May-June 2020
ISSN: 0193-4120 Page No. 3873-3875

Comparison of AES, Blowfish and Twofish

[1]P V Dashika, [2]Mohammed Mannan Ali Baig, [3]Mohammed Ayub. Z, [4]Vijayalakshmi P Chiniwar

[1,2,3]MCA 4th SEM, [4]Assistant Professor
[1,2,3,4]School of CSA, REVA University,
[1]dashikapv17@gmail.com, [2]Mannanbaig98@gmail.com , [3]Ayubkhan9888@gmail.com,
[4]chiniwarvijaya@reva.edu.in

Article Info
Volume 83
Page Number: 3873-3875
Publication Issue:
May-June 2020

Article History
Article Received:*19 November 2019*
Revised: *27 January 2020*
Accepted: *24 February 2020*
Publication: *12 May 2020*

Abstract
In fast-growing population and their use of the internet is creating a huge amount of data in the form of images or files. These data, images or files need to be kept secure from unauthorized users. To secure the privacy of a file or data it has to be encrypted using Encryption Algorithms. In this paper, we tried to explore the features, advantages, and limitations of AES, Blowfish and Twofish, a general-purpose encryption algorithm and also gives a comparison between them.

Keywords: *Network Security, Cryptography, AES, Blowfish, Two fish.*

1. Introduction

Cryptography is the process to secure our data or information from an unauthorized user. Cryptography operations performed are encryption and decryption. Usually, the encryption and decryption operation are carried out by using key management.

2. Cryptography Mechanism

1. Key
2. Plain text
3. Cipher
4. Encryption
5. Decryption

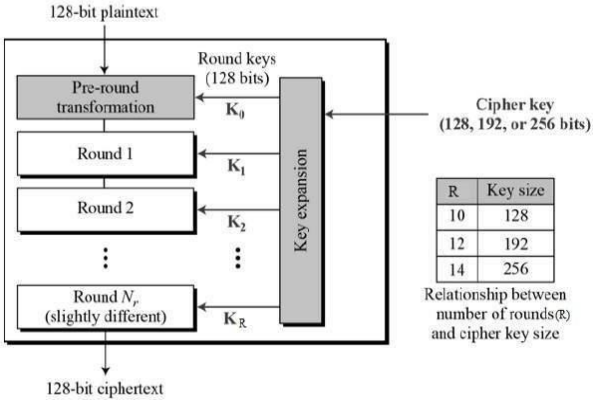
3. Advanced Encryption Standard (AES)

Here we utilize symmetric key encryption and one solitary secret key in favor of encryption and decryption. [1]

It is competent for hardware and software and sustains block length of 128bits and a key length of 128, 192 and 256bits. It is the most advanced encryption technique developed and used in recent times. **[3]**

Application of AES algorithm

- The symmetric key has 128, 192, 256-bit keys.
- It gives us the benefit to view specification and design details
- Its Encryption is more powerful than Triple-DES



R	Key size
10	128
12	192
14	256

Relationship between number of rounds(R) and cipher key size

Figure 1: AES structure

Advantage of AES

1. AES algorithm is the robust security protocol as it is implemented on hardware as well as software.
2. As it uses huge key the length is less prone to hacking.

Disadvantage of AES

1. A simple algebraic structure is used.
2. Encryption in every block is the same.

4. Blow Fish

It is a key block cipher of 64 bit, deliberated in 1993 by Bruce Schneier. It has a unpredictable key length of 32 bit to 448 bits making it more flexible and secure.

May-June 2020
ISSN: 0193-4120 Page No. 3873-3875

This algorithm being faster than DES and IDEA Encryption algorithm, used in household and exportable purpose.

It is a Feistel network or structure. Which is very efficient on large processors? Rather Initialization phase is complex. Bit generation is in random order. It is mainly used in Government agencies and are not allowed to be used by Non-Government agency hence, this algorithm has no patent. It is considered as the fastest algorithm which uses only up to 5KB Memory or even less.

Algorithm

Blowfish algorithm uses primitive operations like addition, XOP, XOR Table Lookup.
It has two sections:
a) Key Expansion
b) Data Encryption
Key extension: A key of 448 bits is made by numerous associate key arrays making a total of 4168 bits. Every surrounding encompasses key-dependent permutation and substitution. Key extension employs 18 P-array of 32 bit and 4 to 5 S-box with 256 entries each.
Data Encryption: unadorned text is being alienated into two parts of 32bit each: - XL and XR.
For i=1 to 16 do the following,
Calculate XL=XL XOR P1;
Calculate XR=F(XL) XOR XR;
Swap XL and XR;
End
Calculate XR=XR XOR P17;
Calculate XL=XL XOR P18;
Combine XL and XR // we get ciphertext. **[5]**

Application of Algorithm

- File and Disk supervision like Blow Torch
- Password Management like Password Store or Yaps
- Backup Software like LEO Backup, UBACKPro
- DB Security like SQL Server 2000
- E-Commerce Software like X-Cart, CS-Cart.
- E-Mail Encryption.

