International Journal of Innovative Technology and Exploring Engineering (IJITEE)
ISSN: 2278-3075 (Online), Volume-11 Issue-10, September 2022

Three Fish Algorithm: T-Mix Cipher using SHA-256

S Shajarin, P Leelavathi, B Reddaiah, G Amrutha Vani, C Swetha

Abstract*: In every organization, use of online services is increasing. With this the sensitive data is carried over internet on daily basis. Hence, there is a chance of misleading the data by unauthorized parties. So, there is need to provide security for that data and cryptography is the science that helps in providing security. By using cryptography ddifferent types of security algorithms have been developed. Three fish is a symmetric-key and tweakable block cipher algorithm designed as a part of the skein hash function. The strength of three fish encryption relies on 128-bit tweak value. The proposed work focuses on strengthening Encryption Process by implementing tweak buffer along with input. Whereas key scheduling is secured by applying SHA-256 algorithm. SHA-256 is a secured hash function which belongs to SHA-2 family. Three Fish is used in providing security on software and hardware. It is also implemented in electronic media such as transactions like banking.

Keywords: Three Fish Block Cipher Algorithm, Symmetric Keys, Tweakable Block Cipher, Electronic Media.

I. INTRODUCTION

Security becomes prior in every platform. Now-a-days confidential data is being stolen by the intruders from different sectors like banking, digital money fraudulent through online gaming, Betting Applications and so on. Sensitive data is required to be transmitted in an inexplicable form by the intruders [4]. The major issue of end user experiencing is to enter their personal details in any kind of websites. Cryptography is the Science used for the purpose of providing security. By the help of cryptographic techniques, our data is getting secured. Cryptography is derived from the Greek words which means "Secret Writing".

Blowfish is one of the encryption algorithms intended for providing security. The Blowfish works on 64-bit block size. The key size [2] of the Blowfish Algorithm uses 32-bits to 448-bits. There are 16 rounds and four number of substitution boxes of 512 entries (each of 32-bits). Blowfish generates 18 Subkeys for encryption. The steps that are involved in the Blowfish Algorithm [2] are Sub Key Generation, Initialization of Substitution Boxes and Encryption. Encryption process mainly involves Rounds and Post Processing. The major drawback of Blowfish is it is limited to 64-bit size only and the key generation of Blowfish is time consuming. On considering the drawbacks of Blowfish, it is replaced with two fish. Two fish is an encryption algorithm [3] which is a symmetric block cipher. The block size of two fish is 128-bits and the key size is up to 256-bits. There are 16 rounds in two fish. The building blocks of two fish are Feistel Network, S-Boxes, MDS Matrix, Pseudo-Hadamard Transform, Whitening and Key Scheduling [3]. The major drawback of two fish is key dependent S-boxes. Three Fish is a tweakable[1] block cipher. The block size and the key size of three fish are same which is of 256,512 or 1024-bits. There are 72 number of rounds[3] for 256 and 512-bit block cipher and 80 number of rounds for 1024-bit block cipher. Threefish, however, is still not commonly applied on image encryption. Most of the studies used Threefish block cipher focused on hardware implementation on FPGA [7] [8] [9] [10]. Three fish uses tweak values which gives strength to the algorithm. In traditional model, tweak values are added to the key scheduling, whereas in the proposed model the tweak values are added in the encryption.

II. LITERATURE SURVEY

"Ahmed S. Nori, Ansam O. Abdulmajeed" in 2021, designed and implemented Threefish block cipher on grayscale images by applying the encryption just on the 2^n most significant bits of image pixels. It is to reduce time and the amount of data to be encrypted while maintaining encryption performance. Their proposed method shows the resistance of statistical analysis. More than one study has examined the performance of different block cipher algorithms based on various parameters [5] [6].

"Litty.P. Oommen, Anas A S" in 2015, shown Skein is good replacement of SHA family". It is efficient for both hardware and software platforms. It can be built using Threefish block Cipher. "V.Vijaya, Ramavath. Anusaria, N. Surya" in 2017, designed and implemented Threefish Cipher Block using FPGA. There is reduction of time complexity for 256-bits when compared to 128-bits of Advanced Encryption Standard. The length of the key can be reduced by keeping the same security in order to optimize the utilization of resources.

