HYBRID BLRC ALGORITHM FOR ENCRYPTION

Hevisha Shah[1], Rachana Patel[2]
[2]Assistant Professor, [1,2]L.D. College of Engineering (I.T.), Gujarat, India

Abstract: Faster data transfer and Security both are very important for Wi-Fi. At present, Advanced Encryption Standard (AES) is used for Wi-Fi that is more secured than other encryption algorithms. Blowfish is a faster encryption algorithm but it cannot apply on Wi-Fi because of security problems. Main aim of this research is proposing the hybrid algorithm of Blowfish and Rivest Cipher 6 (RC6) that solves the security problems of Blowfish and maintain the fastness of blowfish.
Keywords: Blowfish, RC6, Collision key attack, Known plaintext attack, reflectively weak key attack (key words).

I. INTRODUCTION

Wi-Fi is a very popular technology but security is a matter of great concern for the field of Wi-Fi. Among many security processes, Cryptography is very popular network security process where the message of any formats is converted into a encrypted version that is unreadable by a human or computer. There are two types of cryptography Algorithms are found: one is Symmetric key cryptography where same key is used for both encryption and decryption (e.g. AES, Blowfish, RC6) and the another is Asymmetric key cryptography where different keys are used for encryption and decryption (e.g. RSA). At present, AES [2] Symmetric key encryption algorithm is used for Wi-Fi network security but it is not so fast. On the other hand, Blowfish algorithm is so fast but it has some security problems. In this paper, a 128 bit hybrid algorithm of Blowfish and RC6 is proposed that removes the security problems of Blowfish and also take less Encryption decryption time than AES.

A. Blowfish

In [1], Blowfish is 64 bit symmetric key algorithm which contains eighteen 32 bit sub keys and four 32bit S-boxes with 256 entries each. The main function of it is given below: The Encryption process of Blowfish is , 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
XL = XL XOR P18.
Finally, recombine XL and XR to get the cipher text.
The F function is: F(XL) = ((S1,A + S2,B mod 2^32) XOR S3,C) + S4,D mod 2^32. Here 64 bit is divided among A,B,C,D registers where each of the register contains 8 bit.

B. RC6

In [3], RC6 is a 128 bit symmetric key encryption algorithm. The procedure is given below:
Input: Plaintext is stored in four w-bit input registers A,B,C,D
.Number r of rounds. w-bit round keys S[0,…….,2r+3].
Output: cipher text is stored in A,B,C,D. Procedure:
B=B+S[0]
D=D+S[1] For i=1 to r do
{
t=(B+(2B+1)) <<< lgw u=(D+(2D+1))<<< lgw A=((A XOR t) <<< u)+S[2i] C=((C XOR u) <<< t)+S[2i+1] (A,B,C,D) = (B,C,D,A)
}
A = A+S[2r+2]
C = C+S[2r+3]

II. RELATED WORKS

In[5],The B-R algorithm is also a mixer of Blowfish and RC6. It is also a 128 bit algorithm and the algorithm uses two S-boxes with 259 entries each. But this algorithm's time complexity is too large because in every iteration it uses two functions: one is Blowfish function and the other is RC6 function and it also contains the risk of Reflectively weak key attack and collision key attack for using the same function and two s-boxes.

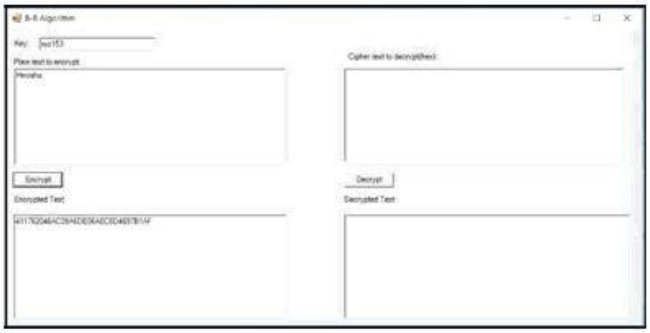

Figure 1-B-R Algorithm for Encryption

Figure 2-B-R Algorithm for Decryption

Avalanche Effect of Existing Algorithm(B-R Algorithm)
Input: hevisagopalbhais
Key:15
Changed Input: ievisagopalbhais

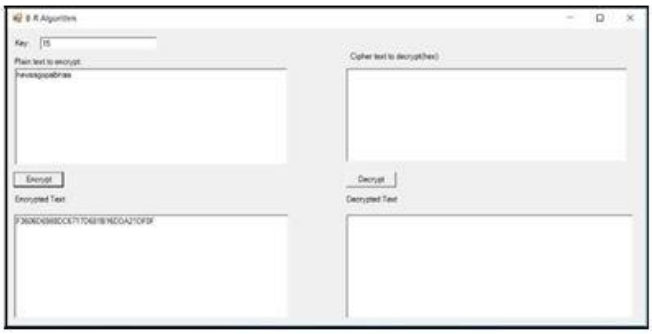

Figure 3 Avalanche Effect calculation of B-R algorithm by changing one bit in input

