A COMBINED APPROACH USING TRIPLE DES AND BLOWFISH RESEARCH AREA: COMPUTER SCIENCE (CRYPTOGRAPHY)

Shreya Singh

singh_shreya@yahoo.com

Abstract

In this paper we study about the triple DES algorithm along with the blowfish algorithm. This is a combined approach and is aimed at improving their individual performances. Then this is briefly compared to the advanced encryption standard;

***Keywords**:-DES, Blowfish, TDES, AES.*

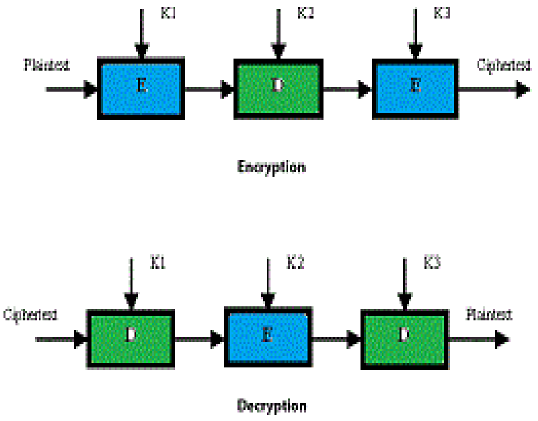
---***---

1. INTRODUCTION

There are two ways of communication possible cryptographically. One is by the use of the public key system. Here two different keys are used for encryption and decryption. The three main forms of public key systems are public key distribution systems, digital signature systems, and public key cryptosystems, which can perform both public key distribution and digital signature services. In a Public-key cryptographic system, two keys are required. One is a secret key and the other one is a public key. The second method is the use of symmetric key cryptography. Here the same key is used for both the encryption and the decryption. These are a class of algorithms which are used for cryptography. In the case of public key cryptosystem two different keys were being used for the process of encryption and decryption. In symmetric key cryptosystem we use the same cryptographic keys for both encryption of the plaintext and decryption of the cipher text. Symmetric encryption is a faster procedure. DES is one algorithm which have been widely used for the encryption of data. It was developed in 1975 by IBM. It is now considered insecure. Another variant of the DES was developed later known as the triple DES which is considered to be more secure in nature. Though nowadays the AES is in use instead of DES. AES is a symmetric block cipher with a block size of 128 bits. Key lengths can be 128 bits, 192 bits, or 256 bits; 8 called AES-128, AES-192, and AES-256, respectively. AES-128 uses 10 rounds, AES-192 uses 12 rounds, and AES-256 uses 14 rounds. Blowfish has a 64-bit block size and a key length of anywhere from 32 bits to 448 bits. It is a 16-round Feistel cipher and uses large key-dependent S-boxes. It is similar in structure to CAST-128, which uses fixed S-boxes. Blowfish is not subject to any patents and is therefore freely available for anyone to use. This has contributed to its popularity in cryptographic software. Blowfish is one of the fastest block ciphers in widespread use, except when changing keys. Each new key requires pre-processing equivalent to encrypting about 4 kilobytes of text, which is very slow compared to other block ciphers.

2. DES

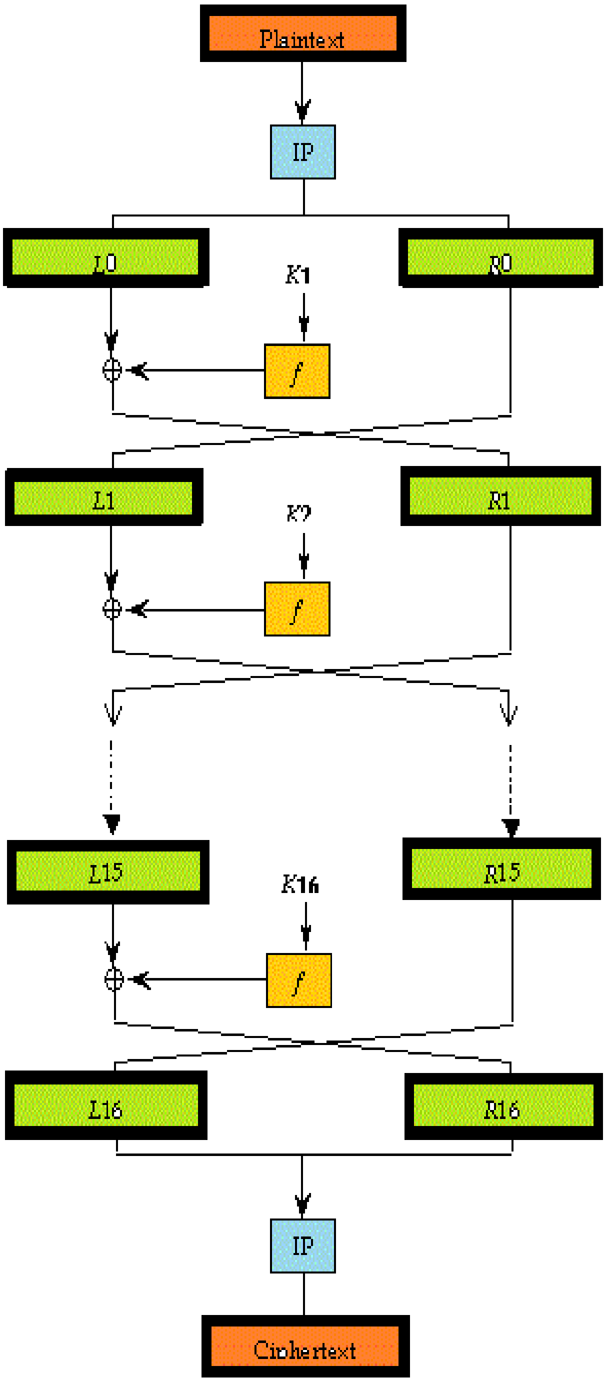
In DES the block cipher was used 64 bits at a time. The initial permutation rearranges 64 bits. The encoding was done in 16 rounds.