Manuscript received on 23 August 2022 | Revised Manuscript received on 30 August 2022 | Manuscript Accepted on 15 September 2022 | Manuscript published on 30 September 2022.
***Correspondence Author
S. Shajarin*, Department of Computer Science and Technology, Yogi Vemana University, Kadapa (A.P), India. Email: shajarinshaik3105@gmail.com
P. Leelavathi, Department of Computer Science and Technology, Yogi Vemana University, Kadapa (A.P), India. Email: leelapeddaputha180@gmail.com
B. Reddaiah, Department of Computer Science and Technology, Yogi Vemana University, Kadapa (A.P), India. Email: b.reddaiah@yogivemanauniversity.ac.in
G. Amrutha Vani, Department of Computer Science and Technology, Yogi Vemana University, Kadapa (A.P), India. Email:amruthagodina@gmail.com
C. Swetha, Department of Computer Science and Technology, Yogi Vemana University, Kadapa (A.P), India. Email: reddyswetha95@gmail.com

"P.Gayathri, Kana Sateesh, Cherukupalli Navya" in 2015, proposed a High-Throughput Hardware Implementation of Three Fish Block Cipher on FPGA. The technique by which the algorithm has been implemented by using Verilog HDL has reduced the time. The improvement has been observed and found better as compared to classical DES technique.

III. PRELIMINARIES

A. Threefish

Threefish is a symmetric-key encryption algorithm. The block size of the Threefish [1] is 256, 512 or 1024 bits. The key size is equal to the block size. This algorithm uses 128-bits tweak value. The block diagram of three fish is depicted in figure 1. The operations in the algorithm uses modulus addition, bitwise Exclusive-OR, and bit rotation. There are 72 rounds for 256 and 512 bits block size and for 1024-bits 80 rounds. Threefish works on 64-bits which means the plain text is divided into N_w words of 64-bits.

B. Key Scheduling

In key scheduling, the inputs are key(K-Buffer) and tweak values(T-Buffer). The key and the tweak values operate to generate 19 subkeys (Nr/4) by using the constant [1] value C_{240}=1BD11BDAA9FC1A22.

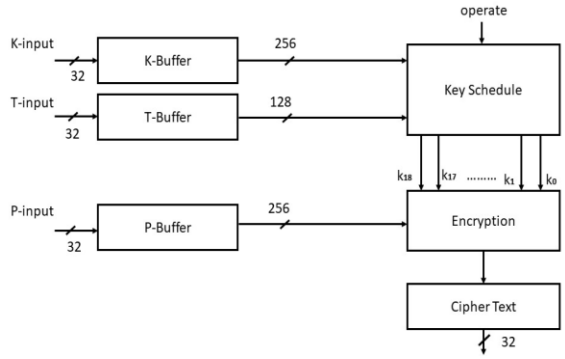

Fig.1. Block Diagram of Threefish

C. Encryption

The encryption process of Threefish is done by adding the plain text with the first subkey generated in key scheduling. Each subkey is used for every four rounds. The plaintext is of 64-bit words. After adding the subkeys to the plaintext, the round of the algorithm starts by performing mix operation and permutation. It is clearly described in figure 2. This will repeat for every four rounds.

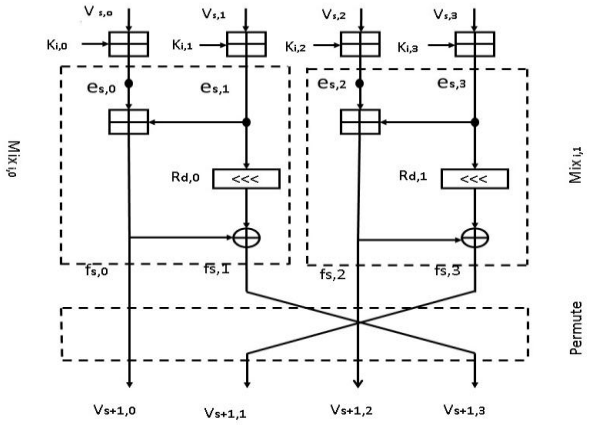

Fig.2. Encryption of Three fish for single round

Mix operation consists of arithmetic addition, bit rotation and bitwise addition. Each mix operation works on two 64-bit words. The mix operation performs as follows:

$$f_{0,0} = e_{s,0} \boxplus e_{s,1}$$
$$f_{s,1} = (e_{s,1} <<< R_{d,j}) \oplus f_{s,0}$$

where d = s mod 8,

left bit-rotation by R times (R = Constant)

