Authentication Aspects of Dynamic Routing Protocols: Associated Problem & Proposed Solution

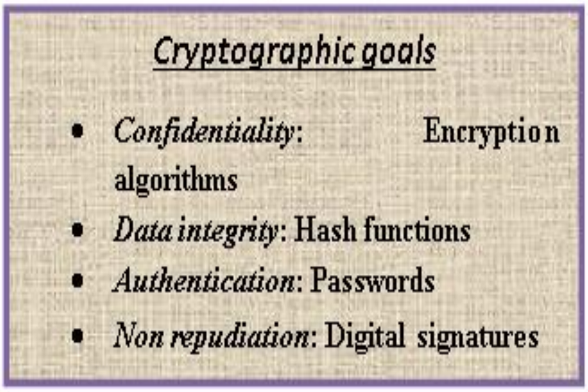
Varun Shukla, Atul Chaturvedi, Neelam Srivastava

Abstract*: Cryptography as a stream is very important for communication security. Cryptography provides many goals for communication security and authentication is one of them. Routing is an integral part of computer networks and router security is extremely important because routing provides suitable path to the traffic generated in the network. Authentication is very important for routing protocols. In this paper we discuss security flaws in routing authentication and provide a unique solution which is never presented to overcome this problem. We also discuss the security analysis of the proposed method which proves that the proposed method is robust in various aspects. The proposed method provides many advantages and the method is so simple that anybody can use it.

***Index Terms*: AES (Advance Encryption Standard), Dynamic Routing, Exterior Gateway Protocol (EGP), Hash Functions, Interior Gateway Protocol (IGP), MD 5 hash**

I. INTRODUCTION

In the fast and modern world where data communication is a necessity of life, cryptography plays a key role by providing data communication security. Cryptography is a collection of algorithms, procedures and techniques required for communication security. Cryptanalysis is opposite to cryptography because it deals with breaking the codes by various means. Cryptography and cryptanalysis are jointly knows as cryptology. Cryptography provides data security through some objectives and they are known as cryptography goals as shown in figure 1 **[1-2]**. Confidentiality is the first goal which makes sure that only authorized receiver can access the data. Many encryption algorithms are there to provide confidentiality. Data integrity is second in the list and it is responsible for the prevention of any unauthorized alteration or modification of data. Hash functions are used to validate data integrity. Authentication is the third goal and we talk about it in detail in the later section of this paper. At the basic level, authentication is a service which makes sure that communication is in between legitimate entities. Passwords, thumb impression etc are used for it. Non repudiation is the fourth goal and it makes sure that a participating entity, in a communication process, can't deny previously made commitments. Digital signatures are used for it.



Cryptographic goals

- *Confidentiality*: Encryption algorithms
- *Data integrity*: Hash functions
- *Authentication*: Passwords
- *Non repudiation*: Digital signatures

Figure 1. Showing cryptographic goals required for secure communication.

For communication process, routing is the core part. Routing can be classified as static routing and dynamic routing **[3]**. In static routing, routers are configured by network administrator. Usually static routing is preferred for small networks requiring only two or three routers. One promising application of static routing is to define an exit point when no existing routers are left. It can also be used as a backup and the CPU overheads are very low. The drawback is that the administrator can do mistakes when numbers of routers are high. On the other side, in dynamic routing (also known as adaptive routing), as the name suggests, a router can transfer data to a route based on present conditions. Many protocols are there in this category and we will discuss them in a later section of this paper. A dynamically configured network adapts changes very quickly because each router declares their presence to the other routers present on the network. The rest of this paper organized as follows: In section 2, we talk about authentication and dynamic routing protocols in brief. In section 3, we discuss security flaws with some existing solutions. In section 4, we provide proposed solution. Section 5 is all about the security analysis of the proposed method. Section 6 takes care of the advantages of the proposed method. Paper ends with conclusion and future scope which is in section 7.

II. AUTHENTICATION & DYNAMIC ROUTING PROTOCOLS

In a peer to peer or in group communication, it is essential that participating entities must recognize each other via some specific procedure. Broadly, authentication can be classified in entity authentication and data origin authentication **[1]**.