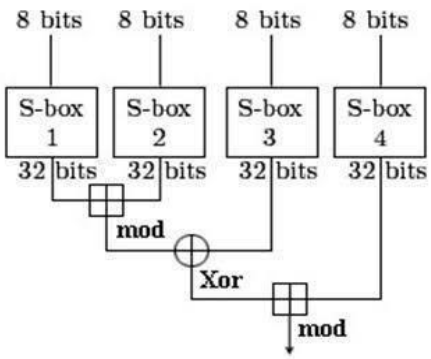


Figure 2: The Feistel structure of Blowfish

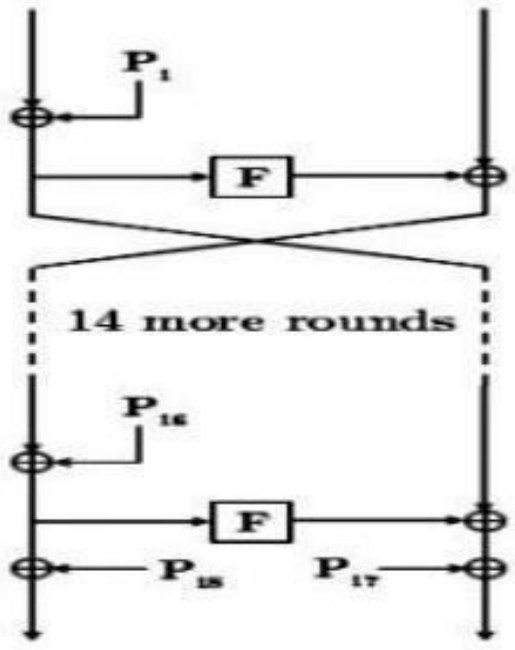


Figure 3: Blowfish Encryption Algorithm

Advantage of Blowfish

1. Blowfish algorithm generates block cipher in faster rate.
2. Blowfish algorithm is not been patented so it is a open source algorithm.

Disadvantage of Blowfish

1. Since the block size of key is less it is not suitable for security.
2. Since two people have same key there is no concept of authentication.

5. Two Fish

It is a 128-bit Symmetric block cipher and considered as a flexible and secure algorithm. Encryption and decryption process make use of solitary key. It works in a high speed in 32 bit and 8 bit CPU.
There are no weak keys used therefore it proves to be an efficient and simple designed algorithm. Pre and Post whitening is used with key-dependent S-boxes. Algorithm

Input and output is XORed with 8 subkeys K0…K7. R0 and R1 are the rounds which are passed through the function F and result are F0 and F1. In each round 64bit the word is divided into 4 bytes and send to S-boxes.

The MDS-Maximum Distance Separable matrix is pooled with 4 output bytes

The two 32bit words are packed using PHT=Pseudo Hadamard Transform which is added to 2 round subkeys then XORed with the right half of the text

There is two 1-bit rotation happening one before and one after XOR. **[10]**

.

May-June 2020
ISSN: 0193-4120 Page No. 3873-3875

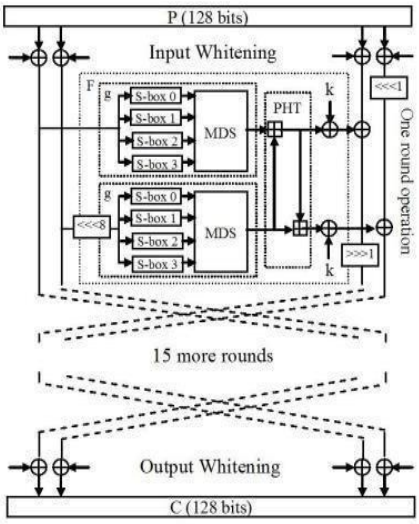


Figure 4: Two fish Encryption Algorithm

Advantage of Twofish

1. Twofish algorithm is flexible enough for tiny smartcard CPU's.
2. Speed makes it unique amongst the AES encryption algorithm.
3. Twofish screams on high-end CPUs. It also works well in hardware.
4. Twofish is the fastest AES candidate across all CPUs.

Disadvantage of Twofish

1. Twofish is comparatively slower than Rijndael for 128-bit keys.
2. The Twofish cipher has not been patented yet.
3. Twofish is being used less as compared to Blowfish.

6. Difference Between Aes, Blow Fish &Two Fish

In both 32-bit and 8-bit CPU and hardware. It is used in

Algorithm	AES	Blow Fish	Two Fish
Original text	240KB	240KB	240KB
Ciphertext	847KB	955KB	955KB
Plain text	240KB	240KB	240KB
Speed	Faster	Very Fast	Fast
Space	Less than Blowfish & Two fish	More Than AES	Same a Blowfish
Security	Excellent security	Highly secure	Secure

7. Conclusion

Encryption is a very important aspect as it allows us to secure our file, data, image and various other information. It encodes all our information in a pattern where an intermediator or trespasser would find it very difficult to find the actual information. Many encryption techniques have been evolved like blowfish, two fish, three fish, AES, Triple AES, DES and so on.

As in this paper, we have discussed the basic difference between Blowfish and two fish algorithm these both have a Feistel structure and an open-source algorithm. For text encryption two fish algorithm takes less time to encrypt than Blowfish.
Blowfish is faster than DES and never broken.

References

[1] "A Survey On Encryption Algorithms Using Modern Techniques" Venkat
[2] Prasad.K, S. Magesh.
[3] Ahmad, Md Hussain, and Manish Madhava Tripathi. "Development Of Encryption And Decryption Technique To Secure The Confidential Data." *Iijarcs,Vol (*2) (2018): 60.
[4] Singh, Gurpreet. "A study of encryption algorithms (RSA, DES, 3DES and AES) for information security." *IJCA,67(19)*- (2013).
[5] Abood, Omar G., and Shawkat K. Guirguis. "A survey on cryptography algorithms." *IJSRP, Vol.8(7)*- (2018).
[6] Rajesh, Sreeja, Varghese Paul, Varun G. Menon, and Mohammad R. Khosravi. "A secure and efficient lightweight symmetric encryption scheme for transfer of text files between embedded IoT devices." *Symmetry* 11, no. 2 (2019): 293.