International Journal of Electrical and Computer Engineering (IJECE)
Vol. 9, No. 1, February 2019, pp. 352~358
ISSN: 2088-8708, DOI: 10.11591/ijece.v9i1.pp352-358

Implementation of message authentication code using DNA-LCG key and a novel hash algorithm

Gurpreet Kour Sodhi[1], Gurjot Singh Gaba[2], Lavish Kansal[3], Mohamed El Bakkali[4], Faisel Em Tubbal[5]
[1,2,3]School of Electronics and Electrical Engineering, Lovely Professional University, India
[4]Signals, Systems & Components Lab., Fac. of Sciences & Tech., Sidi Mohamed Ben Abdellah University, Morocco
[5]School of Electrical, Computer and Telecommunications Engineering, University of Wollongong, Australia
[5]School of Computing, Engineering and Mathematics, Western Sydney University, Australia
[5]Technological Projects Department, the Libyan Centre for Remote Sensing and Space Science, Libya

Article Info

Article history:

Received Feb 18, 2018
Revised Aug 20, 2018
Accepted Aug 30, 2018

Keywords:

Data integrity
Hash
Linear congruential generator
Message authentication code
message digest, security

ABSTRACT

With the introduction of electronic form of data, the need for an automatic system of security to protect the integrity of data while being transferred from one place to another is required. This is especially the case for a network in which the systems are accessed over a public network or internet. Security mechanisms involve the use of more than one algorithm. They further require that the participants should possess a secret key, which raises issues about creation, distribution and proper usage of these keys. The most effective technique used in provisioning security is Message Authentication Code (MAC) which helps in preserving integrity. MAC involves the use of secret key along with a hash algorithm. In this paper, we present an implementation of MAC using a secret key created by Deoxyribonucleic Acid (DNA) and random output sequence of Linear Congruential Generator (LCG). The hash algorithm used is made more robust by adding complexity to the traditional SHA-160. The presented scheme RMAC (Robust Message Authentication Code) is tested on National Institute of Science and Technology (NIST) test suite for random numbers, avalanche criteria and resistance towards network attacks. The results reveal that the scheme is efficient and is applicable for a variety of security demanding environments.

Corresponding Author:

Lavish Kansal,
Department of Electronics and Electrical Engineering,
Lovely Professional University,
Jalandar, Punjab, India.
Email: lavish.15911@lpu.co.in

1. INTRODUCTION

Security aspects come into picture when there is a need to protect the information from an adversary who may be a threat to data authentication, confidentiality or integrity [1]. Various techniques like digital signatures are used for authentication purpose; encryption provides data confidentiality and data integrity is preserved using MAC [2]. MAC falls into two categories; those involving the use of secure hash algorithm known as HMAC [2] and those based on symmetric block cipher (CMAC).Typically most of the Hash algorithms use a compression function, which is a combination of binary and logical operations [2].

The composition of a MAC algorithm explain in (1). It takes a message and a secret key as input and produces an authentication code as output.

$$MAC = C(K, M) \quad (1)$$

where, M: Input Message

C: MAC Function
K: Shared Secret Key
MAC: Message Authentication Code

The integrity of the received message is verified at the receiver end, as the recipient posses the secret key which can be used to generate the authentication code again and thus, comparing it with the one received. A popular form of MAC [2] uses a cryptographic hash function; the secret key can either be given as an input along with the hash or it can be embedded in an existing hash algorithm.

Various researches have been reported with enormous protocols of data security in the last few decades [2]. An implementation of Advanced Encryption Standard (AES) algorithm on a microcontroller for securing data in a small scale network has been presented in the past [3]. Sofia [4] presents a biometric based MAC algorithm called WBAN, which can be applied to assure data authenticity and integrity in a wireless body network. Dilli and Chandra [6] presented another scheme which uses HMAC SHA 256 Algorithm for message authentication and data integrity. Hans, Christian and Ulrich implemented a heterogeneous flexible computing platform for the network nodes, i.e. the Universal MAC (UMAC) using Universal Hashing [3]. Verma and Prajapati [6] present a novel SHA that possess less execution time and better bit difference value, this can be impleted in order to increase the security.