Figure 4 Avalanche Effect calculation of B-R algorithm by changing one bit in input

Outputs for one bit change in input	Avalanche
F3606D6988DC6717D681B16DDA21DF0F FB73ED22FE37AF9781D04BAD6A5173B5	54

Table1.Avalanche effect calculation of B-R Algorithm

III. PROPOSED ALGORITHM

A possible faster and secure encryption algorithm is proposed here: In this proposed algorithm, 128 bit block of plaintext will be used as input. Here sub key generation of blowfish is used for making cipher text more powerful against brute force attack. The p-array consists of eighteen 64 bit sub keys from p1, p2……p18.Here will be used one 64bit s-box with 263 entries for substitution purpose. F(XL) that is used for Blowfish encryption function for finding next XR will be adjusted here with one s-box. Using one s-box can able to risk of collision attack between more than one S-boxes. 1-16 round of iteration is divided between Blowfish and RC6 modified using a variable 'a'.The value of 'a' is only known by sender and receiver. This type of variation will be able to reduce the risk of reflectively weak key attack[4]. The rotation number 'w' that is used at the portion of RC6 is also a variable that only known by sender and receiver.

Proposed Algorithm Input: Plaintext 128-bits P.
Output: Cipher text 128-bits C. P-array consists of 18 64 bits subkeys
P1,p2…….p18
Split plaintext into two 64-bit halves: XL, XR For I= 1 to a Do
XL=XL XOR P[I]
XR = F (XL) XOR XR Swap XL and XR
For I= a to 16 Do
u= (XR × (2XR +1)) <<<w
XL= (XL <<< u) + P [I] XR= XR + P [I]
Swap XL and XR
XR = XR XOR P17 and XL = XL XOR P18 End.

F function of Proposed Algorithm
Input: XL (64-bits)
Example : If XL (64-bits) contains 0X11083aeb47809123 in hexadecimal then it is devided into eight parts a=0X11,b=0X08,c=0X3a,d=0Xeb,e=0X47,f=0X80,g=0X91, h=0X23.
Z1=(((S-box1[11]+S-box1[08])MOD 2^32) XOR S-box1[3a]) + S-box1[eb]) MOD 2^32
Z2=(((S-box1[47] + S-box1[80]) MOD 2^32) XOR S-box1[91]) + S-box1 [23]) MOD 2^32 Combined Z1, Z2 into Z.
Output: Z (64 bits).

