UNIVERSITI TEKNOLOGI MARA

CRYPTOGRAPHIC BLOCK CIPHER ALGORITHM BLOWFISH

COURSE	:	CSC796 – WEB INFORMATION SECURITY
STUDENT NAME	:	SITI SYAHIRAH BT IBRAHIM & TEAM
LECTURER	:	ASSOC. PROF. TS. DR. SURIYANI ARIFFIN
SUBMISSION	:	18 JANUARY 2021

ORIGINAL BLOWFISH

Blowfish design in 1993 by Bruce Schneier as a fast and free encryption algorithm and through numerous updates, it has becomes one of the strongest encryption algorithm available. Blowfish is a 64 bit block cipher, based algorithm on Fiestal rounds, and F-funtion design it has use simplified DES which provided same strength of securitu with better speed. These are the main characteristic of Blowfish algorithm.

- blockSize: 64-bits
- keySize: 32-bits to 448-bits variable size
- number of subkeys: 18 [P-array]
- number of rounds: 16 Fiestal netwrok
- number of subsitution boxes: 4 [each having 512 entries of 32-bits each]
- consist of two part: key-expansion and data encryption.
- key expansion converts key at most 448 bits into several subkeys which totals 4168 bytes.

Image below shows structure of Blowfish algorithm.

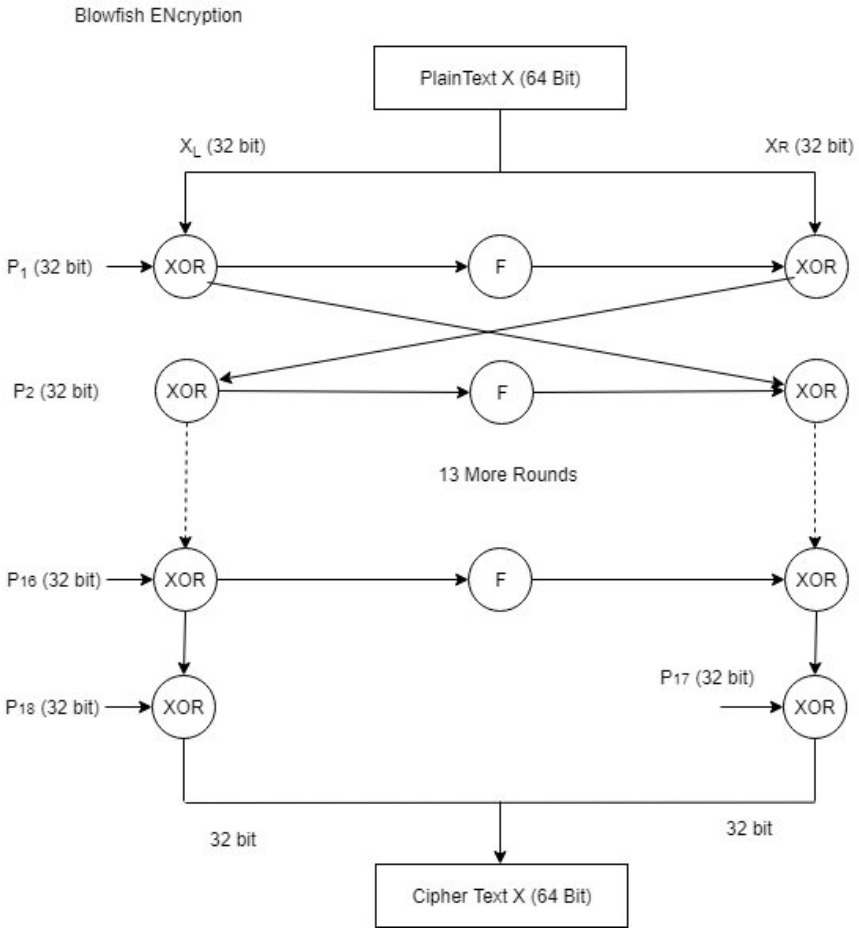

Figure 1 Blowfish algorithm architecture

Blowfish Algorithm Process:

1. Divide Plaintext X into two blocks XL and XR of equal sizes. Thus both XL and XR will consist of 32 bit each
2. For i=1 to 16

   XL = XL ⊕ PiPi

   XR = f(XL) ⊕ XR

   Swap XL ,XR

   (undo last swap)

1. XR = XR ⊕ P17P17
2. XL = XL ⊕ P18P18
3. Concatenate XL and XR back into X to get ciphertext CT

The F function uses the substitution boxes of which there are four, each containing 256 32-bit entries. If the block XL is divided into 8-bit blocks a, b, c and d, the function F(XL) is given by the formula:

F(XL)= ((S1,a + S2,b mod 2^32) S3,c) + S4,d mod 2^32.

The decryption process is just reverse of the encryption process.