Security is a broader term which involves three requirements; Authenticity, Confidentiality and Integrity. Authenticity ensures that the received message is authorized and has been received from the intended party, confidentiality is prevention of data from unauthorized access, and integrity is detecting if the data contents have been altered by an unauthorized party [3]. Usually data integrity provides methods include the use of a shared key and a hash algorithm forming a MAC. In this scenario, the data sent by the source has a tag appended with it which is the result of a MAC function and is known as a Message Digest (MD). At the receiver end, the hash is again computed and then compared with the received value. If the received and the computed one are same then the message received is concluded to be unaltered else there has been a modification. This is formulated on the basis of the principle concept of MAC, which says that the MAC value is a unique representation of a data value and it cannot be same for two different values. MAC constructed from block cipher like DES, are called MAC schemes and those which are formed using cryptographic hash function like SHA are called as HMAC schemes [8].

Considering the significance of data integrity, a new MAC scheme RMAC is proposed which involves biological features of the user and LCG sequence as the key, along with a novel hash algorithm. The algorithm integrates a crypto-hash function along with a biometric key generation technique which involves the use of the DNA characteristics and LCG sequence [9].

2. PROPOSED ALGORITHM

Data integrity is preserved using MAC which is a function of a secret key and a hash algorithm. RMAC uses a novel hash algorithm which follows the basic structure of SHA-160 and has an 'f' function integrated into it along with a secret key that has been produced using a DNA sequence and LCG output random sequence. The details are explained in the following subsections:

2.1. Novel hash algorithm

The novel hash algorithm used in this scheme is an outcome of the 'f' function embedded in the basic structure of SHA-160 that consists of 80 rounds and for every 20 rounds, a constant 'K' is used as an input. So, there are total four 'K' values, each of which is an eight digit hexadecimal value. The MD produced is of 160-bits. The 'f' function used in the algorithm constitutes of three operations; Expansion (EXP), S-Box substitution (S) and modulo 2^{48} addition (+) applied on the five register values (A, B, C, D, E) [10]. The structure of the proposed hash algorithm is explained using Figure 1.

2.2. DNA-LCG based secret key:

The proposed hash algorithm is applied on the message input along with the secret key. The secret key used in the presented technique is deduced using the characteristics of DNA. The DNA is represented in the form of a sequence constituting of 'agct' characters adhering to a unique paradigm for every individual. The characteristic uniqueness of a DNA sequence makes it impossible to be replicated or stolen.

To enhance the efficacy of the secret key, a random number generator LCG is used which produces a random output sequence of 256-bits; this output sequence is a result of the secret seed value given as an input to the random number generator. The DNA sequence is converted into its binary form and exclusive-or operation is applied between DNA and LCG sequence. The result is a 256-bit key, which is used in the formation of RMAC [9].

2.3. Formation of RMAC

MAC is also known as keyed Hash i.e. a hash algorithm which requires a secret key to operate. The generated DNA-LCG key is of 256-bits and in order to use it in RMAC, it needs to be converted into four 32-bit keys. This conversion is done using few operations on the 256-bit key, which are explained using Table 1. Figure 2 explains the operations applied on DNA-LCG key in order to obtain four keys, which are to be used in MAC

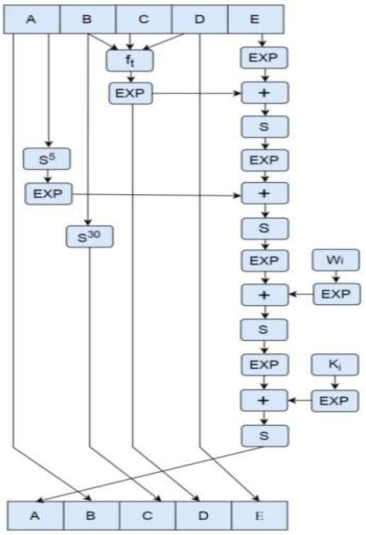

Figure 1. A novel hash algorithm [11]

