Proceedings of the Fifth International Conference on Communication and Electronics Systems (ICCES 2020)
IEEE Conference Record # 48766; IEEE Xplore ISBN: 978-1-7281-5371-1

Honey Encryption based Hybrid Cryptographic Algorithm:A Fusion Ensuring Enhanced Security

Mr. Vivek Raj K
Department of Telecommunication
Dayananda Sagar College of Engineering
Bangalore, India.
Vivekgowda1990@gmail.com

Ankitha H
Department of Telecommunication
Dayananda Sagar College of Engineering
Bangalore, India.
ankithatonapi@gmail.com

Ankitha N G
Department of Telecommunication
Dayananda Sagar College of Engineering
Bangalore, India.
ankitha.ganapatibhat@gmail.com

Kanthi Hegde L S
Department of Telecommunication
Dayananda Sagar College of Engineering
Bangalore, India.
kanthishegde@gmail.com

Abstract—**Providing high security to data exchange is one of the most primary concerns with fast evolution in communication technology. So, a Hybrid cryptographic algorithm is proposed where, Rivest Cipher 5 (RC5) is used for encryption and decryption of data and Honey Encryption (HE) is used for secret key exchange, which is a major challenge of symmetric cryptography. In this paper, number of rounds of RC5 is varied and its strength is studied based on randomness, considering avalanche effect. Time complexity of RC5 is also analyzed and increasing strength is chosen over time complexity as RC5 shows very slight increase in time when number of rounds is increased. Additionally, HE involves Distribution Transforming Encoder (DTE) and generation of honey-words. HE acts an additional layer of protection for RC5 cryptographic algorithm. HE is password based and it gives fake messages if any intrusion is detected and have utilized this concept to protect sharing of secret key. Both algorithms are efficiently integrated; obtained results clearly justify that greater number of rounds provide more randomness and hence better security and key exchange is done securely. Thus, proposed Hybrid cryptographic algorithm efficiently provides enhanced security as it involves double encryption.**

Keywords—Cryptography; Distribution Transforming Encoder; Honey Encryption; Key exchange; RC5.

I. INTRODUCTION

In today's era, security is the utmost concern for the transmission of data from sender to receiver. Cryptography is the process of protecting 'Data' from being attacked. It hides information by transforming it into cipher text through encryption and authorized users can get back plain text from cipher text through decryption. This encryption and decryption are initiated by keys [6].

Symmetric key cryptography is comparatively faster than Asymmetric key cryptography and it is efficient for usage on larger amount of data. Symmetric key cryptography is further classified into two types, namely: Stream cipher and Block cipher. Some of the stream ciphers are A5/1, RC4. Examples of Block ciphers are DES,3-DES, RC2, RC5, etc.,[3]. Stream cipher converts plain text to cipher text by taking one byte of plain text at a time. Block cipher converts plaintext to cipher text by taking one block of plain text at a time. In software, Block cipher can be easily implemented when compared to Stream cipher, as it consumes less time and bit manipulation. Rivest Cipher 5 (RC5) is one such symmetric block cryptographic algorithm. This algorithm needs secure channel for exchange of secret key. For this Honey Encryption (HE) is used in this paper.

A. RC5

RC5 is a symmetric-key block cipher proposed by Ronald Rivest in 1994. It has variable block size, variable number of rounds and variable-length secret key, providing flexibility in performance, security and light weight [8]. Novel feature of RC5 is heavy use of data dependent rotations and encourages assessment of cryptographic strength [7]. Flexibility and adaptability are a vital feature of RC5 [9]. Parameterized RC5 can be represented as: RC5-w/r/b, where w=word size in bits, r=number of rounds and b=key size in bytes [2]. Table 1 explains the parameters of RC5 algorithm [12].

TABLE 1: PARAMETERS OF RC5.

Parameters	Definition	Values
w	Word size in bits	16,32,64
r	Number of rounds	0, 1……255
b	Number of bytes in secret key	0, 1……255

RC5 Algorithm mainly involves Key Expansion, Encryption and Decryption. RC5 encryption involves 3 simple operations and their inverses, such as addition, ex-or and rotation, which makes encryption algorithm very simpler [2].

