ISSN: 2454-1907

International Journal of Engineering Technologies and Management Research
June 2020, Vol 7(06), 131 – 140
DOI: https://doi.org/10.29121/ijetmr.v7.i6.2020.705

SECURITY ANALYSIS OF VARIOUS HASH ALGORITHMS FOR AUTHENTICATION UNDER HARDWARE CONSTRAINED ENVIRONMENT

Rashid Husain [1], Rabia Khan [2], Dr. Rajesh Kumar Tyagi [3]

[1] Department of Mathematics and Computer Science, Sule Lamido University, Kafin Hausa, Jigawa State, Nigeria

[2] MCA, Punjab Technical University, India

[3] Department of Computer Science, Amity University, Haryana, India

DOI: https://doi.org/10.29121/ijetmr.v7.i6.2020.705

Article Citation: Rashid Husain, Rabia Khan, and Dr. Rajesh Kumar Tyagi. (2020). SECURITY ANALYSIS OF VARIOUS HASH ALGORITHMS FOR AUTHENTICATION UNDER HARDWARE CONSTRAINED ENVIRONMENT. International Journal of Engineering Technologies and Management Research, 7(6), 131-140. https://doi.org/10.29121/ijetmr.v7.i6.2020.705

Published Date: 27 June 2020

Keywords:
Security Algorithms
Remote Keyless Entry System (RKES)
Authentication Protocols
MAC
Hash Algorithms such as SHA
MD5

ABSTRACT

Protecting passwords is now a big challenge because users want to do all types of work online via user-friendly devices such as mobile, tablets etc. Now, It is difficult to implement the secure heavy weight algorithms such as AES, RSA etc. in hardware constrained devices. It has been observed that users want all types of security services in an online public environment. Authentication is the first and foremost step to enhance security. Various applications are available for real time authentications such as keyless car entry and opening home-doors through security algorithms under remote keyless entry System (RKES). Now, it is the demand of the time to implement the lightweight security algorithms without compromising the security. In order to fulfill this challenge, this paper proposed a strong model for enhancing authentication security. In this work, strong authentication techniques are implemented with the light weight algorithms. This model received good comparison results.

1. INTRODUCTION

Today's era is an information era; everything is being done today by exchange of information. We can say that the present time is a digital millennia [1], [2]. This moving and storing information is classified into two categories, one is structured data and the other is unstructured data. Structured data are following the nomenclature of RDBMS (Relational Database Management Systems) while unstructured data are those, which don't follow the RDBMS rules. In the 21st century, data is called oil because after data mining we can find some important outcomes, results and behaviors [17].

Information is available from anywhere and everywhere and hence we call today's digital era ubiquitous. In this scenario, managing real time authentication is a challenging task. All the communicating nodes are open for the information. So, building a secure real–time authentication model is a challenging task [18].

Small size devices are handy to use and look attractive for easy working but these devices are very prone to security. These small devices have less hardware capability as compared desktops and hence, these small devices are not compatible with much secure symmetric keys algorithms such as DES (Data Encryption Standards) and AES (Advanced Encryption Standards). Hence, due to mismatching of hardware capability with heavy weight security algorithms creates few new problems such as latency and hanging. These problems must be focused and trade-off [19].

It has been observed several times that if we do not put any security on the data and it moves towards the public domain there may be a possibility of capturing the data by hackers, who may already keep an eye on the data and if the information is important then it may be possible that they can copy for future purpose [20]. For example, suppose one customer conducts an online transaction. He entered all his important information on a website such as his credit card/ debit card number with a pin, then it may be possible that some hackers hack that data and steal all the important above information of the respective user, this may cause a lot of financial damage to the users and it will create panic among users [21].

For solving these problems without compromising the users security, Security developers may implement the secure authentication technique. In this way legitimate users can send and receive the information [10].

The Complete Security System requires a standard for which we all know that X.800 is a security service for standardizing the security system and it is defined in RFC 2828 [22]. As per this RFC following are the points to follow for enhancing the security systems:

- Authentication service is that security service on which we come to know that it is the same verified claiming communication unit. It is the responsibility to find out the authorized communicating unit. Login and password/OTP matching are some techniques to verify the correct communicating party.
- Access Control: Secure a resource in such a way that no unauthorized use can be made on it. By this, we can control the user's service as per permission.
- Data confidentiality: Provide protection of information from unauthorized person
- Data integrity: It gives guarantee that information which is received is exactly the same as per authorized sender sent. This service assures that nobody can do modification, insertion, deletion, or replay etc.
- Non-repudiation: - Gives protection against denial by any-one of the communicating parties involved in a communication of having participated in all or some part of the communication.
- These above X.800 security services are very important to judge the security of any system [22].