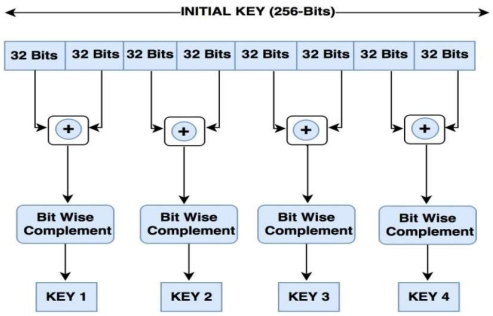

Figure 2. Operations applied on DNA-LCG key

Table 1. Pseudo Code for Operations

```
Y= initial key of 256-bits
for i=0:7                    //splitting the key into 8 parts of 32-bit each
x(i+1,:)= Y(32*i+1:32*(i+1))
end
for j=1:4 //Applying exclusive-or operation between each consecutive pair forming four 32-bit
sequences and then complementing the results.
k(j)= ~xor (x(2*j-1,:), x(2*j,:))
end
//k represent the key//
//The four key values are converted into hexadecimal form before being used in MAC//
```

The four final keys in hexadecimal form are shown in Table 2. These four keys are replaced with the four 32-bit constant values used in elderly SHA-160 [10]. This frames a RMAC algorithm. The MAC values obtained, using the proposed technique are presented in Table 3. The obtained MAC values are converted into binary form and evaluated on randomness and avalanche criteria.

Table 2. Security Key

Key no.	32-bit Keys (Hexadecimal)
K_1	F270633E
K_2	BDB5DC13
K_3	591C502C
K_4	3A404009

Table 3. MAC Values

Input	Input (Hex.)	MAC Values (Hexadecimal)
g	67	5caeebc819a2162167c042a9571bd535b8c80ed0
Sodhi	536f646869	1afbefabcc370d6d080e7a0c603313598ed17876
unitedstates	56e69746564 737461746573	b12f957691b3161f7a5e56b3e58ceddf1c1c8f4c

3. RESULTS AND DISCUSSIONS

The performance of RMAC is analyzed on the basis of NIST tests of randomness and avalanche criteria. This is done for three inputs values having varying lengths. These tests compute the P-value for a binary sequence; which must be greater than 0.01 for a sequence to be declared as random sequence [12]. The simulations have been carrierd out on MATLAB. The computed values for RMAC under various tests signifies the efficiency of the proposed technique and signifies its applicability in practical sensrios. In order to certify the efficiency of our presented scheme, the NIST results of RMAC are compared with those of the traditional ones. The eight digit hexadecimal key used for these algorithms is '3A54E26B', which is kept constant throughout for all the traditional techniques. A brief overview of the various NIST tests is given as:

a. Frequency Test

This test computes the ratio of the number of ones and zeros in a sequence. It observes the closeness between the number of ones and zeros. A sequence is random if the proportion of both is close to each other [12]. The results in Table 4 illustrate that the proposed algorithm produces better proximity between the count of ones and zeros as compared to most of the other schemes.

Table 4. NIST Test Results for Frequency Test

Hash Technique	P-values		
	g	Sodhi	unitedstates
MD2	0.3768	0.3768	0.4795
MD5	0.8597	0.5959	0.8597
SHA-160	0.8744	1.0000	0.8744
SHA-256	0.2606	0.9005	0.0801
SHA-384	0.2207	0.1258	0.3074
SHA-512	0.7909	0.9296	0.9296
RMAC	0.8884	0.9776	0.9289

b. Binary Derivative Test

The Binary Derivative Test proceeds by applying exclusive-or operation between consecutive bits of a sequence until only one bit is left. Then, the ratio of number of ones to the total length of the sequence in each case is computed. Lastly, the average of the ratio for all the sequences is calculated, if this value lies near to 0.5, the sequence is said to be random [12]. The results in Table 5 depict that the output of the proposed scheme is random.

Table 5. NIST Test Results for Binary Derivative Test

Hash Technique	P-values		
	g	Sodhi	unitedstates
MD2	0.4952	0.5126	0.5016
MD5	0.5129	0.4901	0.5149
SHA-160	0.5069	0.4924	0.5026
SHA-256	0.5046	0.5007	0.5040
SHA-384	0.5005	0.4964	0.4993
SHA-512	0.5026	0.5034	0.4987
RMAC	0.5191	0.5138	0.5121

c. Discrete Fourier Transform Test (DFT)

The DFT test finds the peak heights in the DFT of a sequence. It determines the presence of identical patterns in the sequence which indicates a deviation from the assumed randomness. The aim is to

check if more than 5% of the peaks exceed the 95% threshold. The results for DFT test are summarized in Table 6.