B. HE

HE is the best algorithm in provide security to data against Brute Force Attack (BFA). The term 'Honey' describes a false message and Honeyword is a fake user name which is stored in database. This algorithm also provides a clue of previous attempt of vulnerability. When an attack is found since it throws a valid looking invalid message attacker will be confused whether message is original or not. In this paper this concept of HE is used for secure key exchange.

II. RELATED WORKS

Various works have been carried out to solve the problem of security and various researches are being carried out on different cryptographic algorithms. Here are some of the unique approaches on RC5 and HE.

Harsh Kumar Verma, Ravindra Kumar Singh et al [1], have done comparison of Blowfish and RC5. Blowfish is faster than AES and DES. Comparison is done based on parameters i.e. execution time, security. Results showed that time taken by RC5 are very less compared to Blowfish; it is 1.54 times much faster than Blowfish. Also, RC5 is more secure.

Ronald L Rivest et al [2], has performed RC5 encryption algorithm against a text file. Author showed that as number of rounds and the size of key increases, security also increases.

Harsimranjit Singh Gill et al [3], author has suggested a simple approach to augment performance of RC5 algorithm. He has suggested use of prime number to improve the security. Using prime no. of rounds instead of non-prime no. of rounds according to this approach, has provided better strength.

Khin Su Myat Moe, Thanda Win et al [4] proposed a stronger encryption technique against BFA i.e., HE which is a key exchange algorithm. They have proven than HE is a better and more secure algorithm than RSA for key exchange.

In the above-mentioned related works, RC5 is proven to be more secure and faster when compared to other algorithms such as RSA and Blowfish. Honey encryption is better than RSA for secure key exchange. However, as RC5 is a symmetric key cryptosystem it still faces the challenge of sharing secret key securely. Thus, to overcome these drawbacks,integrated RC5 retaining its advantages and by increasing its strength, along with Honey encryption with an increased buffer size of randomly generated passwords. Analysis of RC5 and Proposed Hybrid cryptographic algorithm is discussed in below sections of this paper.

III. PROPOSED WORK

A. RC5 Algorithm

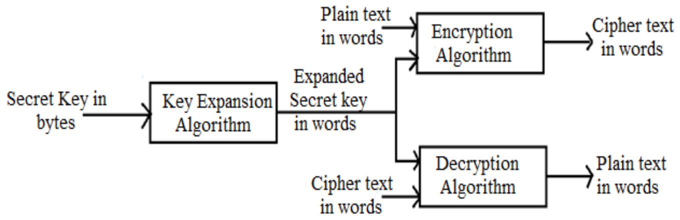

Figure.1. Simple block diagram of RC5 algorithm.

Simple block diagram of RC5 algorithm is as shown in the Figure 1, which briefly explains about 3 steps of RC5 algorithm.

1) Encryption: It takes plaintext as an input and produces cipher text as output. It takes 2 blocks from input and that will be stored in 2 registers E and F, where E stores first 32 bits and F stores next 32-bits of input.

2)Key Expansion: This involves 3 steps namely; Conversion, Initialization and Mixing. Key expansion algorithm uses 2 magic constants, which are required for generation of sub keys. 2 magic constants are represented as Rw and Sw as shown in (1) and (2).

$$Rw=Odd\ ((e-2)2w) \quad (1)$$
$$Sw=Odd\ ((\emptyset-1)2w) \quad (2)$$

Where, e=2.718281828459 (base of a natural algorithm). Ø=1.618033988749(goldenratio) [2].

a)Conversion: This step converts secret key in bytes to words.

b) Initialization: This step involves initialization of an array T using the magic constants Rw and Sw.

c) Mixing: This is 3rd step of key expansion which mainly involves mixing of user's secret key in 3 passes. Among these 2 arrays, array which is larger that will be processed for 3times.

3) Decryption: This process takes 2 blocks of cipher text as input and gives 2 blocks of original plaintext as output [2].

