BLOWFISH

CS 608 Algorithms

Professor Altion Simo

Samarth Venkatesh Gowda

ABSTRACT

Online communication system are one of the most reliable and fastest mode of communication available for the common people. There are lots of different algorithms that have helped in encrypting the data to secure them from various attacks. This paper explore the working and characteristics of the blowfish algorithm based on real time situations around the world. it is hoped that this paper would contribute the improve the overall condition of the online communication system.

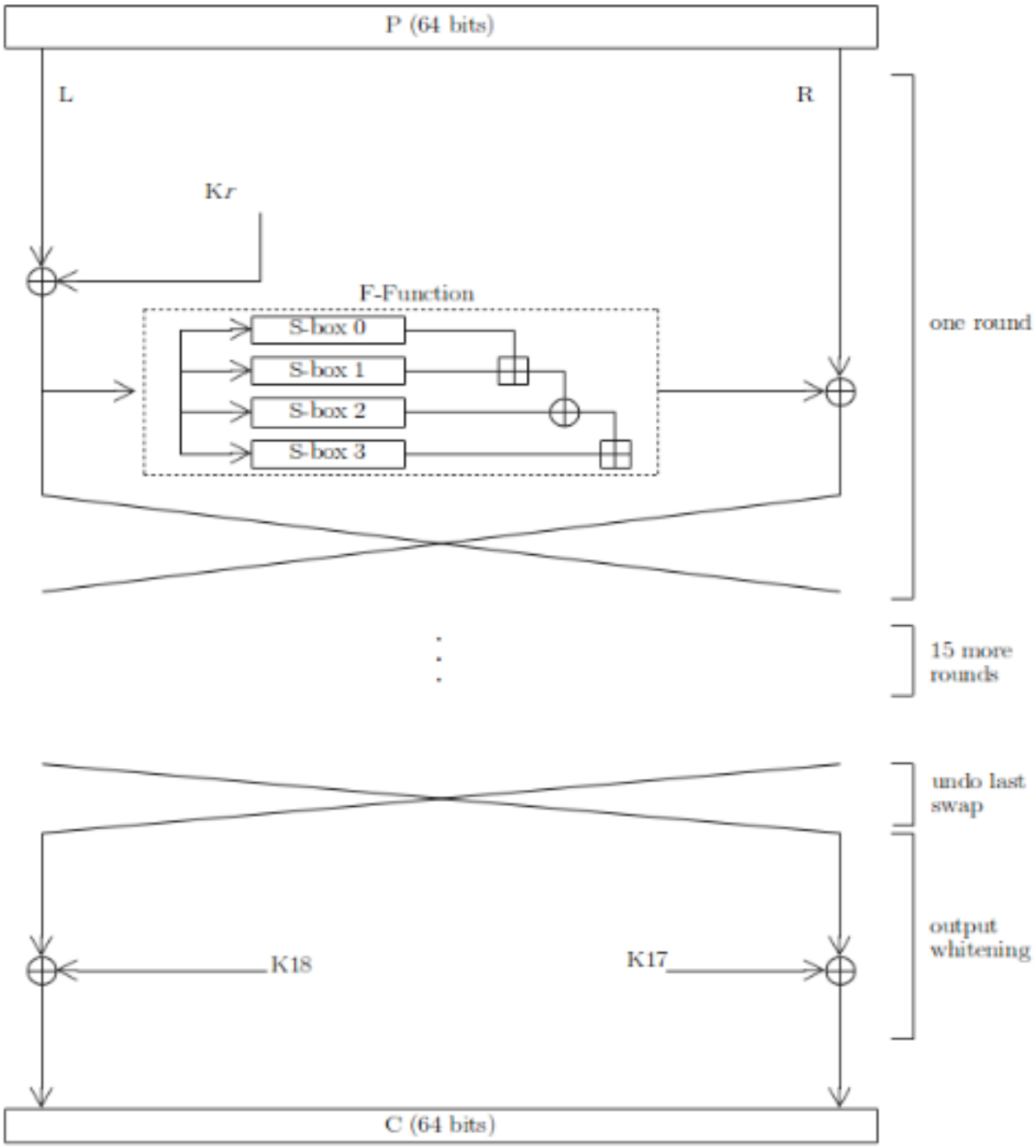
Introduction

Blowfish is a symmetric key encryption algorithm developed by Bruce Schneier in 1993, It was designed as a improvised version to replace the DES encryption algorithm. It is one of the best first, secure block ciphers without no effective cryptanalysis technique found till date. Blowfish is not subjected to any patent hence it is easily available for anyone to use. (Bruce Schneier,1993).