The 64 bits were divided into left, right halves. The right half goes through function f, mixed with the key. The right half was added to the left half. Then these halves were swapped. The right side was then expanded from 32 to 48 bits and the 48 bits of key were added. In the S-boxes, the set of 6 was reduced to 4. The P-box then permutes 32 bits.

Eight bits are used only for checking parity. These are later discarded. Thus the effective key length is 56 bits.
Three modes of operations are present. They are:

- ECB
- CBC
- OFB



In the electronic CodeBook mode each 64-bit block is encrypted independently. This is prone to attacks as the attacker can easily build the CodeBook. In the Cipher Block Chaining mode the encryption and decryption as carried as follows:

- Encryption: Ci = EK(Pi Ci-1)
- Decryption: Pi = Ci-1   DK(Ci)

The OFB mode allows byte-wise encryption.

3. TRIPLE DES

Triple DES is also known as the Triple Data Encryption Algorithm block cipher. Here the DES cipher algorithm is applied thrice. This is done to each data block. Triples DES increases the key size of DES and thus provides improved protection against attacks. The algorithm is described as follows:

Triple DES uses a "key bundle" which comprises three DES keys. These are K1, K2 and K3. Each comprise of 56 bits. The encryption algorithm is:

- ciphertext = EK3(DK2(EK1(plaintext))), DES encrypt with K1, DES decrypt with K2, then DES encrypt with K3.

Decryption is the reverse:

- plaintext = DK1(EK2(DK3(ciphertext)))that is , decrypt with K3, encrypt with K2, then decrypt with K1.

Each triple encryption encrypts one block of 64 bits of data. In each case the middle operation is the reverse of the first and last. This improves the strength of the algorithm when using keying option 2, and provides backward compatibility with DES with keying option 3. The three keying options are :

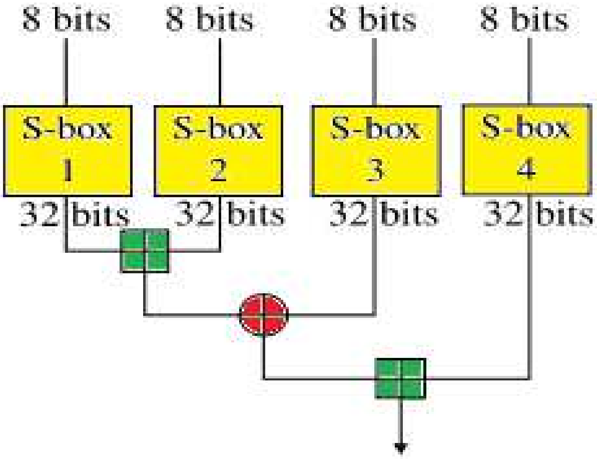
- Keying option 1: All three keys are independent.
- Keying option 2: K1 and K2 are independent, and K3 = K1.
- Keying option 3: All three keys are identical, i.e. K1 = K2 = K3.

Keying option 1 has a key length of 168 bits consisting of three 56-bit DES keys. One of the known attack is the meet in the middle attack due to which option 1 can only provide 112 bits security. Keying option 2 reduces the key size to 112 bits. Again this option is prone to certain chosen-plaintext or known-plaintext attacks. It thus provides us with only 80 bits of security.

