International Journal for Innovative Engineering and Management Research

A Peer Revieved Open Access International Journal

www.ijiemr.org

IJIEMR Transactions, online available on 12th Dec 2018. Link :http://www.ijiemr.org/downloads.php?vol=Volume-07&issue=ISSUE-13

Title: **A CLADDED FEEDBACK APPROACH TO CONSTRUCT HIGHLY SECURE AND HIGH PERFORMANCE CLADDED CIPHERTEXT FILES**

Volume 07, Issue 13, Pages: 377–382.

Paper Authors

YJN LAKSHMI, KONERU SUDHIR, T.MALLESHWARI

PB Siddhartha College of arts and science, vijayawada

International Journal for Innovative Engineering and Management Research
PEER REVIEWED OPEN ACCESS INTERNATIONAL JOURNAL
www.ijiemr.org

A CLADDED FEEDBACK APPROACH TO CONSTRUCT HIGHLY SECURE AND HIGH PERFORMANCE CLADDED CIPHERTEXT FILES

[1]YJN LAKSHMI, [2]KONERU SUDHIR, [3]T.MALLESHWARI
[1]Lecturer, Department of Computer Science, PB Siddhartha College of arts and science, vijayawada.
[2]Lecturer, Department of Computer Science, PB Siddhartha College of arts and science, vijayawada.
[3]Lecturer, Department of Computer Science, PB Siddhartha College of arts and science, vijayawada.
[1]boppana.yl@gmail.com

Abstract— In mobile communication, messages are sent by means that of the air. this might attract programmers to spy and at the moment break them. later on, the safety may be an important issue ought to are attended. Advanced Standard Encryption (AES) is at the present AN as typically as a doable utilized encoding approach. In any case, AES is unreliable presently since it's been halfway explained. on these lines, during this paper, we tend to gift a security framework, named Random Cladding with Feedback Mechanism encryption method (RCFM for short), that utilizes the key phrase key or the channel key entered by a basic shopper because the underlying encoding key, and embraces a powerfully assembled moving substitution system along with a TwoDimensional Operation encoding technique to form a sub-keys gathering. It to boot recovers this time parameters and irregular range keys as powerful parameters to play out a cladded input encoding. Through supposed investigation and laptop recreations, the RCFM shows all the way down to earth security in system communications.

Keywords-Mobile Communication, AES, DES, Block cipher encryption, Current time key

I. INTRODUCTION

Because of the fast improvement of versatile correspondence ways and therefore the net advances, hand-held gadgets ANd an expansive scope of utilizations nowadays are magnificently used to advance our regular daily existences and provides North American country a useful living and looking condition. Then again, as AN outcome of the fast development in versatile system examines, people could send or transfer touchy data through the mobile phone for capability or making ready. However, amid the knowledge exchange, the fragile data will while not a lot of-of a stretch be listened stealthily by malignant gatherings, transfer regarding extreme security problems. on these lines, a compelling insurance an instrument for data exchange is needed. Data Encryption Standard (DES) and Advanced coding customary (AES), the 2 most usually used sq. figure parts, each utilize the combinative explanation because of the center of the making ready procedure. In Gregorian calendar month 1999, during a joint effort with distributed.net, the Electronic Frontier Foundation (EFF) decoded DES-encoded message with not precisely multi-day [1]; in like manner, security of AES is likewise in question [2], implying that we tend to need a safer sq. data coding strategy. to require care of the problem, during this paper, we tend to propose a security plot, named the Random protective covering with Feedback Mechanism coding strategy (RCFM for short), to enhance the safety of sq. coding ciphertext for moveable correspondence. The RCFM utilizes a secret key or channel key entered by the hidden consumer as AN underlying coding key, and embraces a dynamic moving substitution system associated with a Two-Dimensional Operation coding strategy to make a sub-keys gathering, and later recovers current time parameters and irregular numbers [3] as powerful parameters to continue cladded input coding [4]. By the RCFM, even disorganized the equivalent plaintext with an analogous secret word, the created cladded ciphertext record and therefore the relating ciphertext are distinctive with varying lengths since the used current time parameters and capricious range keys modification. As such, even military workers or general as usually as attainable transfers or downloads mystery data with a mobile phone, the RCFM will safely make sure the information. The rest of this text is sorted out as pursues. space two quickly presents the connected examines of this paper. space three depicts the projected technique. phase four examines the safety of our strategy. phase five abridges this work and descriptions our future investigations.

II RCFM

The main purpose of the RCFM is to hide the ciphertext in the wrapped cipher file dynamically such that cracker cannot obtain the (plaintext, ciphertext) pair, thus effectively raising the security level.

3.1 Parameters and Operators

The parameters and operators used in the RCFM are defined as follows.