After adding the plaintext with the key, two 64-bit words performs mix operation and permutation as shown in the table above. After 72 rounds, all the 64-bit words performs addition with the last subkey to give the final output as cipher text. Each word will be permuted as by the following table shown.

D. Decryption

The reverse process of encryption is known as Decryption. The reverse order of the same steps of encryption involved in decryption of three fish block cipher algorithm.

IV. PROPOSED METHOD

In the proposed method, the tweak values are included in the encryption whereas in traditional three fish, the tweaks are used in key scheduling. By the use of tweak values one plaintext generates different ciphertexts with different tweaks. In this process four 32-bit tweaks is required (t0,t1,t2,t3). Initial tweak values (t0,t1) are taken from the 128-bit of T-buffer and the rest are calculated by adding C_{240} with T-buffer (t2= C_{240}+t0, t3=C_{240}+t1). C_{240} is a constant value defined in three fish algorithm. The process is as follows Key Scheduling, Addition, Mix operation, T-mix operation and Permutation. Plaintext and Tweak values are the inputs for encryption. It is shown in the below figure 3.

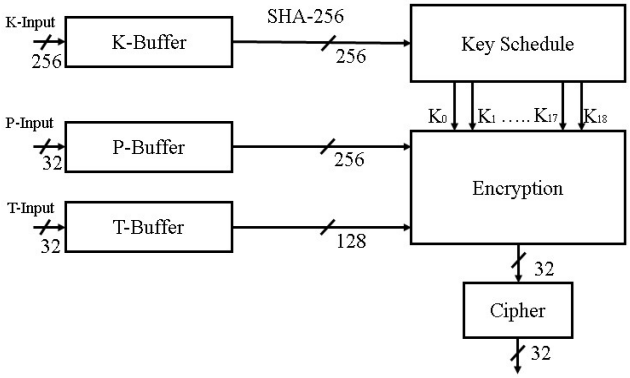

Fig.3. Block Diagram of Modified Three fish

A. Key Scheduling

SHA-256 is applied to generate the subkeys in key scheduling. As it is secure and no such cryptanalytical attacks found yet. SHA-256 is one among the three versions of SHA family, utilized in this proposed method. Append padding bits, append length, Initialize Hash Buffer and Output are the steps of SHA-256. The functioning of SHA-256 is described in figure 4.

Published By:
Blue Eyes Intelligence Engineering
and Sciences Publication (BEIESP)

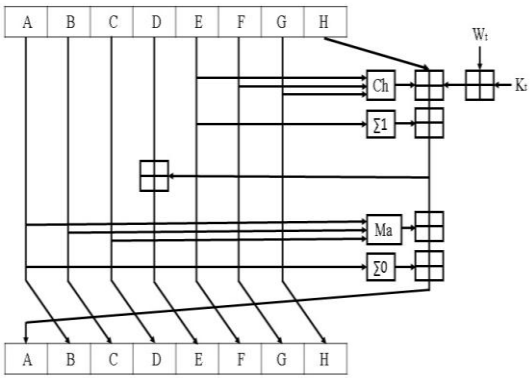

Fig.4. Round function of SHA-256

B. Encryption

In encryption, the following rounds are performed. Addition, Mix operation, T-mix operation and permutation. The procedure starts by adding plaint text with subkeys. The result is given as an input to the mix operation. After executing the mix operation, it carries out to add with the tweak values. Then the T-mix functioning will perform and adds with the preceding outcome. (4)