4. BLOWFISH

Blowfish is a symmetric block cipher that can be used for encryption and protection of data. It takes a variable-length key, from 32 bits to 448 bits. Blowfish was designed in 1993 by Bruce Schneier. It is suitable for applications where the key does not change often. . The block size is 64 bits, and the key can be any length up to 448 bits. Data encryption occurs via a 16-round Feistel network. Each round consists of a key dependent permutation, and a key- and data-dependent substitution. All operations are XORs and additions on 32-bit words. The only additional operations are four indexed array data lookups per round. Blowfish has 16 rounds. There are four 32-bit S-boxes with 256 entries each:

S1,0, S1,1,..., S1,255;
S2,0, S2,1,..,, S2,255;
S3,0, S3,1,..., S3,255;
S4,0, S4,1,..,, S4,255.

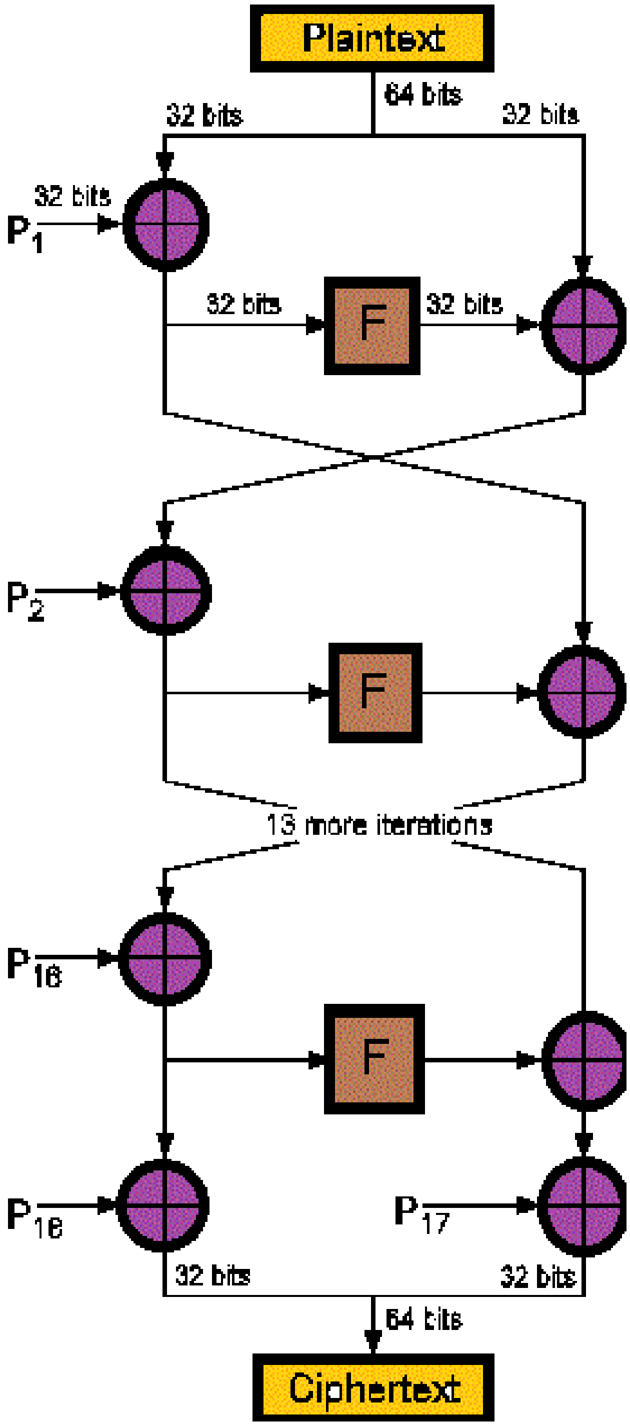


The subkeys are generated in the following manner:

1. Initialize first the P-array and then the four S-boxes, in order, with a fixed string. This string consists of the hexadecimal digits of pi.
2. XOR P1 with the first 32 bits of the key, XOR P2 with the second 32-bits of the key, and so on for all bits of the key (possibly up to P14). Repeatedly cycle through the key bits until the entire P-array has been XORed with key bits.
3. Encrypt the all-zero string with the Blowfish algorithm, using the subkeys described in steps (1) and (2).
4. Replace P1 and P2 with the output of step (3).
5. Encrypt the output of step (3) using the Blowfish algorithm with the modified subkeys.
6. Replace P3 and P4 with the output of step (5).
7. Continue the process, replacing all entries of the P array, and then all four S-boxes in order, with the output of the continuously changing Blowfish algorithm.

Encryption is done in this way:

- The input is a 64-bit data element, x.
- Divide x into two 32-bit halves: xL, xR.
- Then, for i = 1 to 16:
- xL = xL XOR Pi
- xR = F(xL) XOR xR
- Swap xL and xR
- After the sixteenth round, swap xL and xR again to undo the last swap.
- Then, xR = xR XOR P17 and xL = xL XOR P18.
- Finally, recombine xL and xR to get the ciphertext.