3.1.1 Definitions of parameters

PW: the password, consisting of 8 to 16 characters is inputted by the user.

KPW：the password key produced from processing PW with a particular algorithm.

ct：a shifting counter.

SS, SB：character variables.

KCH：the channel key, which is established between the user end and the sever of the underlying system before communication starts.

K0：the initial encryption key defined as K0 = KPW or K0 = KCH.

K1~K5：the encryption sub-keys generated by the RCFM at its initial process

PRNS1：pseudo random number sequence

1. PRNS2：pseudo random number sequence

2. Δh：length of PRNS1 in bits.

Δt：length of PRNS2 in bits.

KCT：the current time key, which is 128 bits in length and is generated according to the current CPU time, consisting of nanosecond/date/hour/minute/second/nanosecond/hour/ minute/second. KRCT：the reversed key of KCT, which is 128 bits long, consisting of second/minute/hour/nanosecond/second/minute/hour/d ate/nanosecond.

RK：Random encryption Key.

CRK：Cipher of RK.

b0 ~ bn : an internal feedback-code sequence.

Plaintext : P1P2…Pj…Pn, where1≦j≦n, each of which is 128 bits long.

Ciphertext : C1C2…Cj…Cn, where1≦j≦n, each of which is 128 bits in length.

3.1.2 Operators and functions

1) Exclusive-OR operator : ♁

Encryption: c=p ♁ k, where p represents the plaintext, and c is the ciphertext and k is the encryption key.

Decryption: p=c ♁ k

2) Binary adder operator : +2

Encryption: c=p+2k, where the carry out of the most significant bit of the binary addition is dropped.

Decryption:

$$p = c -_2 k = \begin{cases} c-k & \text{if } c \geq k \\ c+\bar{k}+1 & \text{otherwise} \end{cases} , \quad \text{where}$$

$-_2$ is the inverse operation of $+_2$.

3) Modulo operator: mod

c=p mod n, where n is an integer.

4) Two-Dimensional Operation: the encryption operation that encrypts a message with two different operators, i.e., ♁ and +2, and some encryption keys.

5) Dynamically accumulated shifting substitution: Input: SS which is a character, and ct which is a shifting counter.

Output: SB which is a character It uses an S-Box as the substitution box. The substitution first finds the image character in S-Box of the inputting character SS, and then shifts the position from the image character ct times along the S-Box to obtain the target character SB.

6) Fct(SS) : a function that counts the number of binary digit of 1s contained in character SS.

7) Mid(PW, i, n) : a function that retrieves n characters from PW starting at the i-th character of PW.

8) Right(PW, n) : a function that retrieves n rightmost characters of PW

3.2 Password Key (KPW)

In the RCFM, KPW is the initial key of the system, i.e., K0. Its content significantly affects system security. To generate KPW, we expand PW following three principles. (1) The original content of PW is reserved; (2) The expansion code is generated based on the original content of PW; (3) When the same character repeatedly appears in PW, the expansion code corresponding to each of them varies.

Algorithm 1: generating KPW from PW by the method of dynamically accumulated shifting substitution, mentioned above.

Input: PW.

Output: KPW

1) Find the length of PW, i.e., l in bytes;

2) If l < 8 or l>16, then request the user re-input a PW; /*8 16 ≤ ≤l */

3) If l=16, then KPW = PW, and stop;

4) n=16 – l; ct=l; KPW = Null; SS = Null;

5) For i = 1 to n SS = Mid(PW,i,1); /*the i-th character*/ ct = ct + Fct(SS); Generate SB from SS and ct by the method of dynamically accumulated shifting substitution. KPW = KPW //SS//SB; Next i

6) KPW = KPW //Right (PW, l – n) 7) END.

3.3 Message and Key Encryption/Decryption

3.3.1 Initial process

1) Input PW (or KCH);

2) If the input is PW

then generate KPW from PW by invoking Algorithm 1 and

K0=KPW; else K0=KCH;

3) Calculate the number of binary digit of 1s in K0 , e.g., ct0;

4) Generate K1 from K0 and ct0 by the method of dynamically accumulated shifting substitution;

5) $K2 = K0 +_2 K1$; (1)

6) Calculate the number of binary digit of 1s in K2 , e.g., ct1;

7) $ct2 = ct0 + ct1$;

8) Generate K3 from K2 and ct2 by the method of dynamically accumulated shifting substitution;

9) $K4 = (K0 +_2 K3) \oplus K2$; (2) $K5 = (K1 \oplus K4) +_2 K2$; (3)

10) Generate Δh, $3 \leq \Delta h \leq 3072$, where $\Delta h=[(K0+2K5) \oplus (K1+2K4) \oplus (K2+2K3)] \bmod 3070+3$; (4)

11)END

3.3.2 Encryption process:

The encryption process has three steps.