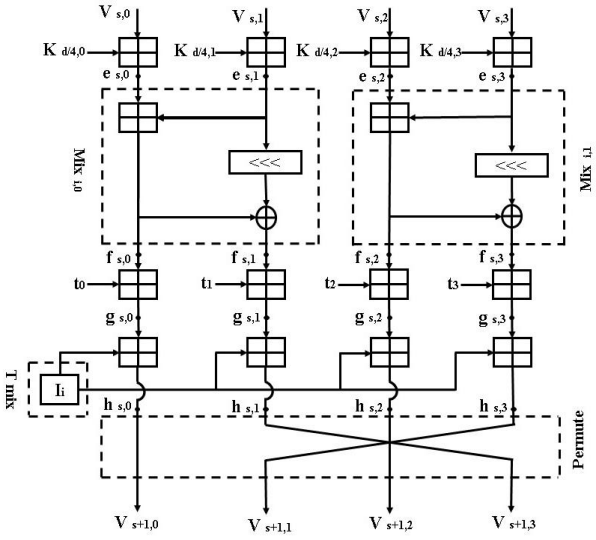

Fig.5. Encryption of Modified Three fish(single round)

From the above figure 5, it has been noticed a function defined as 'I'. In the 'I' function the tweak mix operation takes place. In tweak mix – addition, bit rotation, and XOR would be performed. The representation of tweak mix is shown in the figure 6.

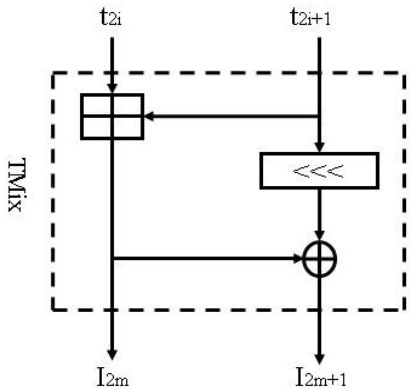

Fig.6. T-Mix Operation

1) Addition

Performing addition with plaintext to subkeys is the first operation that start the process of encryption.

2) Mix Operation

In mix operation- addition, bit-left rotation and Exclusive-OR operations should be accomplished. The rotation of bits relies on the R-table as shown below table 1.

Table I. Bit-Rotation

j/d	0	1	2	3	4	5	6	7
0	14	52	23	5	25	46	58	32
1	16	57	40	37	33	12	22	32

3) T-Mix Operation

T-mix operation is closely like Mix operation. Within the mix operation the inputs are taken from the uppermost addition part. But in T-mix operation the inputs are used as tweak values. The activity of T-mix is same as Mix operation.

4) Permutation

This is the last round in encryption which involves permutation of words according to the word number. It is depicted in table2.

Table II. Words Permutation on Threefish

Word Number	0	1	2	3
Word Number after Permutation	0	3	2	1

C. Pseudo code for Encryption

The following is the pseudo code for encryption of modified three fish.

for i←0 to N_w-1 do
  $V_{0,i} \leftarrow Pi$;
end for
for d ← 0 to Nr-1 do
for i ← 0 to Nw-1 do
if d mod 4 = 0 then
  $e_{d,i} \leftarrow V_{d,i} + K_{d/4,i}$;
else
  $e_{d,i} \leftarrow V_{d,i}$;
end if
end for
for j←0 to N_w/2-1 do
  $f_{d,2j} \leftarrow e_{d,2j} + e_{d,2j+1}$;
  $f_{d,2j+1} \leftarrow f_{d,2j}$ xor $(e_{d,2j+1} <<< Rd,j)$
end for
for i ← 0 to N_w-1 do
  $g_{d,i} \leftarrow f_{d,i} + t_i$
  $h_{d,i} \leftarrow g_{d,i} + I_i$
end for
for m = 0 to N_w/2-1 d0
fun I(m)
  $I_{2m} \leftarrow t_{2m} + t_{2m+1}$;
  $I_{2m+1} \leftarrow I_{2m}$ xor $(t_{2m+1} <<< R_{d,j})$;
end for
for i ← 0 to N_w-1 do
  $V_{d+1,i} \leftarrow f_{d,\Pi(i)}$;
end for
end for
for i ← 0 to N_w-1 do

Published By:
Blue Eyes Intelligence Engineering
and Sciences Publication (BEIESP)

$c_i \leftarrow V_{Nr,i} + K_{Nr/4,i}$;
end for
return
C = c0,c1, …….. cN_w-1;

D. Decryption

The process of converting cipher text to plain text is called Decryption. As in figure 1, T-buffer is added with plaintext for encryption, likewise in decryption T-buffer is added with ciphertext to decrypt the plaintext. The block diagram of decryption is shown in figure 7.