Information hackers are targeting the users for getting important information from impersonates and this trend is increasing rapidly [16]. They do so by re-programming the interfaces of the communicating channels [11], [12], [13]. Thus, some of the major secure techniques are not able to provide secure systems to the users. It has been proven that any communication system can be exposed to a Scan Attack, Playback Attack, Two-Thief Attack, Challenge Forward Prediction Attack and a Dictionary Attack. Also communicating devices are used fixed algorithms of the security in the transmission process between to and fro which make this vulnerable to replay attack. So in this paper we used a LFSR with a random key sequence which will provide additional safety to these types of attacks [7].

Although there are many techniques like rolling code, fixed code and response challenges for authentication, rolling code authentication is one of the widely used techniques all over the world [11]. But the important factor to understand is that various criminal organizations are there which can build sophisticated techniques for attacking the purpose of these types of systems which are not having tight security [13], [14], [15]. Our proposed work provides security to many of these attacks and in case a user can forget or stolen or lost his password then our model enables a user to change the security code by using one time password(OTP) [13].

Here in this paper, MAC and Hash are two important concepts for implementing the real time security.MAC will be generated with help of a secret key as input and a specified length based message to be authenticated and outputs a MAC (Tag). This specified generated MAC value protects both a message's data integrity and its authenticity, by allowing verifiers to detect any changes to the original message content. To provide privacy, integrity and authenticity to data in any communicating environment, HMAC will be implemented for generating a cipher text which can be sent safely without being worried about the loss of the data. MAC (M, K) is a one-way transformation of the message M and a secret key K is shared with the verifier. Both values M and MAC (M, K) are sent to the verifier to detect any changes to the original message. Upon receiving these values, the verifier generates himself a value MAC (M, K) based on the received M and using the value of K known to him.

Complete process of MAC working is shown in the below figure:1

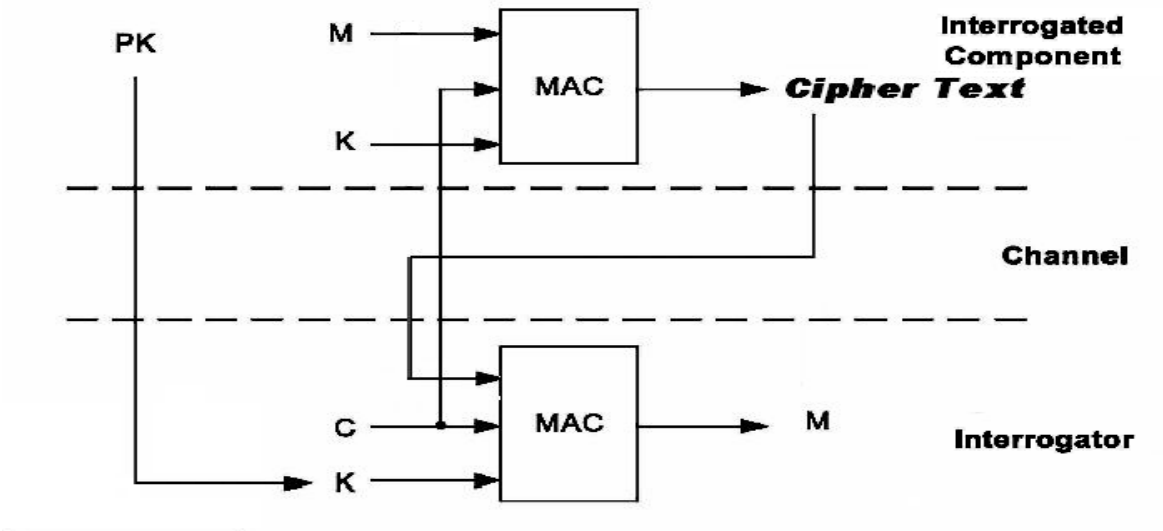

Figure 1: MAC Operations [5]

Claude Shannon introduced two very important security concepts called Confusion and Diffusion. These two techniques enhanced security and thwart cryptanalysis based on statistical analysis. Here with the help of LFSR (Linear feedback shift register) and padding proposed algorithm enhancing the security with the help of confusion and diffusion [22].

Encryption of Linear Feedback System Register (LFSR) is as follows:

Linear feedback shift register is a shift register whose input is a linear function of its previous state. Apply linear feedback polynomials using XOR gates and generates output bits per iteration. Right shift the content of the shift register. Insertion of output bit at most significant bit position