Step 1: Generating RK and CRK

1) Generate the zeroth random Key RK0;

2) Fetch CPU time; generate current time key KCT and the reverse of the current time key KRCT;

3) Generate the random encryption key RK where $RK = (RK0+2KCT) \oplus (RK0 \oplus KRCT)$ ----(5)

4) Encrypt RK to obtain CRK, where $CRK=[(RK+2K1) \oplus K4] \oplus [(K2 \oplus K3)+2 K5]$; ----(6)

Step 2: Generate internal feedback-code and ciphertext

1) Let plaintext be P1P2…Pn, and let ciphertext be C1C2…Cn.

2) Input the plaintext block Pi, $1 \leq \leq i$ n ;

3) $b0 = K4; C0 = K3$;

4) For i = 1 to n $bi = (Pi \oplus bi-1) +2[(Ci-1 \oplus K5) +2bi-1]$ (7) $Ci=[(Pi \oplus bi-1)+2(RK \oplus bi-1)] \oplus [(Ci-1 \oplus K5)+2bi-1]$; ------- (8) .

5) $\Delta t=[(K2+2RK) \oplus K5+2(K4 \oplus RK)] \bmod 2046+3$; ----- (9)

The plaintext encryption process is shown in Figure 1.

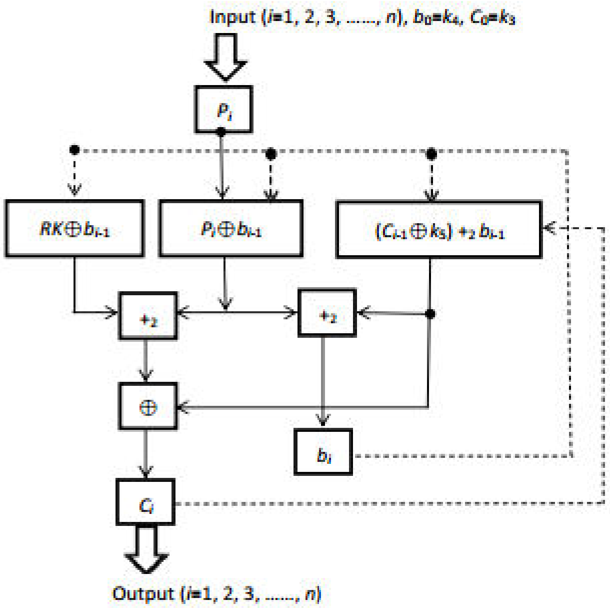
Input (i=1, 2, 3, ……, n), b_0=k_4, C_0=k_3
P_i
$RK \oplus b_{i-1}$
$P_i \oplus b_{i-1}$
$(C_{i-1} \oplus k_5) +_2 b_{i-1}$
$+_2$
$+_2$
$\oplus$
b_i
C_i
Output (i=1, 2, 3, ……, n)

Figure 1: the plaintext encryption process.

Step 3: Generating PRNS1 and PRNS2

1) Generate a random key RK1;

2) Input RK1, Δh and Δt into a pseudo random number generator(PRNG) to obtain PRNS1 and PRNS2;

Step 4: Generate the cladded ciphertext file, the format of which is shown in Figure 2.

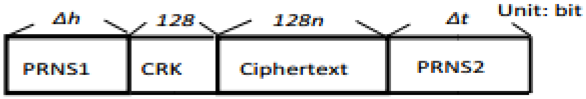

Figure 2: The format of the cladded ciphertext file

3.3.3 Decryption process:

The decryption is as follows.

1) Execution the Initial process to generate K1~K5 and Δh;
2) Remove PRNS1 from the cladded ciphertext file;
3) Fetch CRK from the remaindering file and remove it from the file;

4) Decrypt CRK to obtain RK, where $RK=[CRK\oplus((K2\oplus K3)+2K5)]\oplus K4-2K1$; (10)
5) $\Delta t=[(K2+2RK)\oplus K5+2(K4\oplus RK)] \bmod 2046+3$;
6) 6) Delete PRNS2 from the remaindering portion of the file to obtain the ciphertext; b0 = K4; C0 = K3;
7) Let n be the length of the ciphertext being 128 bits as a unit;
8) For i = 1 to n $Pi = [Ci\oplus((Ci-1\oplus K5)+2\ bi-1)]-2(RK\oplus bi-1)\oplus bi-1$; (11) $bi = (Pi\oplus bi-1)+2[(Ci-1\oplus K5)+2\ bi-1]$; (12)
9) Output the plaintext block Pj, $1 \geq \leq j$ n ;