Description of the Blowfish Algorithm

Blowfish is a block cipher that encrypts 64 bit block size(8 bytes) with a variable key length from 32 bits to 448 bits. the algorithm is divided into two parts: Sub-key generation and Data encryption. Blowfish has a 16 round feistel cipher structure and utilizes large key-dependent S-boxes(Youssouf Mahamat koukou, 2016).

The below diagram provides the working of the blowfish encryption routine. each line in the diagram represents 32 bits, they also have different arrays involved such as P-arrays initialized with digits of pi and four 256 entry S-boxes(s0,s1,s2,s3).



Structure of Blowfish Algorithm

Each round (r) consists of four actions in the blowfish algorithm:

1. Action 1: Left half (L) of the information is XOR with the *r* th P- array entry.
2. Action 2: Utilize the XORed information as input to the blowfish F- function.
3. Action 3: F-function's output is XOR with the right half(R) of the data.
4. Action 4: Swap Left(L) and Right(R).

The function F breaks the 32 bits input into four eight bit quarters and use each quarter as input to the S-boxes. The S-boxes take 8-bits as input and produce 32 bit ouput, this output are added with modular arithmetic and XORed to produce the final 32 bit result(Bruce Schneier,1993) . After the sixteenth round, the left is XORed with K18 and right part is XORed with K17.

Generation of Sub-keys

The blowfish algorithm uses 18 sub-keys for both encryption and decryption processes and these sub-keys are stored in a P-array with each array element of 32-bit entry size and they are initialized with the hexadecimal digits of Pi.

Initialization of S-boxes

The blowfish algorithm has four S-boxes which are required for encryption and decryption process and each of the S-boxes have 256 entries, where each entry is

32-bit. finally these S-boxes are initialized with hexadecimal digits of Pi after assigning the P-array.

Analysis of Blowfish Algorithm (Big-*O*)

Blowfish algorithm works on a fixed block size and it takes approximately the same time independently of input, therefore the blowfish time complexity is $O(1)$. Blowfish is also known for its quite slow key schedule, but it is still $O(1)$.

Blowfish, DES, CAST and AES Encryption Algorithm Comparison

Blowfish is a 16-round fiestel structure and it is largely dependent on the S-boxes(Youssouf Mahamat koukou, 2016). The structure of CAST-128 is nearly similar to blowfish, which uses stable s-boxes. Cast-128 is remarkably faster than DES. Blowfish is unpatented, open source and available free to all the users. CAST-128 is similar to DES and it uses a 128-256 bit key structure(Youssouf Mahamat koukou, 2016). Cast-128 is less secure than DES but it is quicker than Blowfish and DES.

FACTORS	CAST-128	DES	BLOWFISH	AES
Key length	128-bits	56 bits	448 bits	128 bits

Cipher Type	Symmetric Block Cipher	Symmetric Block Cipher	Symmetric Block Cipher	Symmetric Block Cipher
Block Size	64 bits	64 bits	64 bits	128 bits
Developed	1996	IBM in 1975	1993	2000
Speed	Fast	Slow	Fast	Fast
Security	Less secure	Not secure enough	Secure enough	Excellent security
Structure	Feistel structure	Feistel structure	Feistel structure	Substitution-permutation network
Number of rounds	12	16	16	10
Number of S-boxes	4	8	4	1

source: (Youssouf Mahamat koukou, 2016)

The encryption performance of these four algorithms is stronger and faster than the DES algorithm which has the lowest speed compared to others because of the largest size of the four major algorithms mentioned above has been given a fastest and strongest speed level compared to DES.

Application of Blowfish Algorithm

The following are the applications that uses Blowfish Encryption:

1. AEdit : A free Windows word processor incorporating text encryption.
2. Coolfish: A free Windows encrypting text editor.
3. Foopchat: Uses a client/server architecture for sharing files and encrypted chat.
4. JFile : A database program for the PalmOS platform.
5. Freedom : Privacy for web browsing, e-mail, chat, telnet, and newsgroups.
6. Access Manager : A password manager for Windows.
7. AEdit: A windows word processor with data encryption incorporated.

Conclusion

The proposed blowfish algorithm is a variable- length key block cipher and this algorithm is mainly used where there is strong communication link and where the key will not be changed frequently. Blowfish is quicker than DES. It is a 16 pass block encryption algorithm that is hard to be broken.

References

Youssouf Mahamat koukou, Siti Hajar Othman, Maheyzah MD Siraj. Herve Nkiama. Comparative Study Of AES, Blowfish, CAST-128 And DES Encryption Algorithm. Retrieved: 06 February 2016 from https://pdfs.semanticscholar.org/7af1/ac803d2ba5a2a9b419eb41974811c8fcf558.pdf

Bruce Schneier**.** Description of a New Variable-Length Key, 64-Bit Block Cipher (Blowfish). Retrived: December 1993 from **https://www.schneier.com/academic/archives/1994/09/description_of_a_new.html**