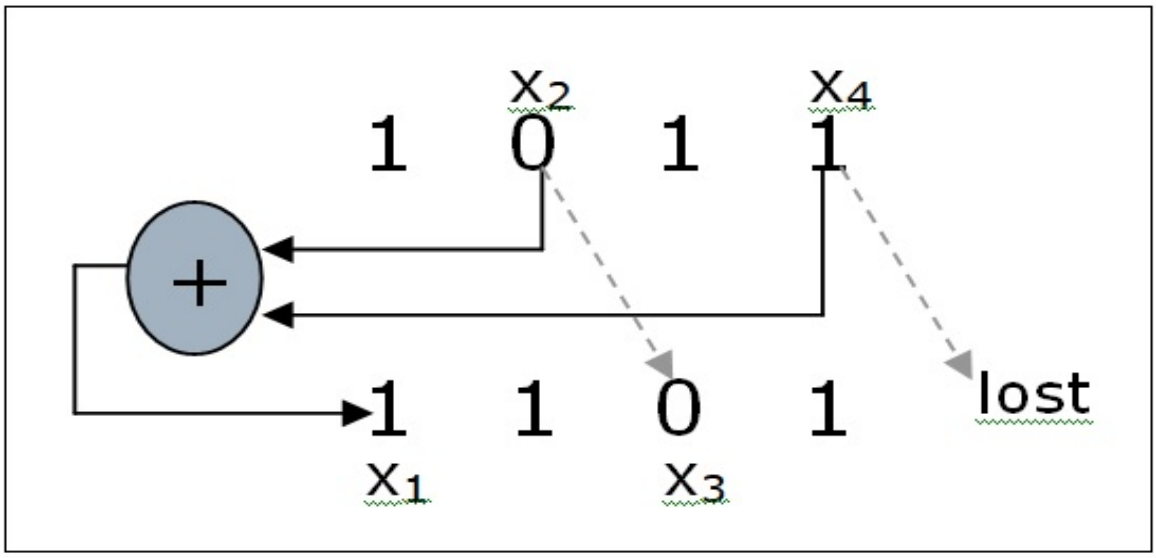

Figure 2: Depicted the encryption process of LFSR

Encryption of Linear Feedback System Register (LFSR) is as follows: Apply modified linear feedback polynomial using XOR gates and generates output bits per iteration. Left shift the content of the shift register. Insertion of output bit at least significant bit position [6].

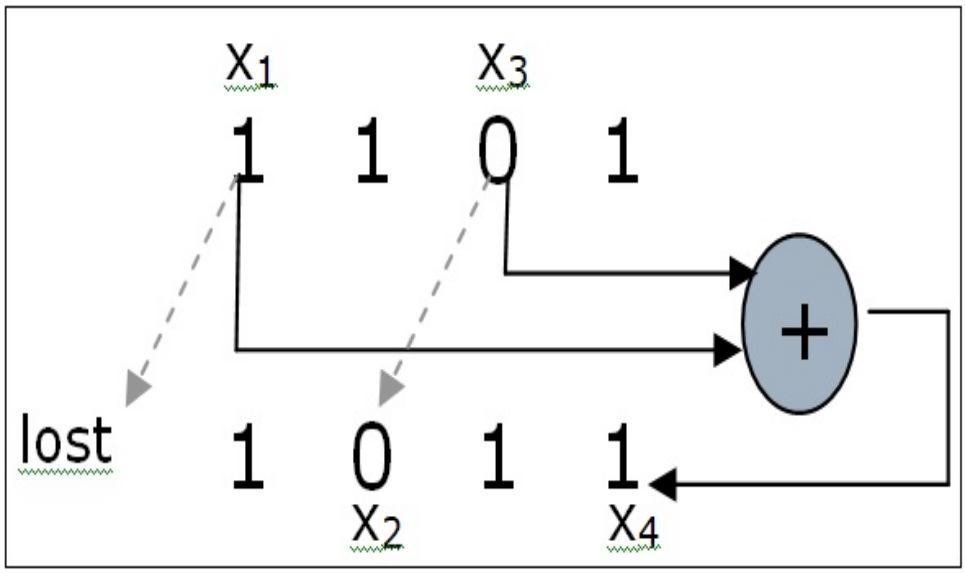

Figure 3: Depicted the decryption process of LFSR

2. LITERATURE REVIEW

Various papers taken into consideration are as follows:

Vanesa Daza and Xavier Salleras (2019) [1] - This paper presents a lightweight and integrated solution for Remote Keyless Entry systems with a secure transmission protocol. Against a popular jamming and replay the solution guarantees a secure communication is guaranteed and attacks are been relayed without any tricky cryptographic algo's and schemes.

Vinita Patel Manic All Das Secular Nandi (2018) [2] - In this paper a new RKE system is proposed after discussing one recent RKE system which overcomes many attacks. The proposed system uses an un clone able security module and manages to defeat the port scan attack of OBD and many other threats known while preserving the privacy of the vehicle.

Tobias Glocker, Timo Mantere, Mohammed Elmusrati (2017) [3] - In the paper, various attacks against a Remote Keyless System are described. The paper proposed a secure protocol which includes a lightweight Symmetric Encryption Algorithm for Remote keyless Entry System.

Flavio D. Garcia,David Oswald,Timo Kasper,Kasper & Oswald GmbH (2016) [4] - In this paper , the various vulnerabilities present in Remote Keyless Entry Systems of worldwide manufacturers. Here, it shows that cloning of remote control and gaining unauthorized access by third parties is done via capturing algorithms of cryptography and electronic control keys.