IV. CONCLUSION AND FUTURE STUDIES

Generally, our projected strategy is created hooked in to the shopper secret word or channel key by utilizing a cladded criticism thanks to cater to build exceptionally secure and elite cladded ciphertext records. The dynamic cryptography strategy, that uses discretional variety keys and current time keys, whereas accretive the equivalent plaintext at numerous time focuses can manufacture numerous cladded ciphertext records of assorted substance and lengths, during this means exceptionally upgrading the safety of knowledge. hypothetic examination demonstrates that the RCFM is secure for info remote transmission or for individual records cryptography. The speed of encryption/unscrambling of the RCFM on a record larger than 128kb is around multiple times faster than that of AES. Since the transfer speed of 4G is regarding 7~10 occasions that of 3G [15], and, with the fast advancement of science and innovation, a better transmission speed is traditional, whereas maintaining the state of helpful security. Our future analysis can focus on increase a faster encryption/unscrambling strategy. in addition, once a shopper overlooks the key key, he/she cannot reinstate the plaintext from the ciphertext, on these lines inflicting hopeless loss of the encoded records. During this means, a protected and superior "overlooked secret phrase healing component", is needed. Whereas dominating the key phrase, the important shopper will pursue the means that of the instrument to firmly recoup the primary plaintext. These establish our future investigations.

References

[1] Wiki, the EFF DES cracker. http://en.wikipedia.org/wiki/EFF_DES_cracker.

[2] A. Bogdanov, D. Khovratovich, and C. Rechberger, “Biclique Cryptanalysis of the Full AES,” Proceeding of Annual International Conference on the Theory and Application of Cryptology & Information Security , pp. 344-371, 2011.

[3] Y.-L. Huang, F.-Y. Leu, J.-H. Chen, W. C.-C. Chu, and C.-T. Yang, “A True Random-Number Encryption Method,” the Seventh International Conference on Innovative Mobile and Internet Services in Ubiquitous Computing, pp. 654-659, 2013.

[4] Y.-L. Huang, C.-R. Dai, F.-Y. Leu and I. You, “A Secure Data Encryption Method Employing a Sequential-logic Style Mechanism for a Cloud System,” International Journal of Web and Grid

Services, vol. 11, no. 1, pp. 102-124, January 2015.

[5] National Institute of Standards and Technology, Advanced Encryption Standard, NIST FIPS PUB 197, 2001.

[6] WIKI, Advanced Encryption Standard http://en.wikipedia.org/wiki/Advanced_Encryption_Standard. [7] Federal Information Processing Standards Publication 197, "Announcing the Advanced Encryption Standard (AES)" November 26, 2001.

[8] J. Daemen and V. Rijmen, "AES Proposal: Rijndael," the First Advanced Encryption Standard Candidate Conference, NIST, September 1999.

[9] J. Daemen and V. Rijmen, "The Design of Rijndael: AES - The Advanced Encryption Standard," Information Security and Cryptography, Springer 2002, ISBN 3-540-42580-2.

[10] Y.-L. Huang, F.-Y. Leu, I. You, Y.-K. Sun, and W. C.-C. Chu, "A Secure Wireless Communication System Integrating RSA, Diffie-Hellman PKDS, Intelligent Protection-key Chains and a Data Connection Core in a 4G Environment," Journal of Supercomputing, vol. 67, no. 3, pp. 635-652, 2014.

[11] Y.-L. Huang and F.-Y. Leu, "Constructing a Secure Point-toPoint Wireless Environment by Integrating Diffie-Hellman PKDS RSA and Stream Ciphering for Users Known to Each Other," Journal of Wireless Mobile Networks, Ubiquitous Computing, and Dependable Applications, vol. 2, no. 3, pp. 96- 107, September 2011.

[12] Y.-L. Huang, F.-Y. Leu, and K.-C. Wei, "A Secure Communication Over Wireless Environments by Using a Data Connection Core," Journal of Mathematical and Computer Modelling," vol. 58, no. 5-6, pp. 1459-1474, 2013.

[13] Y.-L. Huang, F.-Y. Leu, J.-C. Liu, and J.-H. Yang, "A Block Cipher Mode of Operation with Two Keys," Proceeding of Information & Communication Technology-EurAsia Conference, pp. 392-398, 2013.

[14] L. Cui and Y. Cao, "A New S-Box Structure Named AffinePower-Affine," International Journal of Innovative Computing, Information and Control, vol. 3, no. 3, pp. 751-759, June 2007.

[15] ComputerWorld, 3G vs. 4G: Real-world speed tests. http://www.computerworld.com/article/2511923/wirelessnetworking/3g-vs-4g-real-world-speed-tests.html?page=2