Table 6. NIST test results for DFT test

Hash Technique	P-values		
	g	Sodhi	unitedstates
MD2	0.1443	0.0940	0.3304
MD5	0.8711	0.5164	0.0744
SHA-160	0.1468	0.4682	0.0295
SHA-256	0.4220	0.4220	0.1359
SHA-384	0.7787	0.7787	0.5121
SHA-512	0.3723	0.2561	0.6265
RMAC	0.8763	0.7812	0.6192

d. Approximate Entropy Test

The motivation of this test is to calculate the frequency of all the overlapping bit patterns existing in the sequence. It compares the frequency of overlapping blocks of two sequential lengths with the expected outcome for a random sequence. The results are given in Table 7.

Table 7. NIST test results for Approximate Entropy test

Hash Technique	P-values		
	g	Sodhi	unitedstates
MD2	0.7464	0.7727	0.7310
MD5	0.4533	0.8983	0.8863
SHA-160	0.9288	0.8835	0.9883
SHA-256	0.8330	0.9440	0.9587
SHA-384	0.9817	0.9836	0.9865
SHA-512	0.9949	0.9891	0.9855
RMAC	0.9929	0.9889	0.9885

e. Maurer's "Universal Statistical" Test

This test focuses on finding out if a sequence can be compressed without any loss of information. A sequence is said to be random if it is not compressible [12]. The results are summarized in Table 8.

Table 8. NIST Test Results for Maurer's Test

Hash Technique	P-values		
	g	Sodhi	unitedstates
MD2	0.9268	0.9528	0.9553
MD5	0.9831	0.9833	0.9951
SHA-160	0.9713	0.9600	0.9255
SHA-256	0.9912	0.9599	0.9705
SHA-384	0.9774	0.9909	0.9913
SHA-512	0.9865	0.9909	0.9765
RMAC	0.9923	0.9916	0.9914

As observed from Table 4 to Table 8 RMAC performs better by passing the NIST criteria of generating a random MAC. Thus, indicating its efficiency as a MAC technique. The purpose of MAC is to preserve data integrity and to significantly detect any change in the message [13]. Also, a particular MAC is unique for particular data content and thus it can indicate any change in the data. Thus, a change can be observed in a particular MAC value if the data file is altered [14]. To study this parameter, another test has been applied to the RMAC values, this is the Avalanche Test. This test calculates the avalanche effect i.e. the change in the output with respect to a change in the input, which is calculated using the formula given in (2). The input consists of 128-bits.

$$\text{Avalanche Effect} = \frac{\textit{No.of bits flipped}}{\textit{Total no.of bits in the sequence}} \times 100 \quad (2)$$

The more the avalanche effect, better is the efficiency of the algorithm. This test has been applied by altering a single character of the input value. The Avalanche Test results are summarized in Table 9.

Table 9. Avalanche Test

Original Input	Altered Input	No. of bits Flipped	Avalanche effect
g	P	88	51.87
Sodhi	Sodhb	79	49.37
unitedstates	Unitedstraten	80	50.00

It is observed that RMAC performs well under this criteria too, thus demonstrating its efficiency. The increased complexity of RMAC makes it highly resistive towards various network attacks on data integrity, a brief summary analysing the behaviour of the technique is presented in Table 10 [15]. The RMAC algorithm is complex and therefore is highly resistive towards various attacks on integrity, thus increasing its applicability in a data sensitive environment.

Table 10. Resistance against Attacks

Network Attacks on Integrity	Preventive Features
Salami attacks	As observed from the avalanche test analysis, a small change in the input results in a major change in the output. Hence, even the minute modification in the data would be detected.
Data diddling Attacks	Since the proposed scheme uses biological characteristics to frame the secret key, therefore it is not possible for the data to be modified by an unauthorized party.
Man-in-the-middle attacks	The proposed technique is hash based, thus it is highly resistive towards any unauthorized alterations in the transmitted data.
Seed Attacks	Keys generated using only the random number generator outputs are susceptible towards seed attacks; the key used in the proposed MAC is a result of fusion of DNA and random number generator output, thus increasing its resistance towards seed attacks.