Ansaf Ibrahem Alrabady and Syed Masud Mahmud (2005) [5] - This paper describes the various attack types on the remote keyless system of vehicles and analyzes these attacks and focuses on how the system will respond under these attacking conditions.

Some other papers are taken into considerations are - “S. Indesteege, N. Keller, O. Dunkelman, E. Biham, and B. Preneel (2008)”, “Ben Davis, Ron DeLong (2005)”, “Amir Moradi and Timo Kasper(2009)”, “O. Akinsanmi, A.D. Usman, A. Abdulraheem, G.D. Obikoya, B.G. Bajoga (2015)”

The article entitled “Automotive remote technology” by Remotes Unlimited, 2019 talks about the remote key fobs for vehicles that use several important technologies to accomplish what they do. Automotive Remotes are both computing devices and radio signal transmitters. And they utilize important encryption concepts to protect your security etc.

3. PROBLEM DESCRIPTION

Traditionally single signal coded remote operated on simple radio frequencies are used for automobiles etc. Here, by pressing the remote button from a little distance (within about 50m) from the vehicle will send a radio frequency signal to the console inside the vehicle. If it matches with the code present in the console then the door will open otherwise not. Then comes the burglary part, the specially designed electronic circuits by burglars will help them in catching the signal code which was obtained by pressing the remote button. Later on they can use the code for creating a duplicate remote. Thus a duplicate remote is ready with burglars for accessing vehicles.

This improvised version consists of several security codes present in both remote and console of vehicle. These codes used here are randomly chosen both in vehicle and remote units. Since, every time a new code will work so the signal caught and duplicate remote creation will be a failure for burglars. However, since the limited numbers of codes are used, the burglar can catch all those and will use them in its remote. So, the present work proposes something different i.e. encrypted system with random sequences of keys for keyless access.

4. METHODOLOGY

Followings are the steps for achieving the above secure objectives:-

Step 1:- In the first step, Communicating Party (A) wants to be challenged by Communicating Party (B). Both the Party (A) and (B) already had stored passwords and also this password can be updated via web application using a one time password methodology. The communication can be done as shown below:

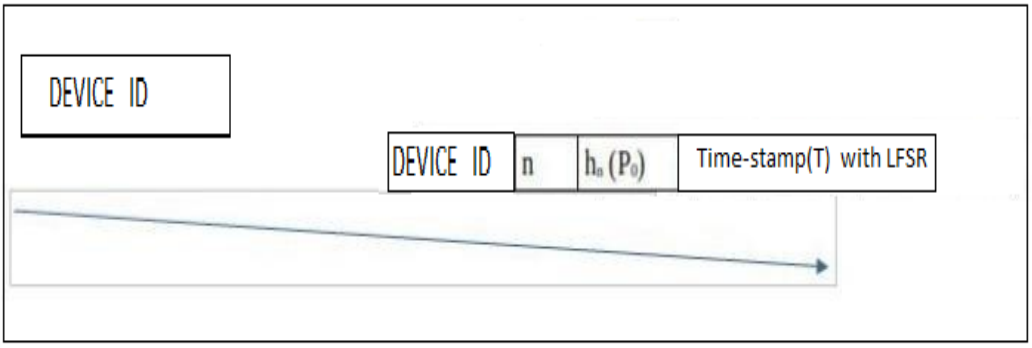

Figure 4: (A) wants to be challenged by (B)

Step 2: - In the second step, Party (B) will share n (random number) and timestamp (T) by applying LFSR with Party (A).

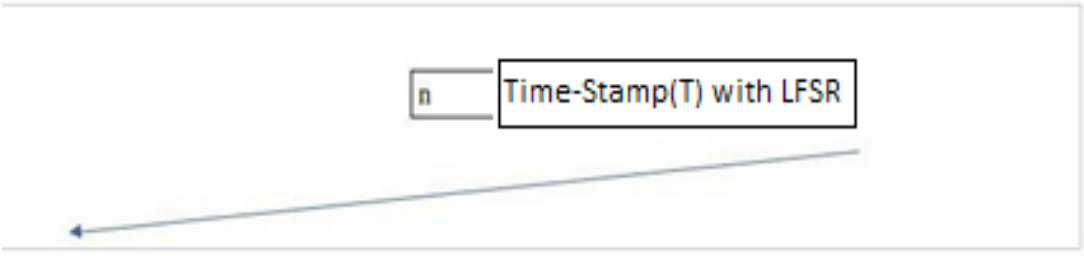

Figure 5: Sharing of n and Time-stamp (T) with LFSR

Step 3: - In Third step, Party (A) will calculate the hash value of the given password by (n-1) times. Therefore mathematically, it would be written as $h_{n-1}(P0)$, where h is called hash and P0 is the password. After calculation of $h_{n-1}(P0)$, it will send it to party (B) for finding the value of $h_n(P0)$ for making a challenge with a unique time-stamp (T) with LFSR.