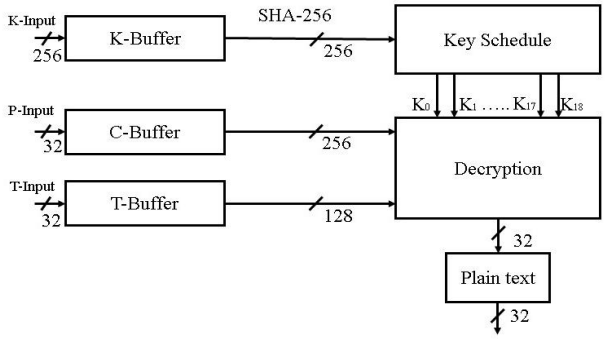

Fig. 7. Block Diagram for Decryption

For single round, the same steps of encryption are performed in decryption but in reverse order.

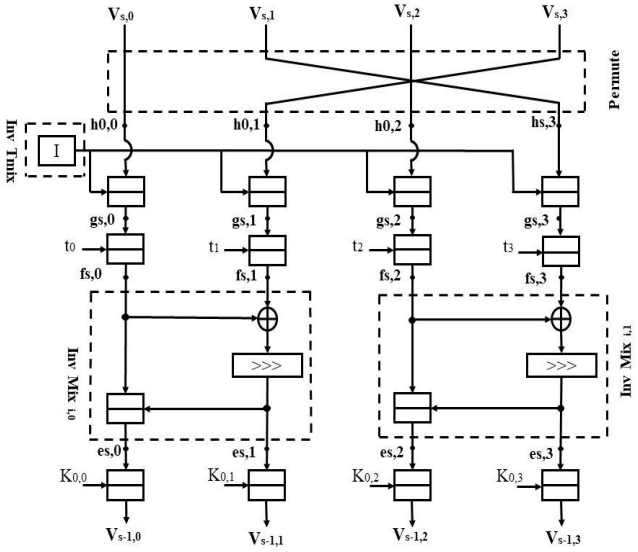

Fig.8. Decryption of Modified Threefish (single round)

The tweak mix operation for decryption is represented as in the below figure 8. The inverse T-mix act according as T-mix but in opposite arrangement. It is depicted in figure 9.

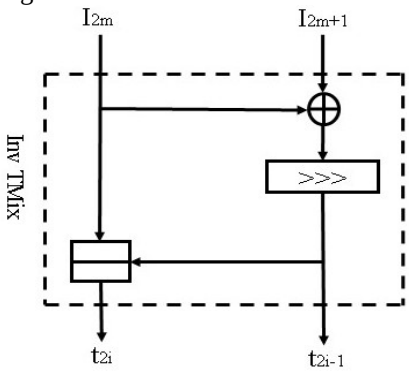

Fig 9. Inverse T-Mix Operation

E. Pseudocode for Decryption

The following is the pseudo code for Decryption.

for i← 0 to N_w-1 do
V0.i ← Ci;
end for
for d ← 0 to N_r-1 do
for i ← 0 to N_w-1 do
Vd+1,i ← fd,Π(i);
end for
for m ← 0 to N_w/2-1 d0
fun I(m)
$I_{2m} \leftarrow t_{2m} - t_{2m+1}$;
$I_{2m+1} \leftarrow I_{2m}$ xor $(t_{2m+1} <<< R_{d,j})$;
end for
for i ←0 to N_w-1 do
$h_{d,i} \leftarrow f_{d,i} - I_i$;
$g_{d,i} \leftarrow g_{d,i} - t_i$;
end for
for j ← 0 to N_w/2-1 do
$f_{d,2j} \leftarrow e_{d,2j} - e_{d,2j+1}$;
$f_{d,2j+1} \leftarrow f_{d,2j}$ xor $(e_{d,2j+1} <<< R_{d,j})$;
end for
for i ← 0 to N_w-1 do
if d mod 4 = 0 then
$e_{d,i} \leftarrow V_{d,i} - K_{d/4,i}$;
else
$e_{d,i} \leftarrow V_{d,i}$;
end if
end for
for i ← 0 to Nw-1 do
pi ← VNr,i - KNr/4,i;
end for
return
P = p0,p1, …….. pNw-1;

V. RESULT

This paper is successfully completed by modifying the encryption and decryption process of Three fish. These alterations bring more hamming weight than the actual algorithm. It is shown in figure 10 below. The result is calculated for three rounds of modified and actual algorithm of three fish.