The nominal values of parameters used in this paper are, w= 32 bits, r= 12 rounds and b= 16 bytes. Thus, key size is 128 bits.

B. HE

HE involves generation of honey words, process for key or passwords distribution and for message distribution DTE process. The flow of the HE algorithm is given in the Figure 2 [11].

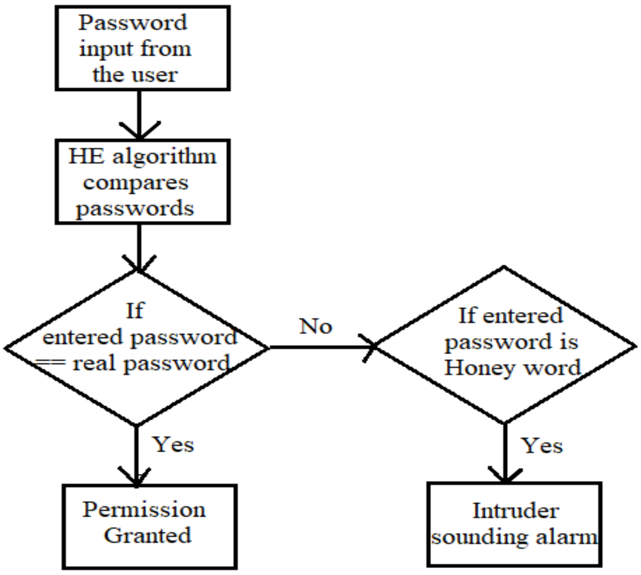
Password input from the user
HE algorithm compares passwords
If entered password == real password
No
If entered password is Honey word
Yes
Yes
Permission Granted
Intruder sounding alarm

Figure.2. Flow diagram of HE.

In order to prevent from BFA, Honey Words are stored along with user's real passwords in database. Honeyword is fake password, created to confuse attackers if they get the password file in the database. The attackers can't know which password is real password by adding the honeywords to the password file. In this process, the combination storage of bogus passwords and real passwords are called sweet words and the real user's password is called sugar word.

DTE is main idea behind pure honey encryption technique. The internal structure of HE comprises of DTE encryption and DTE decryption. The 2 algorithms describe net functioning of HE [5].

- Let probability distribution over message space be over message L.
- The distribution transforming encodes the message Las a K bit seed S? {0, 1} K and decodes the message by inverse DTE method, decode (S) =L.

TABLE 2: HE ALGORITHM.

Honey Encryption Algorithm	Honey Decryption Algorithm

HEnc (X, L)
S←$ encode (L)
R←$ {0, 1} n
S'←H (R, X)
C←S'⊕S
Return (R, C)
	HDec(X,(R,C))
	S'←H (R, X)
	S←C⊕S'
	L←decode(S)
	Return L

Table 2 explains the HE encryption and decryption algorithm. H stands for cryptographic hash function, X is key, L is for message, S denotes seed, R denotes random string, C is cipher text and $ indicates that HE algorithm may use some number of uniform random bits. When HE is applied to plaintext message L, it first encodes message L to S and then encrypts S by key X using suitable symmetric encryption algorithm. The above algorithms describe these steps clearly, HE provides high message security [10].

C. *Proposed Method: "Hybrid cryptographic algorithm for enhanced security"*

In the proposed method as shown in Figure 3, two cryptographic algorithms are used for transmission of information from one end to the other.

•Encryption & Decryption Algorithm: RC5

•Key Exchange Algorithm: HE

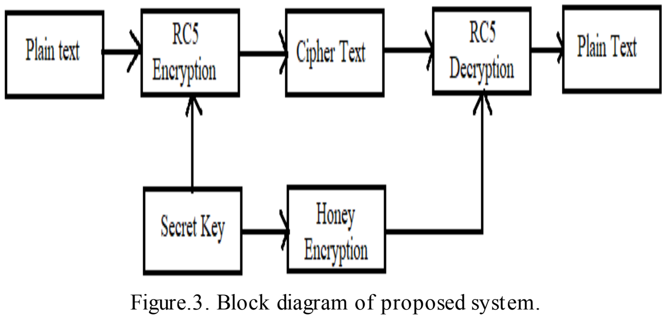

Figure.3. Block diagram of proposed system.