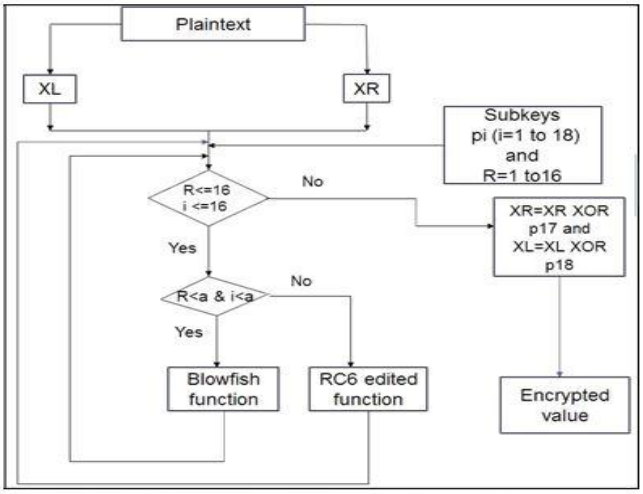

Figure 5-Flowchart of Proposed Algorithm

Implementation of proposed Algorithm

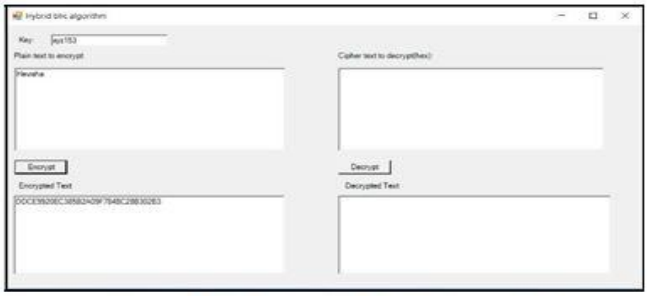

Figure 6-Hybrid BLRC Algorithm for Encryption

Figure 7-Hybrid BLRC Algorithm for Decryption

Value of a	Output for one bit changes in the input	Avala -nche
1	57F6F0C52A992424E63921DA399BA30F B9715586DB0C3BC118FD8F2C986BADD7	71
2	8D89CD2855AB18F7DCA723B683E2DA19 FDDBC4E744FFA96C7A3FACF3904C2A20	57
3	5A2C82BB1C5E28E8374E70CBEF80BB82 AAE93EB2E0F977ABD1081AB6F4A29041	65
4	718D00C390C593464ACC278BCE377794 77592710518B6E8B7562DC897E727E67	66
5	BEFCEFA5E7DCF671555FA527846C3009 E39BB67648CEFD509DC28D3E723269D9	61
6	4D66998F7B94B593932431F0C8707105 DB0DCDD45207B76E3B2159368F1E548C	58
7	2623F48250DA7F90C79981E9E228DAAB C6E85DC8F06A9CDBFA70BF433092E0AF	62
8	575E0FD679AC760AFA0D7794BF7CD4C1 65D777172856D620E0CF2CFDDDC53003	57
9	16FC914DC62F32B5B9613883E0173F47 EE9E413F38C235F55AB43142C2B2368E	58
10	1D713B4555BCC3B1AD178647BBC31D86 0A1E0716E299D8DA2329199CFE10B2A8	72
11	6F5C1322164E4A51CDDDEFA49CA4F6FB 64316934A3CA758AAE537EB2DBCC52B1	61
12	C0B66F755B8DF82687E448A809D35F1A 7E5D29B846E83A4EF56435448DF19DF2	61
13	485DE605196B41EECA5F9336DCE0D73E 0CC6C0B0463709A40B0B815F51FAE0A3	59
14	B644BD5DDAC8F41465199686ADC26842 C18AE1EFBD2A22A942C4A09E448512A	71
15	307C14677CB5F65FCB02D8D62B5EC27A 317C14678AA53097DE7053D2CE6ACA8	44

IV. RESULT ANALYSIS

The proposed and Existing Algorithm are iimplemented in C#.

Size of Data (bytes)	B-R Algorithm Execution Time	BLRC Algorithm ExecutionTime
1024	0.127	0.124
2048	1.010	0.661
3072	2.586	2.155
4096	9.974	6.473
5120	14.002	11.330
6144	34.111	25.132

Table3.Comparison of Execution time

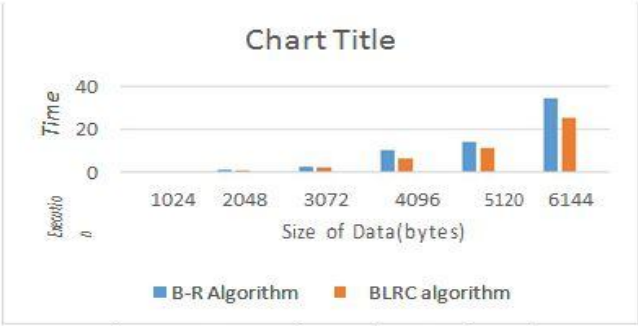

Figure 8-Comparison of Execution Time

V. CONCLUSION

Proposed algorithm produce a faster algorithm like blowfish and more secure than it. The proposed algorithm improves the faster algorithm Blowfish by adding the edited function of RC6 and removing it's different attacks. It also uses "a" and "w" random variable to confuse the intruders by making different cipher text. It's one S-box criteria makes the time complexity little higher than Blowfish but it reduces the memory requirement.

REFERENCES

[1] B. Schneier, "Description of a New Variable-Length Key, 64-Bit Block Cipher (Blowfish)", Fast Software Encryption, Cambridge Security Workshop Proceeedings(December 1993),Springer-Verlag,1994, pp 191-204.

[2] Eric Conrad, "Advanced Encryption Standard", GIAC Research in the Common Body of Knowledge, California.

[3] R. L. Rivest , M.J.B. Robshaw , R. Sidney and Y.L. Yin , "The RC6 TM Block Cipher" ,M.I.T. Laboratory for Computer Science, 545 Technology Square, Cambridge,MA 02139 USA,RSA Laboratories, 2955 Campus Drive, Suite 400, San Mateo,CA 94403, USA, Version 1.1 ,August 20, 1998.

[4] Orhun Kara and Cevat Manap, "A New Class of Weak Keys for Blowfish", TÄUB_ITAK UEKAE, Gebze, Kocaeli, Turkey forhun.

[5] Janan Ateya Mahdi, "Design and Implementation of Proposed B-R Encryption Algorithm" ,IJCCCE, VOL.9, NO.1, 2009.

[6] Evilcry,"Blowfish Study n' Reverse", http://evilcry.altervista.org

[7] Vaibhav Poonia, Dr. Narendra Singh Yadav, " Analysis of modified Blowfish Algorithm in different cases with various parameters", International Journal of Engineering Research and General Science, Volume 3, Issue 1, ISSN 2091-2730, January-February 2015.

[8] Gurjeevan Singh, Ashwani Kr. Singla, K.S. Sandha," Superiority of Blowfish Algorithm in Wireless Networks", International Journal of Computer Applications, Volume 44, No.11, pp-0975 – 8887, April 2012.

[9] Mar Preet Singh and Raman Maini ," Comparison Of Data Encryption Algorithms", International Journal of Computer Science and Communication, Vol. 2, No. 1,pp. 125-127, January-June 2011.