The steps of these modification are addition, Mix operation, T-mix operation and permutation. The detailed process of these steps are discussed in chapter IV.

For decryption of modified three fish, the steps are permutation, Inverse T-mix, Inverse Mix operation and subtraction as shown in the figure 7. The calculated values for modified encryption algorithm are shown in the table III below.

Published By:
Blue Eyes Intelligence Engineering
and Sciences Publication (BEIESP)

Table III. Encryption Process

Key	Plain Text	Add Ition	Mix Oper Ation	Add Ition	Twix Oper Ation	Add Ition	Permu Tation	Ciphe r Text
F9	54	4E	86	FA	E1	DB	DB	DB
C6	68	2E	A6	0C	C9	D6	D6	D6
73	72	E6	D8	3C	D6	13	13	13
B9	65	1E	C8	3D	DE	1C	1C	1C
3D	65	A2	6C	DE	DF	BE	BE	BE
3	66	6A	29	8E	D5	64	64	64
9A	69	4	82	E7	D0	B7	B7	B7
E4	73	57	AE	0F	C6	D5	D5	D5
D0	68	38	7A	E8	FD	E5	5B	5B
0E	69	77	0C	71	13	84	AD	AD
7F	73	F2	AA	1E	8D	AB	97	97
48	61	A9	A7	11	82	93	1E	1E
55	74	C9	B3	21	C4	E5	52	52
48	77	BF	BC	2C	CC	F9	88	88
18	65	7E	4C	B9	8B	44	E4	E4
F6	61	57	B3	18	5F	77	0D	0D
63	6B	CF	43	D2	19	EC	EC	EC
CA	61	2B	68	9F	6C	0B	0B	0B
11	62	73	EB	6A	0E	79	79	79
15	6C	82	A9	F9	94	8D	8D	8D
C5	65	2A	31	4D	33	81	81	81
68	62	CB	13	75	CE	43	43	43
99	6C	5	BA	38	5	3E	3E	3E
4A	6F	B9	7A	FD	0A	7	7	7
10	63	74	3B	C5	96	5B	E5	E5
D2	6B	3D	4F	85	28	AD	84	84
14	63	78	ED	7D	19	97	AB	AB
BD	69	27	E1	25	F8	1E	93	93
95	70	6	85	9D	B5	52	E5	E5
E0	68	48	D2	3F	49	88	F9	F9
4F	65	B4	CE	54	8F	E4	44	44
4F	72	C1	47	CE	3F	0D	77	77

A. Hamming Weight

Hamming weight is defined as the number symbols are different from the zero symbols. This is a factor of encryption. This factor must have a greater impact on proposed method than traditional. The effectiveness of hamming weight is shown in the figure 10.

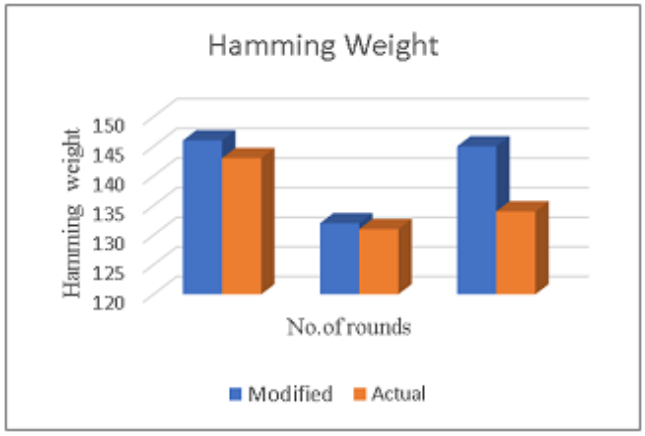

Fig.10. Hamming Weight for three rounds of Threefish

From figure10, the hamming weigh is calculated for three rounds each for modified and traditional three fish algorithm respectively. After performing the three rounds of modified and actual three fish, the result has shown in the figure 10 above.