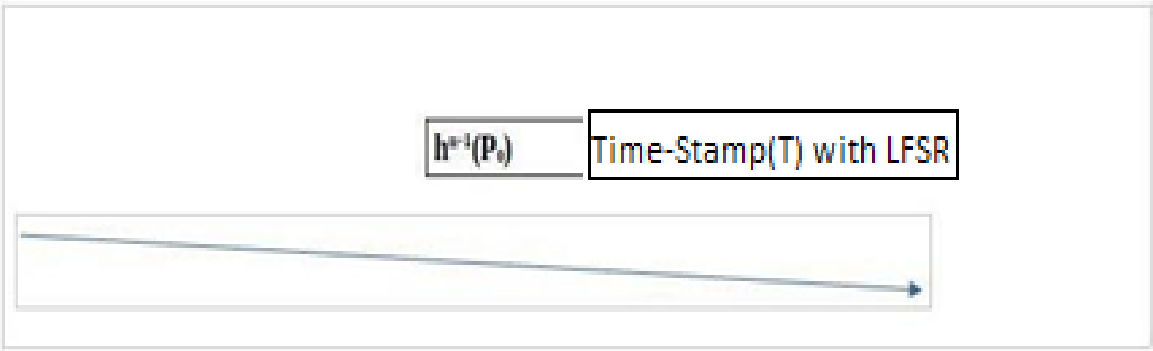

Figure 6: Sending of hash value

Step 4:- In Fourth step, Party (B) will be calculated the hash value of $h_{n-1}(P0)$ again, which will be written as $h_n(P0)$. The party (B) already has one copy of h_n (P0) and the other h_n (P0) will be calculated from the $h_{n-1}(P0)$, which will receive hash value from Party (A). Hence, if receiving one is valid then both should have the same value. If these two values match then the lock of the car will open otherwise not.

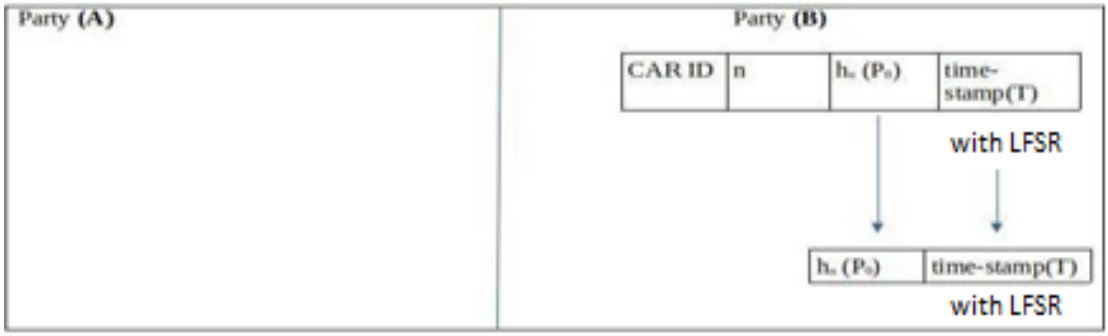

Figure 7: Validation of hash value

These two values must be matched for getting access.

The above principal can be written mathematically as follows: $h_n(x)$ + Time-Stamp(T) with LFSR = $h(h_{n-1}(x))$ + Time-Stamp(T) with LFSR

$h_{n-1}(x)$) + Time-Stamp(T) with LFSR = $h(h_{n-2}(x))$) + Time-Stamp(T) with LFSR

$h_1(x)$) + Time-Stamp(T) with LFSR = h(x) + Time-Stamp(T) with LFSR

In the above shown algorithm, users can easily update password time to time via online or mobile app with one-time password. When the console of receiver party(B) receives a message or signal from sender machines such as remotes etc. then it applies a hash function to the received signal further it matches it to the value which is already stored in its memory. If it faces a match in the two then it will grant access otherwise it will deny it.

Now the system will decrement the value of 'n' which it receives from entry and old password $h_n(P0)$ is replaced by new value h_{n-1} (P0).

So, for the second time when the user tries to access the system, the value of the counter becomes n-1 and it also receives the same, hereby making the third message as $h_{n-2}(P0)$ + Time-Stamp(T) with LFSR from the user side. The concerned part of this technology i.e. it's security is that here users can change all the values such as random (n) and password on its own via web application which they can get access from the developer. This project has been implemented in Python 3.6 and Spyder IDE 3.3.0.

5. RESULTS AND DISCUSSION

Now let's work on the important part of choosing a hash algorithm which will give results faster. Some measurements have been made and the average is calculated. Also, a few cases of strings are taken like some large strings and some small, and a graph is plotted in order of milliseconds that each algorithm will take for generating hash. All these calculations are done on a system of 64 Bits Windows 10 having RAM of 16GB with 1 core Intel i7 2.60 Ghz.