Revised Manuscript Received on July 06, 2019.

Varun Shukla, Department of Electronics & Communication, PSIT, Kanpur, India.
Atul Chaturvedi, Department of Mathematics, PSIT, Kanpur, India.
Neelam Srivastava, Department of Electronics & Communication, REC, Kannauj, India.

DOI: 10.35940/ijrte.B1503.078219

Entity authentication makes sure to the receiver that the sender is legitimate. Data origin authentication makes sure that received message has been generated by legitimate sender or creator. Authentication can further be divided into hardware level and calculation based. Hardware level authentication requires devices and physical interaction. Thumb impression, retina & face detection and RFID based authentication etc all are the examples in this category **[4-7]**. Calculation based authentication involves broad range of algorithms, procedures, password based mechanisms and signature schemes etc **[8-10]**. The advantage of using calculation based authentication is that it does not require any specific hardware module and physical interaction is not required in this case. It can be extended to large number of users and modifications of protocols and algorithms are possible which is required to remain up to date with the pace of intruders. Now we will discuss all the existing dynamic routing protocols in brief as shown in figure 2 **[11-13]** so that readers of this paper feel familiar with them.

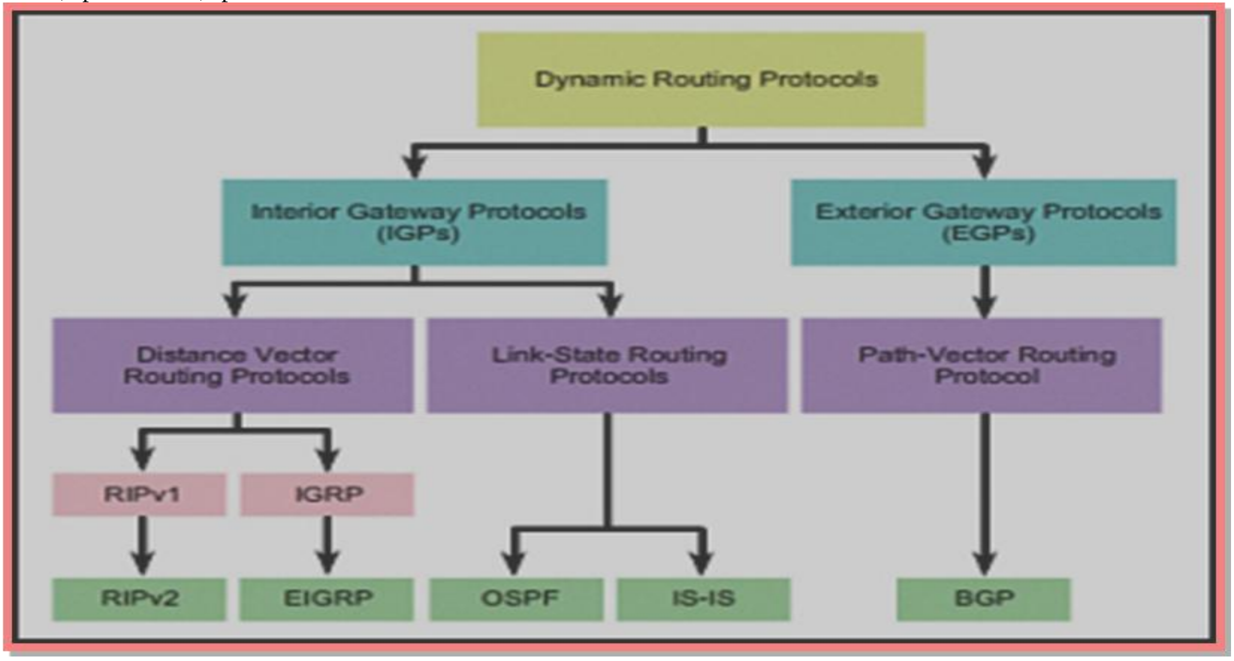

Dynamic Routing Protocols
Interior Gateway Protocols (IGPs)
Exterior Gateway Protocols (EGPs)
Distance Vector Routing Protocols
Link-State Routing Protocols
Path-Vector Routing Protocol
RIPv1
IGRP
RIPv2
EIGRP
OSPF
IS-IS
BGP

Figure 2. Showing classification of dynamic routing protocols.