B. Avalanche Effect

Avalanche effect is one of the factors of encryption. This avalanche effect is performing on different tweaks for same key and plaintext and to show the rate of effect differ from each other. Avalanche effect is calculated as:

Avalanche Effect = (Number of bits changed /Total number of bits) * 100

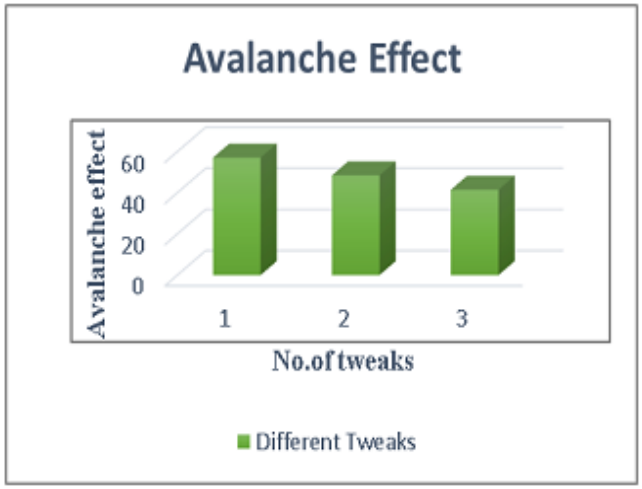

Fig. 11. Avalanche Effect for three different Tweaks

From figure11, the avalanche effect is observed for three different tweaks of modified three fish for the same plaintext and key.The effect varies from one tweak to another tweak value. It is clearly proven that our modified version depends on tweak value and it changes for every tweak value that is given as input. It is impossible to perform cryptanalysis in such cases.

Table-IV: Decryption Process

	Permutation	Subtraction	Inv Twix Operation	Subtraction	Inv Mix Operation	Subtraction	Plain Text	Key
DB	DB	DB	E1	FA	86	4E	54	F9
D6	D6	D6	C9	0C	A6	2E	68	C6
13	13	13	D6	3C	D8	E6	72	73
1C	1C	1C	DE	3D	C8	1E	65	B9
BE	BE	BE	DF	DE	6C	A2	65	3D
64	64	64	D5	8E	29	6A	66	3
B7	B7	B7	D0	E7	82	4	69	9A
D5	D5	D5	C6	0F	AE	57	73	E4
5B	5B	E5	FD	E8	7A	38	68	D0
AD	AD	84	13	71	0C	77	69	0E
97	97	AB	8D	1E	AA	F2	73	7F
1E	1E	93	82	11	A7	A9	61	48
52	52	E5	C4	21	B3	C9	74	55
88	88	F9	CC	2C	BC	BF	77	48
E4	E4	44	8B	B9	4C	7E	65	18
0D	0D	77	5F	18	B3	57	61	F6
EC	EC	EC	19	D2	43	CF	6B	63
0B	0B	0B	6C	9F	68	2B	61	CA
79	79	79	0E	6A	EB	73	62	11
8D	8D	8D	94	F9	A9	82	6C	15
81	81	81	33	4D	31	2A	65	C5
43	43	43	CE	75	13	CB	62	68
3E	3E	3E	5	38	BA	5	6C	99
7	7	7	0A	FD	7A	B9	6F	4A
E5	E5	5B	96	C5	3B	74	63	10
84	84	AD	28	85	4F	3D	6B	D2
AB	AB	97	19	7D	ED	78	63	14
93	93	1E	F8	25	E1	27	69	BD
E5	E5	52	B5	9D	85	6	70	95
F9	F9	88	49	3F	D2	48	68	E0
44	44	E4	8F	54	CE	B4	65	4F
77	77	0D	3F	CE	47	C1	72	4F

The calculated values for the decryption of modified three fish is shown in the table IV.