Case 1: To encode 36 characters length data and without any other wastage of time. Cached UUID is taken and time stamp is not taken, some calculations are been made in milliseconds

Table 1: Encoding 49 char string

Different HASH ALGORITHMS	Case 1 (in milliseconds)	Case 2 (in milliseconds)	Case 3 (in milliseconds)	Case 4 (in milliseconds)	Case 5 (in milliseconds)	Case 6 Average Values
SHA-1	630	596	648	610	590	614.8
SHA-256	759	732	754	735	740	744
SHA-512	1086	1093	1065	1065	1066	1075
MD5	666	640	640	666	626	647.6

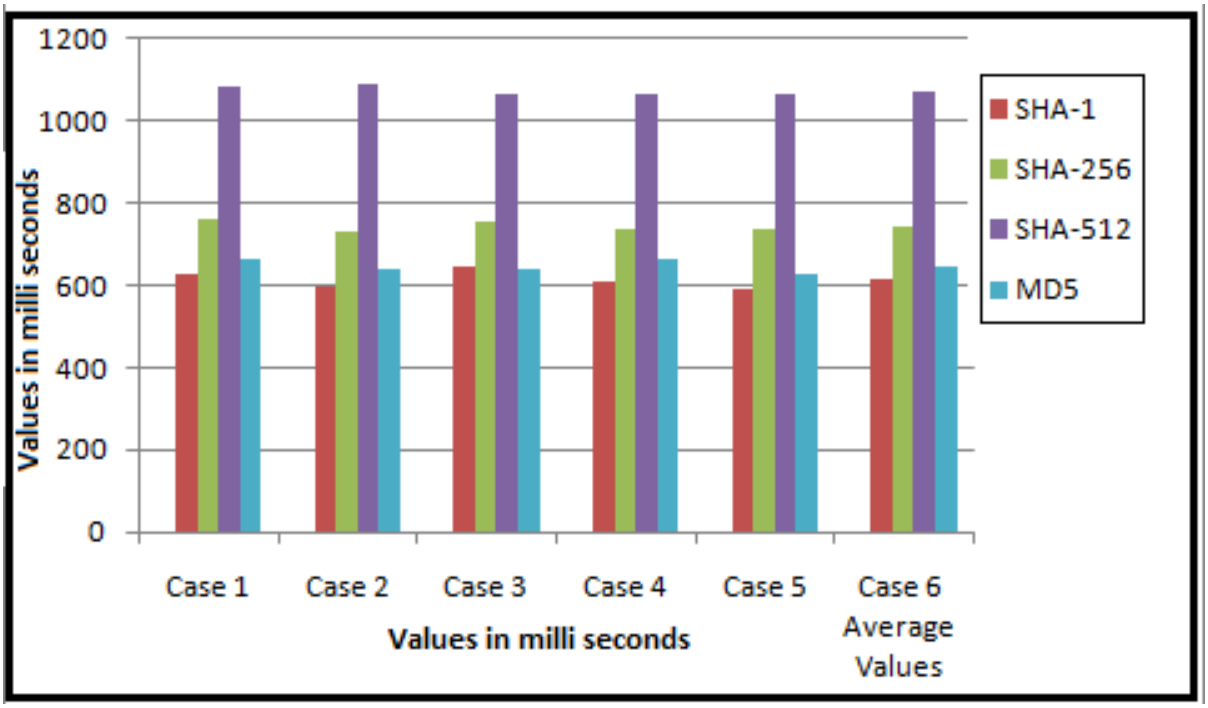

Figure 8: Encoding 36 char string

Case 2: To encode 49 characters length data with cached UUID, so observations are:

Table 2: Encoding 49 char string

ALGO	(i)	(ii)	(iii)	(iv)	(v)	Average in millisec
SHA-1	762	763	692	762	750	745.8
SHA-256	843	873	842	837	852	849.4
SHA-512	1162	1153	1162	1152	1162	1158.2
MD5	752	783	742	802	732	762.2