During transmission of data its necessary to maintain confidentiality and privacy. Hence it should be encrypted before sending it to the recipient. Here data is been encrypted using RC5 encryption algorithm using the secret key. After encryption it gives the cipher text. The secret key will be shared with the receiver. But sharing the secret key with the receiver using an ordinary method may lead to an unauthorized key access. HE algorithm is used which takes RC5 secret key as an input encrypts and decrypts it. If this decrypted secret key is same as original secret key, then it will be used for decryption by receiver and original message will be retrieved back.

Figure 4 shows flow chart for the Proposed Method. The Hybrid algorithm receives text message (plaintext) from sender, that has to be sent to receiver at the other end. It performs RC5 encryption and converts plaintext into cipher text by using secret key generated by RC5 algorithm. If the receiver wants the text message sent by the sender then he needs same secret key for decryption. This secret key is protected by HE in our model.

The HE algorithm protects secret key with a strong password making Brute Force Attack very difficult. HE algorithm generates a set of fake and almost alike passwords to confuse intruder. If attacker tries to crack the password with an intension to get secret key this algorithm gives an intruder alarm immediately and intruder is given fake secret key (which he assumes to be original secret key) with which he cannot decrypt text message and hence attack fails. This whole process happens with help of DTE. If authorized receiver enters correct password then he is given right secret key which he uses for decryption of cipher text to get text message intended to him.

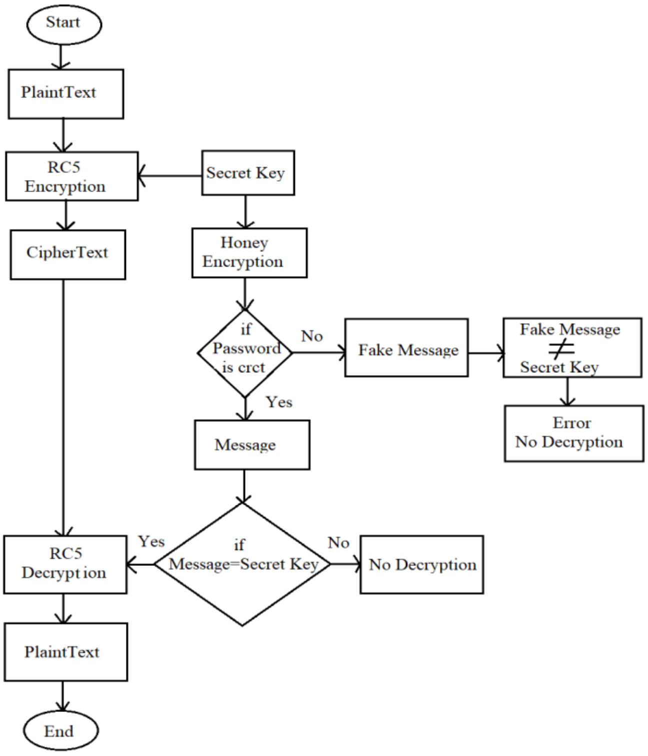

Figure.4. Flow chart for the Proposed Method.

IV. PERFORMANCE ANALYSIS

A. Analysis of Strength of RC5

The number of rounds of RC5 is varied and variation in strength is demonstrated in the Table 3 and Table 4. The nominal values of parameters considered in this paper are w=32-bits, r=12 rounds and b=16 bytes. Depending on the choice of security level the value of parameters can be changed.

TABLE 3: RESULTS SHOWING VARIATION IN R

w	r	Plain text	Cipher text
32	12	12AB34A2 AB12C45B	97C2DEC5 C2E0808
32	16	12AB34A2 AB12C45B	D1FC08EB CB25A884

TABLE 4: RESULTS SHOWING VARIATION IN W

w	r	Plain text	Cipher text
32	12	1A234234 342A1B54	13DAEB77 37DF4252
64	12	1A234234 342A1B54	B1A23001 239D68E

Observed that when r=12 execution time, encryption time and decryption time are 2.951s, 2.080s and 0.871s respectively, and when r= 15 execution time, encryption time and decryption time are 3.016s, 2.103s and 0.913s respectively.