VI. CONCLUSION

The modified Threefish is implemented in this paper. It is focused on key scheduling process and tweak values. In this paper, hash is produced in the key schedule. Different hashes will be brought out for every four rounds of encryption. Tweaks are the important factor in three fish algorithms. It is customized and user defined. These tweaks can differ from one to another. This modification brings the three fish more effectiveness on the basis of encryption factor like hamming weight and avalanche effect. Both these are cryptographic concepts. Finally, the resultant of modified three fish has greater hamming weight.

REFERENCES

1. Ahmed S. Nori, Ansam Osamah Abdulmajeed, “Design and implementation of Threefish cipher algorithm in PNG file”, Sustainable Engineering and Innovation, Vol.3, N0.2, July 2021, pp,72-91. [CrossRef]
2. Theda Flare G. Quilala, Ariel M. Sison, Ruji P. Medina, “Modified Blowfish Algorithm”, Indonesian Journal of Electrical Engineering and Computer Science Vol. 12, No. 1, October 2018, pp. 38~45 ISSN: 2502-4752, DOI: 10.11591/ijeecs.v12.i1.pp38-45. [CrossRef]
3. Anil G. Sawant, 2 Dr. Vilas N. Nitnaware, Pranali Dengale, Sayali Garud, Akshay Gandewar, “TWOFISH ALGORITHM FOR ENCRYPTION AND DECRYPTION”, © 2019 JETIR January 2019, Volume 6, Issue 1.
4. A.H.Zahid, E.Al-Solami, and M.Ahmad, A Novel Modular Approach Based Substiution-Box Design for Image Encryption,” IEEE Access, vol.8, pp.150326-150340, 2020. [CrossRef]
5. R. Bhanot, and R. Hans "A Review and Comparative Analysis of Various Encryption Algorithms," International Journal of Security and Its Applications, vol. 9, no. 4, pp. 289–306, 2015. [CrossRef]

6. S. W. Jang, "Comparative Analysis of AES, Blowfish, Twofish and Threefish Encryption Algorithms," Analysis of Applied Mathematics, vol. 10, pp. 5-24, 2017.
7. K. M. Mhaidat, M. A. Altahat, and O. D. Al-Khaleel, "High-Throughput Hardware Implementation of Threefish Block Cipher on FPGA," in International Conference on Information and Communication Systems., Irbid, Jordan, 2013.
8. N. At, J. Beuchat, and I. San, "Compact Implementation of Threefish and Skein on FPGA," in 5th IFIP International Conference on New Technologies, Mobility and Security, IEEE Press, 2012.
9. L. P. Oommen, and Anas A. S., "Skein and Threefish Implementation on FPGA," International Journal of Science and Research (IJSR), vol. 4, no. 5, pp.1493-1496, 2015.
10. P. Gayathri, K. Sateesh, and C. Navya, "High-Throughput Hardware Implementation of Three Fish Block Cipher Encryption and Decryption on FPGA," International Journal of VLSI System Design and Communication Systems, vol. 3, no. 8, pp. 1325-1329, 2015.

AUTHORS PROFILE

S Shajarin, is pursuing M.Sc Computer Science from department of Computer Science and Technology in Yogi Vemana University, Kadapa. Areas of interest are cyber Security and Software engineering. I am a Hard worker and punctual towards my work. I am interested to do research in the field of cyber security.

P Leelavathi, is pursuing M.Sc Computer Science from department of Computer Science and Technology in Yogi Vemana University. Areas of interest are Software Engineering and Network security. I am interested to do research in the filed of network security and Software Engineering. I am a Hard worker and dedicated to my work. I gave many seminars and received certificates.

B Reddaiah, is working as Assistant Professor in department of computer science and technology, Yogi Vemana University, Kadapa, driven to inspire students to pursue academic and personal excellence. Areas of research and interest is in Network Security and Software Engineering. I published 35 papers in various international journals and published 15 papers in different international conferences.

G Amrutha Vani, has 8 years of experience in teaching. Area of Interest is Software Engineering. My core research area is Network Security. I published 4 papers in various international journals.

C Swetha, has 15 years of experience in teaching and research. Area of interest is Software Engineering. My core research area is Cloud Computing. she published 10 papers in various international journals and published 5 papers in different international conferences.