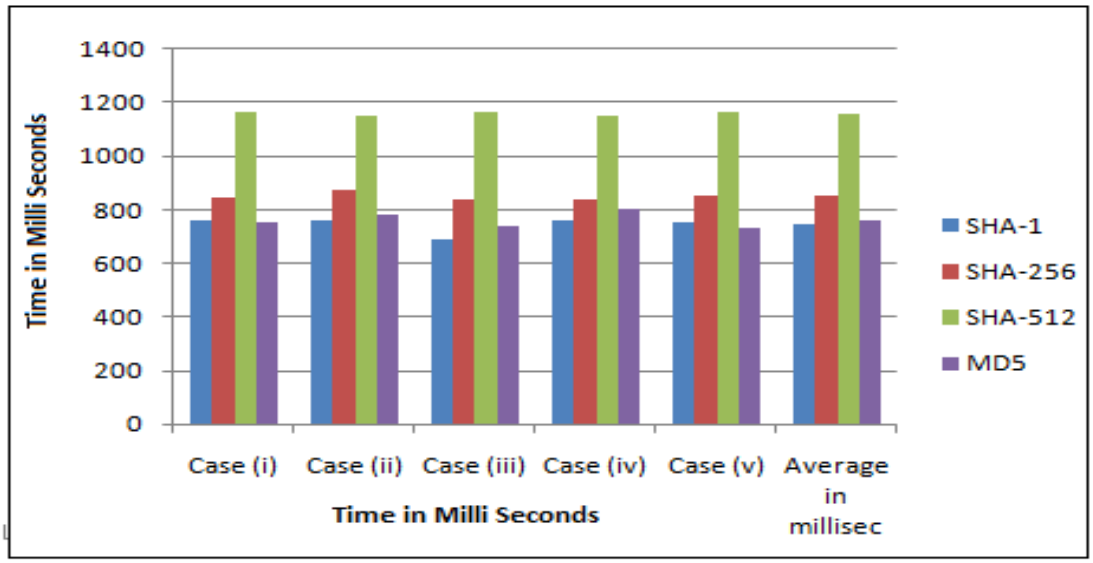

Figure 9: Graph of 49 char string

Case 3: To encode 85 characters length data with cached UUID, some observations are:

Table 3: Encoding 49 char string

ALGO	(i)	(ii)	(iii)	(iv)	(v)	Average in millisec
SHA-1	1004	1012	1022	1003	993	1006.8
SHA-256	1253	1242	1292	1253	1243	1256.6
SHA- 512	1223	1222	1233	1233	1225	1227.2
MD5	1022	1032	1033	1013	1037	1027.4

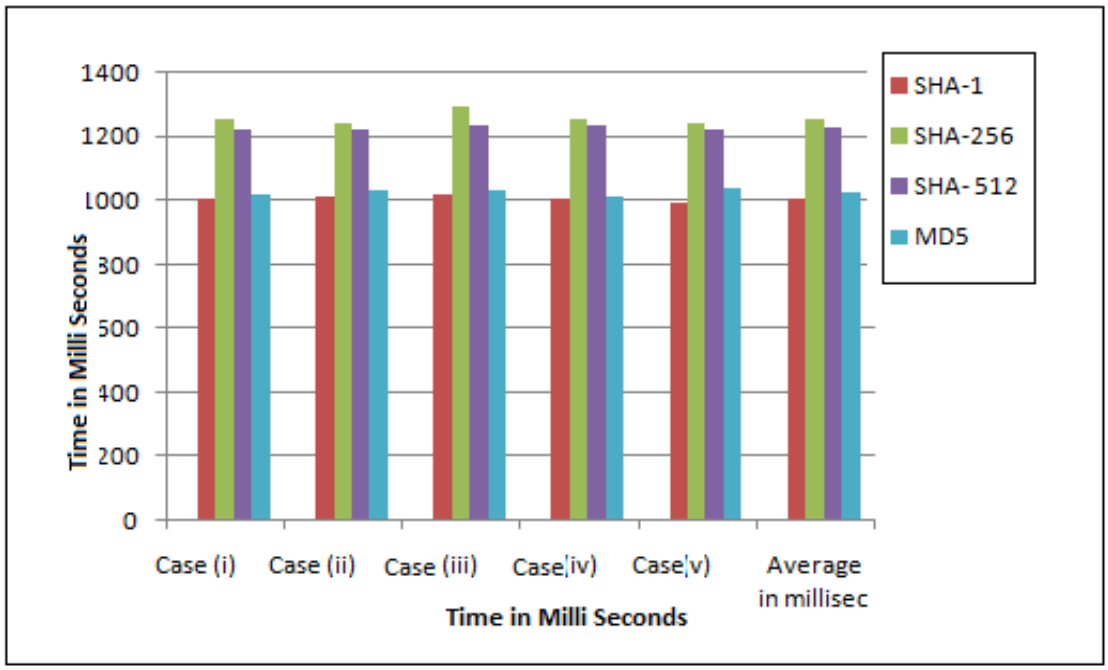

Figure 10: Graph of 85 char string

Calculating Results: On calculating results some observations were been made which are:

- While only small strings hashing, SHA-256 is observed to be faster than SHA-512 with 31%. If hashing is done on longer strings SHA-512 is faster than SHA-256 with about 2.9%.
- For short strings SHA-1 is faster than MD5 with 7.6% and for longer strings it is faster with 1.3%.
- For short strings SHA-1 is faster than SHA-256 with 15.5% and for longer strings it is faster with 23.4%.

6. CONCLUSION

After analyzing the above model results obtained were such that if hashing is done properly at both ends and with proper authentication done, then the sender can access the resource of the receivers such as if there is a remote of a car pressed then after successful authentication car doors will get unlocked otherwise not. Also while doing some research on various algorithms like SHA-256, SHA-512, SHA-1 and MD5 on the basis of time, the observations show that it is good to select SHA-256 for this algorithm in order to complete the task in minimum time without any compromising the security.