RIP: Routing Information Protocol (RIP) is the oldest distance vector routing protocol utilizes hop count for routing metric (max 15). RIPv1 was the older version and does not support any authentication and it is updated by RIPv2 and RIPng which supports IPv6. RIPv2 supports two classes of authentication, one is plain text authentication and other one is MD5 authentication. Plain text authentication is by default but it should not be used because it can create various security issues. MD5 authentication is optional.

EIGRP: Enhanced Interior Gateway Routing Protocol (EIGRP) had replaced IGRP (Interior Gateway Routing Protocol) in 1993. EIGRP is an advanced distance vector routing protocol. It's a dynamic routing protocol and makes sure that routers systematically route information with each other. It provides MD5 authentication between peer routers. In default case, there is no authentication. For authentication, EIGRP provides two classes of authentication. First one is simple password or plain text authentication and other one id MD5 authentication.

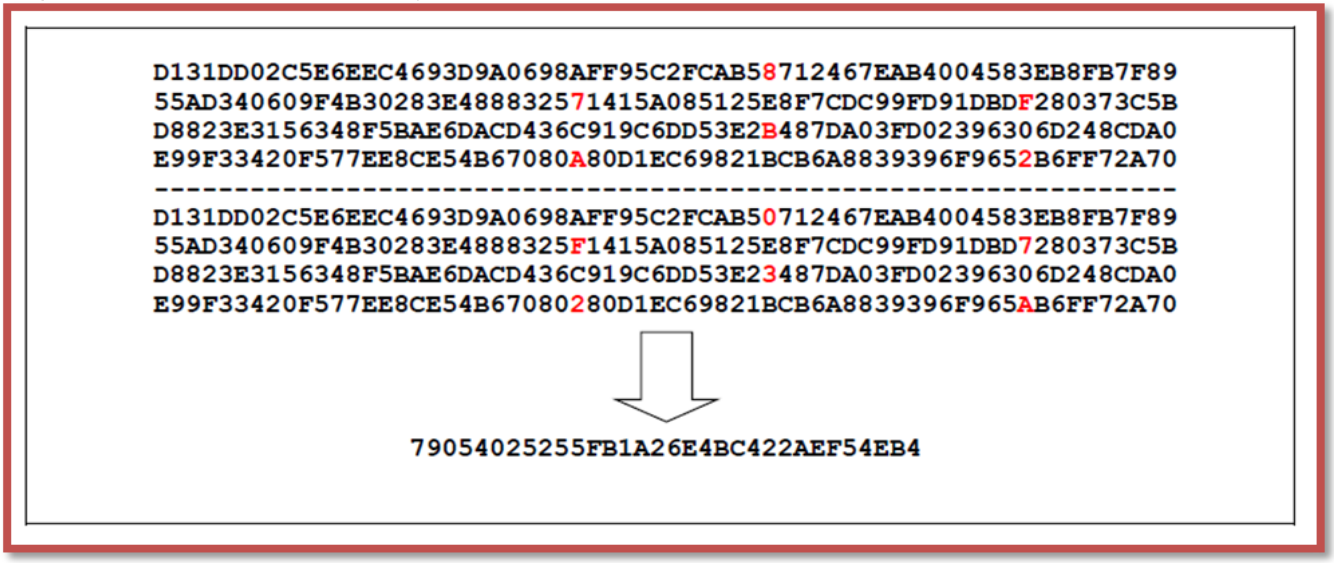
OSPF: Open Shortest Path First (OSPF) uses LSR (link state routing) for IP networks. It's an interior gateway protocol and uses Dijkstra algorithm in order to select optimum path available. OSPF (and it versions) uses three categories of authentication i.e. type 0, type 1 and type 2. Type 0 is the default method and provides no authentication. Type 1 provides authentication in a very insecure fashion. In this case, password goes in clear text or plain text over the network. Type 2 provides MD5 authentication. All peer routers of one area should have MD5 method enabled.