TABLE 5: VARIATION IN EXECUTION TIME AS NUMBER OF ROUNDS IS VARIED FOR SAME PLAIN TEXT.

No. of rounds	Key size (in bytes)	Plain text	Execution time (in sec)
12	16	31323334 35363738	2.951
15	16	31323334 35363738	3.016
20	16	31323334 35363738	3.339

TABLE 6: VARIATION IN ENCRYPTION TIME AS NUMBER OF ROUNDS IS VARIED FOR SAME PLAIN TEXT.

No. of rounds	Key size (in bytes)	Plain text	Encryption time (in sec)
12	16	31323334 35363738	2.080
15	16	31323334 35363738	2.103
20	16	31323334 35363738	3.233

TABLE 7: VARIATION IN DECRYPTION TIME AS NUMBER OF ROUNDS IS VARIED FOR SAME PLAIN TEXT.

No. of rounds	Key size in bytes	Plain text	Decryption time (in sec)
12	16	31323334 35363738	0.871
15	16	31323334 35363738	0.913
20	16	31323334 35363738	1.028

From the results obtained as shown in Tables 5,6 and 7, time taken for 20 rounds is little more compared to time taken for 15 rounds and similarly, time taken for 15 rounds is slightly more compared to time taken for 12 rounds. As results show very less increase in time (by few seconds) for greater number of rounds, slight increase in time can be ignored as security is the main concern. Hence to increase the security, numbers of rounds are increased.

One-bit change in the plaintext, results in momentous change in the cipher text. This method is called as avalanche effect. A good encryption algorithm should always satisfy (3).

$$\text{Avalanche-effect}>50\% \qquad (3).$$

Formula to calculate avalanche effect is shown below in (4).

Avalanche effect= (N0. of bits flipped) / (Total number of bits) [9]. (4).

TABLE 8: AVALANCHE EFFECT SHOWING RANDOMNESS OF RC5.

w	r	b	Plaintext	Cipher text	No. of bits changed in plain text	Hamming Distance	Avalanche Values
32	12	16	Pt1- 31323334 35363738 Pt2- 31323334 35363739	Ct1- 7E24ECFB 8CF2BCAE Ct2- F789114D 44CDD6AD	1 bit	29	42%
32	15	16	Pt1- 31323334 35363738 Pt2- 31323334 35363739	Ct1- 60D27491 BE137039 Ct2- 1D550375 5A2E65F3	1 bit	37	57%
32	20	16	Pt1- 31323334 35363738 Pt2- 31323334 35363739	Ct1- 7CC2C6CC B9AECD49 Ct2- 4DFF4767 D81978E5	1 bit	44	63%

The results obtained when Avalanche values were calculated as given in Table 8. When values of w and b are kept constant and value of r is varied for the same plain text. observed that, if the plaintext is flipped by 1 bit then there is change in 29 bits for 12 rounds with the Avalanche effect being

42%. For 15 and 20 rounds there is 37 bits and 44 bits change respectively, with 57% and 63% Avalanche effect for respective rounds. From above results it can be concluded that increase no. of rounds Avalanche effect increases. Hence strength of RC5 algorithm also increases.

B. Analysis of Hybrid Cryptographic Algorithm

Now that the strength of RC5 is increased and transmission of data is secured, it's very important to exchange the secret key that is used for both RC5 encryption and decryption, very securely with authorized parties only and have proposed a Hybrid encryption model as discussed in section C of proposed work by integrating RC5 and HE, by retaining the advantages of both algorithm and this has increased overall security of data transmission.

C programming is used for coding in fully featured Integrated Development Environment Code Blocks 13.12 platform to integrate both RC5 and HE to get results according to our objective.