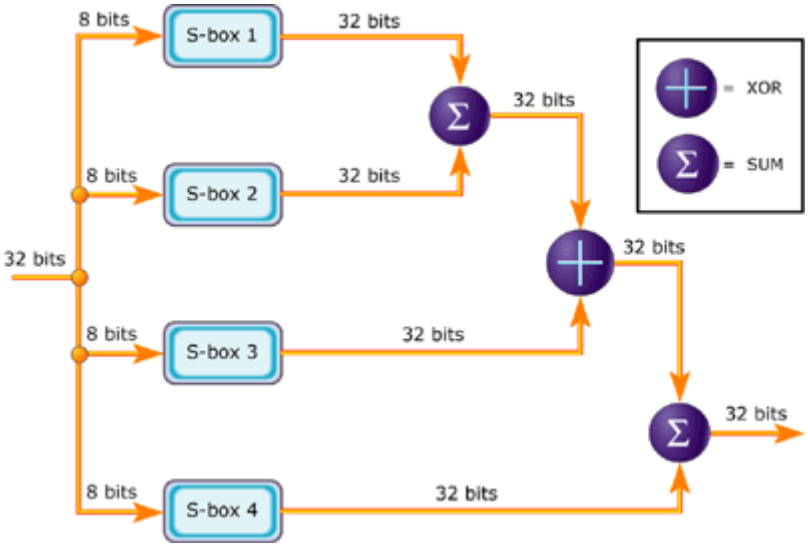

Figure 2 F-function of Blowfish Algorithm

Numerous study had been done in improving the blowfish algorithm. Research done shows that one of the methods in modifying blowfish algorithm is exchange if truth table position. Next chapter will discuss on the modification occurs.

MODIFIED BLOWFISH

One of the method of modification is changing truth table position. In original blowfish algorithm the structure of truth table is SUM, XOR, SUM. Our proposed modification is XOR, SUM, XOR. The Modified Blowfish Algorithm was successfully implemented in Python language as we only understand the python language. The number of rounds was still the same as the original version. This modification has been done in (1) research when comparing different cases of blowfish modification. Our modification was made in F-function, which was performed in figure 3 below:

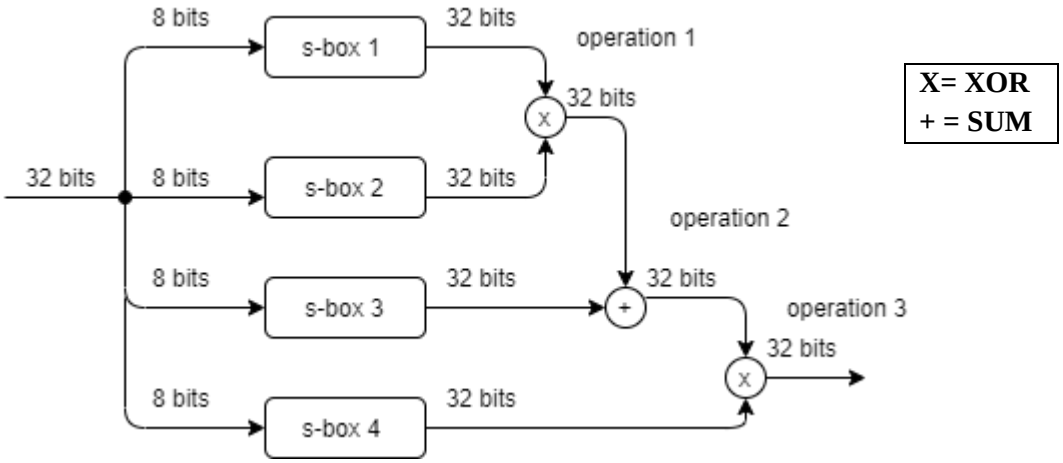

Figure 3 S-box modification in f-function

We modified the original blowfish algorithm with two XOR operation and one ADD operation in the f function. Specifically, in F function, the function divided 32-bit key into four s-box . Then the XOR and ADD function can be described as :

Operation 1: S-box 1 was XOR with S-box 2

Operation 2: Operation 1 was ADD to S-box 3

Operation 3 : Operation 2 was XOR with S-box 4

The operation still occurs in 3 steps and 16 iterations, which is the same as the original blowfish algorithm. In term of the coefficient correlation test, the smallest value is the best value as the correlation measure the dependency of output bit and input bit. The coefficient correlation also measures the

$$r = \frac{\sum (x_i - \bar{x})(y_i - \bar{y})}{\sqrt{\sum (x_i - \bar{x})^2 \sum (y_i - \bar{y})^2}}$$

r = correlation coefficient
x_i = values of the x-variable in a sample
$\bar{x}$ = mean of the values of the x-variable
y_i = values of the y-variable in a sample
$\bar{y}$ = mean of the values of the y-variable

Figure 4 Formula of coefficient correlation from Pearson

clueless chipper text. The coefficient correlation formula that we used in this project is shown in figure ?.

RESULTS

Testing is crucial parts in any software development especially cryptographic algorithm. In this project, we analyse and compare the original blowfish algorithm and modified blowfish algorithm based on Correlation Coefficient Test and Bit Error Test. The input is 50 sequence of 64 bits plaintext with a variable key size of 32 bit. The 50 plaintext were generated randomly.

Correlation coefficient is a statistical measure of the strength of the relationship between the relative movements of two variables. The values range between -1.0 and 1.0. Below table shows the results of original blowfish and modified algorithm.

Correlation Coefficient	
Original Blowfish	Modified Blowfish
0.17911745545913732.	0.11569352396922604

Figure 5 Result Correlation Coefficient

The table shows that the modified blowfish has lower correlation coefficient. A correlation value closest to -1 or 1, shows that it has stronger relationship.

Bit error rate used to recognize the value of bits changes in cyphertext. The bit error rate's value must be high to increase the confusion of cyphertext, which means it will be more secure. Table below shows the results of original blowfish and modified algorithm.

Bit Error Rate	
Original Blowfish	Modified Blowfish
0.007777622767857143	0.007732780612244898

Figure 6 Result Bit Error Rate

As we can see the modified bit error rate is lower than the original value, which indicates that the confusion rate of our modified algorithm also lower.

CONCLUSION

In conclusion, there are numerous methods of modifying a blowfish algorithm as it has endless possibility ahead. This project had been a success as the modified blowfish has better correlation coefficient and bit error rate values.