4. CONCLUSION

This paper presents an efficient MAC technique which is a result of a novel hash algorithm and a secret key generated using DNA and LCG. MAC also known as cryptographic checksum is an authentication technique which uses a hash technique along with a secret key to preserve data integrity and validate the source. The RMAC involves the use biometric characteristics along with a novel hash algorithm to frame the MAC, thus increasing its efficiency. The analysis of the results concludes that the proposed algorithm has higher complexity than most of the other schemes and thus performs better than most of the existing HMAC schemes such as MD2, MD5, SHA-160, SHA-256, SHA-384 and SHA-512. This scheme uses a secret key which involves DNA characteristics of the user, thus making it considerably more reliable and resistive towards attacks. The proposed RMAC scheme can be effectively used in various cryptographic techniques for data integrity and better security.

REFERENCES

[1] A.H. Poursoltan, M. Chehel, F. Faghihi, "Presentation of an Algorithm for Secure Data Transmission based on Optimal Route Selection during Electromagnetic Interference Occurrence", *International Journal of Electrical and Computer Engineering,* vol. 8, no. 1, *pp.* 259-270, 2018.

[2] P. Gayathri, S. Umar, R. Srikanth, "Hybrid Cryptography for Random-key Generation based on ECC Algorithm", *International Journal of Electrical and Computer Engineering*, vol. 7, no. 3, pp.1293-1298, 2017**.**

[3] H. Zhong and L. Shao, "A Lightweight and Secure Data Authentication Scheme with Privacy Preservation for Wireless Sensor Networks", *International Conference on Networking and Network Applications (NaNA)*, pp. 210 – 217, 2016.

[4] N. R. Sofia, M. F. Abdollah and E. Dutkiewicz, "A Biometric-Based Security for Data Authentication in Wireless Body Area Network (WBAN)". *Proceedings of the 15th International Conference on Advanced Communications Technology (ICACT)*, pp. 998 – 1001, 2014.

[5] C.S. Koong, T.Yang and C. Tseng, "A User Authentication Scheme Using physiological and Behavioral Biometrics for Multitouch Devices", The Scientific World Journal Research Article, Tung University, Hsinchu, Taiwan.

[6] R. Dilli and S. Chandra, "Implementation of HMAC-SHA 256 Algorithm for Hybrid Routing Protocols in MANETs", *Proceedings of the IEEE International Conference on Electronic Design, Computer Networks & Automated Verification (EDCAV),* pp. 154 – 159, 2015.

[7] S. Verma and G. S. Prajapati, "Robustness and Security Enhancement of SHA with Modified Message Digest and Larger Bit Difference", *IEEE Symposium on Colossal Data Analysis and Networking (CDAN),* pp.1-5, 2016.

[8] G. K. Sodhi and G.S. Gaba, "An Efficient Hash Algorithm to Preserve Data Integrity", *Journal of Engineering Science and Technology*, vol. 13, no. 3, pp. 778-789, 2018.

[9] G. K. Sodhi and G. S. Gaba, "DNA and BBSG Based Security Key Generation Algorithm", *International Journal of Security and its Applications*, vol. 11, no. 4, pp. 1-10, 2017.

[10] W. Stallings, "Cryptography and Network Security: Principles & Practices", New York, NY: Pearson Education, pp. 752, 2014.

[11] D. Eastlake and T. Hansen, RFC, "Network Working Group," SHA-160, 2006.