7. FUTURE SCOPE

Although, Authentication is the gateway of security, if Authentication is secure then it is hard to crack it and difficult to enter into the system. But there are more important factors such as non-repudiation, availability and access control to explore. This Model can be applied to IoT based automation such as garage doors authentication, shops doors authentication etc.

SOURCES OF FUNDING

None.

CONFLICT OF INTEREST

None.

ACKNOWLEDGMENT

None.

REFERENCES

[1] LASER: Lightweight And Secure Remote Keyless entry protocol: Vanesa Daza And Xavier Salleras(2019).
[2] On the security of Remote Keyless Entry for vehicles: Jinita Patel Manik Lal Das sukumar nandi(2018).
[3] A Protocol for Secure Remote Keyless Entry System Applicable in Vehicles using Symmetric –Key Cryptography: Tobias Glocker, Timo Mantere, Mohammad Elmusrati(2017).
[4] Lock it and Still Lose It: On the security of automotive remote keyless entry systems: Flavio D.Garcia, David Oswald, Timo Kasper, Kasper & Oswald GmbH (2016).
[5] Analysis Of Attack Against the Security Of Keyless Entry Systems for Vehicles and Suggestions for Improved Designs: Ansaf Ibrahem Alrabady and Syed Masud Mahumad(2005).
[6] A. Moradi and T. Kasper," A New Remote Keyless Entry System Resistant to Power Analysis Attacks" in ICICS, 2009 c IEEE. doi:10.1109/ICICS.2009.5397727
[7] Alrabady and S. M. Mahmud," Analysis of Attacks Against the Security of Keyless-Entry Systems for Vehicles and Suggestions for Improved Designs." IEEE Trans. Veh. Technol., vol. 54, no. 1, Jan.2005.
[8] L. Vincent and G. Chevret," Customer identification device, keyless access system for vehicle, vehicle sharing system including such a device and methods using such a device." Patent WO2008044093 A1. Apr,17, 2008.

[9] A. Bogdanov. Attacks on the KeeLoq Block Cipher and Authentication Systems. In RFIDSec 2007. http://rfidsec07.etsit.uma.es/slides/papers/paper- 22.pdf.
[10] S. Chari, J. R. Rao, and P. Rohatgi. Template Attacks. In CHES 2002, volume 2523 of LNCS, pages 13–28. Springer, 2002.
[11] N. T. Courtois, G. V. Bard, and D. Wagner. Algebraic and Slide Attacks on KeeLoq. In FSE 2008, volume 5086 of LNCS, pages 97– 115.Springer, 2008.
[12] T. Eisenbarth, T. Kasper, A. Moradi, C. Paar, M. Salmasi Zadeh, and M. T. M. Shalmani. On the Power of Power Analysis in the Real World: A Complete Break of the KeeLoq Code Hopping Scheme. In CRYPTO 2008, volume 5157 of LNCS, pages 203–220. Springer, 2008
[13] H. Zhong, B. Huang, J. Cui, Y. Xu, and L. Liu, "Conditional privacy preserving authentication using registration list in vehicular ad hoc networks," IEEE Access, vol. 6, pp. 2241–2250, 2018.
[14] E. Hamdaqa, A. Mars, W. Adi, and S. Mulhem. Clone-resistant vehicular RKE by deploying SUC. In Proceedings of International Conference on Emerging Security Technologies, pp. 221-225, 2017.
[15] S. Indesteege, N. Keller, O. Dunkelman, E. Biham, and B. Preneel.A Practical Attack on KeeLoq. In Proceeding of the Theory and Applications of Cryptographic Techniques (EUROCRYPT), LNCS 4965, Springer-Verlag, pp. 1–18, 2008.
[16] D. Rubino. How crooks can steal your car without the key. https://www.autocar.co.uk/car-news/industry/how-crooks-can- stealyourcar-without-key.15
[17] Ibrahim, O. A., Hussain, A. M., Oligeri, G., and Di Pietro,R. (2018). Key is in the air: Hacking remote keyless entry systems. In Proc. of the International Workshop on Cyber Security for Intelligent Transportation Systems (CSIT 2018).
[18] Kamkar, S. Drive It Like You Hacked It: New Attacks and Tools to Wirelessly Steal Cars. Presentation at DEFCON 23, August 2015.
[19] C. Herder, M. Yu, F. Koushanfar, and S. Devadas. Physical Unclonable Functions and Applications: A Tutorial. In Proceedings of IEEE,102(8):1126–1141, 2014.
[20] D. He, S. Zeadally, B. Xu, and X. Huang, "An efficient identity based conditional privacy-preserving authentication scheme for vehicular ad hoc networks," IEEE Transactions on Information Forensics and Security, vol. 10, no. 12, pp. 2681–2691, 2015.
[21] D. Lee," Keyless cars 'increasingly targeted by thieves using computers'." Internet: www.bbc.com/news/technology-29786320, Oct. 2014 [Apr. 2,2016].
[22] Cryptography and Network Security: Principles and Practice, by William Stallings. (3rd edition)