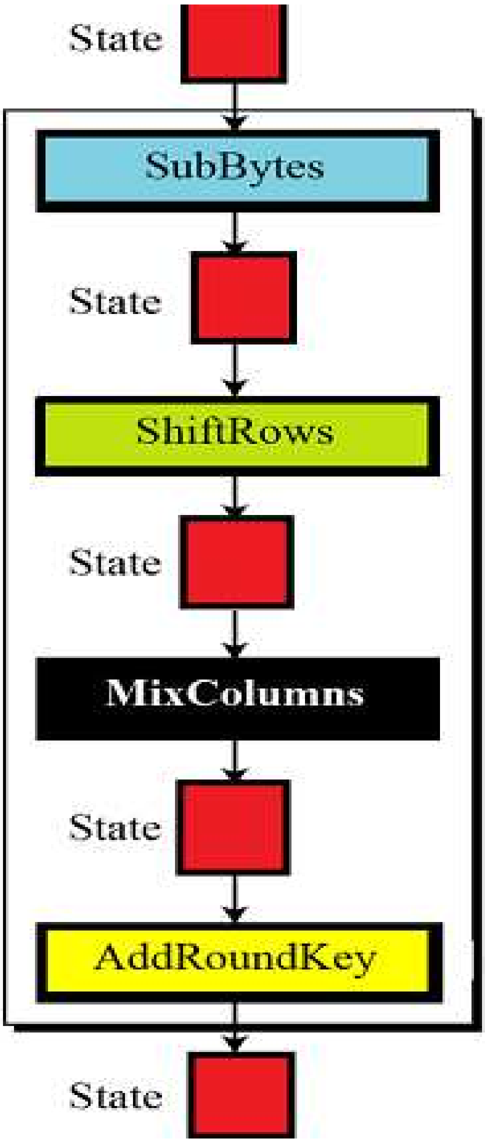


5. COMPARISON WITH AES

The Advanced Encryption Standard (AES) is a symmetric-key block cipher published by the National Institute of Standards and Technology (NIST) in December 2001. AES has defined three versions, with 10, 12, and 14 rounds. It was similar to DES: block cipher (with different modes), but 128-bit blocks 128-bit, 192-bit, or 256-bit key, Mix of permutations, "S-boxes". These S-boxes were based on modular arithmetic with polynomials. Each version uses a different cipher key size (128, 192, or 256), but the round keys are always 128 bits. AES, like DES, uses substitution. AES uses two invertible transformations. The first transformation, SubBytes, is used at the encryption site. To substitute a byte, we interpret the byte as two hexadecimal digits.

- Step 1: ByteSub Transformation
- Step 2: ShiftRow Transformation
- Step 3: MixColumn Transformation
- Step 4: Round Key Addition

Final round is a little different because it removes the MixColumns step.



Each byte of the block is replaced by its substitute in an S-box. Each byte is treated independently and single S-box is used for the entire state. Each row of the state is shifted cyclically a certain number of steps. State columns are treated as polynomials over GF(28). Each column is multiplied by modulo x4 + 1 by a fixed polynomial c(x) = `03` x3 + `01` x2 + `01`x + `02`. It has been shown Rijndael can be written as an over defined system of multivariate quadratic equations. Assuming that one could build a machine that could recover a DES key in a second (i.e., try 255 keys per second), then it would take that machine approximately 149 trillion years to crack a 128-bit AES key.

CONCLUSIONS

DES was prone to attacks and the triple DES standard was considered slow. The blowfish algorithm when combined with the triple DES algorithm would provide a better algorithm. It would be less prone to attacks. Triple DES would provide it with security and the blowfish algorithm will add to the speed of the algorithm.

REFERENCES

[1] William Stallings “Cryptography and Network Security”,3rd Edition, Prentice-Hall Inc., 2005.

[2] A study of DES and Blowfish encryption algorithm, Tingyuan Nie ; Commun. & Electron. Eng. Inst., Qingdao Technol. Univ., Qingdao, China ; Teng Zhang.

[3] Performance Evaluation of DES and Blowfish Algorithms, Tingyuan Nie ; Commun. & Electron. Eng. Inst., Qingdao Technol. Univ., Qingdao, China ; Chuanwang Song ; Xulong Zhi.

[4] A proposed mode for triple-DES encryption, Coppersmith, D. ; IBM Research Division, Thomas J. Watson Research Center, P.O. Box 218, Yorktown Heights, New York 10598, USA ; Johnson, D.B. ; Matyas, S.M.

[5] Integrated design of AES (Advanced Encryption Standard) encrypter and decrypter, Chih-Chung Lu ; Internet Platform Application Dept., Ind. Technol. Res. Inst., Hsinchu, Taiwan ; Shau-Yin Tseng.