Table 9 explains how text data are considered "Meet@9am" undergoes RC5 encryption and Honey encryption. Password that used to protect text data is "PaSs1995@bng". Hybrid algorithm gave us text data back only when right password was entered. When password was "K&APASS1995@BNG#" one of fake passwords generated by HE, it gave an intruder alarm and password entered was incorrect "F589A6959F3E04037EB2B3EB0FF726AC" a fake secret key was given. But the right secret key is this using only which got the message that is "Meet@9am" back, "8ACA0C6C226CA2308436D52CE1E833A8".

TABLE 9: RESULT FOR PROPOSED METHOD.

Name	Plain Text	Key/Password	Cipher Text	Decrypted Text
RC5	Meet@9am	8ACA0C6C226CA2308436D52CE1E833A8	2584249E67A4C416	Meet@9am
HE	8ACA0C6C226CA2308436D52CE1E833A8	PaSs1995@bng (Right password)		8ACA0C6C226CA2308436D52CE1E833A8
		K&APASS1995@BNG# (wrong password)		F589A6959F3E04037EB2B3EB0FF726AC

V. CONCLUSION

In this paper integration of RC5 and HE greatly enhance security during transmission of data as well as secret key. Results clearly show the data dependent rotation and increased number of rounds make RC5 algorithm stronger that gives rise to randomness of 42% for 12 rounds and 63% for 20 rounds, thus it can be concluded that security of RC5 is improved by increasing number of rounds. HE is an excellent solution for the challenge of secure key exchange of symmetric RC5.As HE pushes intruder towards a confusing end whenever a wrong password estimate is made, it is more secure than RSA. Since Proposed model involves double encryption, it is very difficult for any intrusion to occur. Thus, our Proposed model greatly protects data text from unauthorized access and ensures only intended receiver gets the information.

Further this honey encryption-based hybrid cryptographic algorithm can be used for image, audio, video encryption that is multimedia encryption.

REFERENCES

[1]. Harsh Kumar Verma, Ravindra Kumar Singh "Performance analysis of RC5, Blowfish and DES block cipher algorithms", International Journal of Computer Applications, Volume 42– No.16, March 2012.

[2]. Ronald L Rivest, "The RC5 encryption algorithm".

[3]. Harsimranjit Singh Gill, "Selection of parameter 'r' in RC5 algorithm on the basis of prime number", in proceedings of 2014 RAECS UIET Panjab University Chandigarh,06-08 March,2014.

[4]. Khin Su Myat Moe, Thanda Win, "Enhanced Honey Encryption algorithm for increasing message space against Brute Force Attack", in proceedings of the 2018 - 15th International Conference on Electrical Engineering/Electronics, Computer, Telecommunications and Information Technology.

[5]. Joseph Jaeger, Thomas Ristenpart, Qiang Tang, "Honey Encryption beyond message recovery security", Issue-2016.

[6]. Jeba Nega Cheltha C, "An innovative encryption method for images using RSA, Honey Encryption and inaccuracy tolerant system using Hamming codes", in the proceedings of 2017 International Conference on Computation of Power, Energy, Information and Communication (ICCPEIC).

[7]. M. Amin and A. A. El-latif, "Efficient modified RC5 based on Chaos adapted to Image encryption," in Journal Electronic Imaging, Issue-2010.

[8]. Excel B. Villanueva, Ruji P. Medina, Bobby D. Gerardo, "An enhanced RC5 (ERC5) algorithm based on simple random number key expansion technique".

[9]. Jayvee Christopher N. Vibar, Ruji P. Medina, Ariel M. Sison, "ERC5a – An enhanced RC5 algorithm on bit propagation in the encryption function", Issue-2019.

[10]. Ari Juels, Thomas Ristenpart, "Honey Encryption- Encryption beyond the Brute-Force Barrier" in the proceedings of 2014 IEEE Conference on Computer and Reliability societies.

[11]. Piyush, "Advanced Honey Encryption: An Escape-less Trap for Intruders" 2018 4th International Conference on Computing Communication and Automation (ICCCA).

[12]. Osama S. Faragallah, "An enhanced chaotic key-based RC5 block cipher adapted to image encryption" in International Journal of Electronics, Issue-2012.