[12] A. Rukhin, J. Soto, J. Nechvatal, M. Smid, E. Barker, S. Leigh, M. Levenso. M. L. Vange, D. Banks, A. Heckert, J. Dray and L. E. BasshamIII, "A Statistical Test Suite for Random and Pseudorandom Number Generators for Cryptographic Applications", 2010.
[13] P. L. Hans, L, Christian and R.C.S.Ulrich, "UMAC-A Universal MAC Architecture for Heterogeneous Home Networks", *Proceedings of the IEEE International Conference on Ultra Modern Telecommunications & Workshops*, pp. 1-6, 2009.
[14] C. Mavromati, "Key-recovery Attacks against the MAC Algorithm Chaskey", *Springer, International Conference on elected Areas in Cryptography*, pp. 205-216, 2015.
[15] Wongnarukane, Nakinthorn, Kuacharoen, Pramote, "The Security Challenges of the Rhythmprint Authentication", *International Journal of Electrical & Computer Engineering*, vol. 8, no. 3, pp. 1281-1287, 2018.

BIOGRAPHIES OF AUTHORS

Gurpreet Kour Sodhi, has completed her Masters in Electronics and Communication Engineering from Lovely Professional University. Her research area includes - 'Enhancing and Maintaining Security in Wireless Communication Systems' and 'Networks'. She is working in this field since 2015 and has potential to resolve several problems of industry through her expertise.

Gurjot Singh Gaba is currently pursuing Ph.D. in Electronics & Electrical Engineering with Spl. in Cryptography and Network Security of WSN and IoT's. He is working as an Asst. Prof. in Lovely Professional University since 2011. His research interest includes Wireless Sensor Networks, Computer Networks, Optical Communications and Network Security. He is currently engaged in the project of 'Micro Satellite'. He is an author of 8 monographs, published 66 research papers (co-authored with 62 researchers), and filed 2 patents. He has been awarded with the LPU Chancellor Award for Research Excellence in the year 2016 and 2017 consecutively (Most prominent award) and Teacher Appreciation Award in the year 2016 by Union Minister of Human Resource and Development, India, Ms. Smriti Zubin Irani. He has reviewed articles of 50 Journals/conferences. He is associated with 8 technical organizations such as ISCA, Former IEEE, IAENG, IACSIT, CSI, ISTE, ACM, ISDS Society, GIAN. He has referred students to almost 25 International top Universities and is also an active member of various NGO's.

Lavish Kansal, is a passionate researcher in the field of wireless communication. He received his B.Tech degree in Electronics and Communication Engineering from PTU, Jalandhar in 2009 and M.E. degree in Electronics and Communication Engineering from Thapar University, Patiala in 2011. He is currently pursuing his Ph. D. from IKG PTU Jalandhar. He is working as Assistant Professor in the department of Electronics and communication Engineering, Lovely Professional University, Phagwara, India. He has published 35 papers in International journals. His research area includes Digital Signal Processing, Digital Communication & Wireless Communication.

Mohamed El Bakkali, was born in Morocco. He received his B.S. in physics, and M. S. in Control Engineering, Signals & Systems, from Sidi Mohamed Ben Abdellah University, Fez, Morocco, 2014, 2016. He is currently working toward his PhD thesis entitled "Design of Efficient Multiband Antennas with Parasitic elements for CubeSat Applications" in the signals, systems and components laboratory of FST-Fez. His major research interests design of planar antennas with parasitic elements for CubeSat Satellites, and stability and stabilization of bilateral teleoperation systems using Lyapunov-Krasovskii functional approaches.

Faisel Em Tubbal, was born in Libya in 1978. He received the B.S. degree in electronics engineering from the Tripoli College of Electronic Technology, Ben Ashour, and Tripoli, Libya. In 2011, he obtained an Advanced Graduate Diploma in Technology Engineering from the University of Wollongong. In 2012, he obtained a M.S. degree in Telecommunication Engineering from the University of Wollongong. In 2013, he obtained a M.S. in Engineering Management from the University of Wollongong. He went on to complete his PhD thesis entitled "S-band Planar Antenna Designs for CubeSat Communications" in 2017. He has been a Researcher with the Libyan Centre for Remote Sensing and Space Science, Tripoli, Libya. He is an academic assistant at the School of Electrical, Computer and Telecommunication Engineering, University of Wollongong (UOW), and School of Computing, Engineering and Mathematics, Western Sydney University (WSU), Australia. He is also a full member of the IEEE. Currently, Faisel is the Guest editor of the international open access journal "Technologies (ISSN 2227-7080)". He is interested in planar antenna designs and CubeSat communications.