES has better performance than other algorithms. Secondly, AES has advantage over the DES in terms of throughput & decryption time except Blowfish. In future the work may be extended by including the schemes and techniques over different types of data such as image, sound and video and developing a stronger encryption algorithm with high speed and minimum energy consumption.

References Références Referencias

1. "Cryptography: Description of a New Variable-Length Key, 64-Bit Block Cipher (Blowfish) – Schneier on Security". www.schneier.com Retrieved 2015-12-31.
2. Karthikeyan Bhargavan, Gaëtan Leurent (August 2016). "On the Practical (In-) Security of 64-bit Block Ciphers — Collision Attacks on HTTP over TLS and OpenVPN". ACM CCS 2016.
3. Schneier, Bruce (2004-09-27). "Saluting the data encryption legacy". *CNet*. Retrieved 2015-07-22.
4. *Biaoshuai Tao & Hongjun Wu (2015).* "Improving the Biclique Cryptanalysis of AES".
5. *SPIEGEL ONLINE, Hamburg, Germany (28 December 2014).* "Inside the NSA's War on Internet Security". *SPIEGEL ONLINE*. Retrieved 4 September 2015.