IS-IS: Intermediate System to Intermediate System (IS-IS) is also an interior gateway protocol uses LSR with Dijkstra algorithm for the calculation of optimum path. It is used for large networks and it uses HMAC (Hash-Based Message Authentication Code)-MD5 authentication. The difference between OSPF and IS-IS is that OSPF is designed for IP while IS-IS doesn't incorporate IP for carrying routing information messages. IS-IS is a neutral protocol as long as network type is concern. That's why IS-IS naturally supports IPv6 while OSPF needs to be rewritten as version 3.

BGP: In contrast with OSPF and IS-IS, Border Gateway Protocol (BGP) is a path vector exterior gateway protocol. It takes routing decisions based on paths or some rules demonstrated by the administrator. It utilizes MD5 based authentication procedure so that only authorized peers can be added as neighbors. The main application of BGP involves connection of one AS (Autonomous Systems) with another. It is a protocol used between internet service providers. An AS can be seen as a network belongs to one service provider. Flexibility is the key feature of BGP because it provides interconnection of different AS using an arbitrary topology. Since it connects large networks, the importance of authentication is very important here.

III. SECURITY FLAWS WITH EXISTING SOLUTIONS

MD5 has been officially developed by R.Rivest in 1992. It produces 128 bits digest and the input block size is of 512 bits. It follows 4 rounds with Merkle-Damgård construction **[14]**. It is very useful in various applications like checking the integrity of downloaded file, password authentication, routing protocols and still many softwares are using MD5 algorithm for various reasons **[15-17]**. In 2005, Xiaoyun Wang and Hongbo Yu **[18]** proposed a differential attack but it does not used XOR as a difference operation. They used integer subtraction for their measurement which is called as modular differential. The same concept could also be applicable to other hash functions like RIPEMD and HAVAL. In 2010, Tao Xie and Dengguo Feng **[19]** proposed the single block collision for MD5 but they did not publish the details because of security reasons and they gave a challenge to the cryptology fraternity to find another attack. In 2012, Marc Stevens provided single block collision attack on MD5 **[20]**. It was based on low number of bit conditions. He claimed that the challenge proposed by Wang and Yu has been broken now. In 2016, G.C.Kessler discussed that MD5 is often used for integrity verification in the forensic imaging pattern **[21]**. He has shown that two different disks having different content occupy same byte positions on the disk and same size could have the same hash value. The result was very important because earlier people believed that MD5 collision has no problem with associated applications. In 2017, Z.E.Rasjid et al **[22]** reviewed that most digital extraction tools use MD5 hash algorithm to verify the integrity of digital evidence and the collision in algorithm can used in such a way so that denial of usage of evidence is possible in the court and a criminal may be benefitted. Apart from that, researchers from INRIA institute of France, which deals in research of computer science and applied mathematics, suggested that it is dangerous to use MD5 **[23]**. They have shown that MITM-type intruders can impersonate customers communicating with servers those still supports MD5 digest for handshaking transcripts. Now we will show that how block structure of MD5 can be exploited to find a collision. As we have mentioned earlier that MD5 works on Merkle-Damgård iteration. Any given input is offered padding in order to make its length in the multiple of 64 bytes. Now it is divided into blocks having block length 64 bytes and denoted by $x_0, x_1, x_2, \dots, x_{n-1}$. We need to calculate a sequence of 16 byte states $b_0, b_1, \dots, b_n$ where the applicable rule is $b_{i+1} = f(b_i, x_i)$ where f is a complicated function. The initial state b_0 is fixed and it is also known as the initialization vector. The final state b_n is the computed hash. It is possible, for a initialization vector, to search two pairs of blocks x , x' and y , y' such that $f(f(b,x),x') = f(f(b,y),y')$ where b is any initialization vector. By this way, it is feasible to find pairs of files of arbitrary length, for 128 bytes, they are almost identical (except the difference somewhere in one place) and having same MD5 hash. Suppose we have $x_0, x_1, \dots, x_{i-1}, x_i, x_{i+1}, x_{i+2}, \dots, x_n$ and $x_0, x_1, \dots, x_{i-1}, y_i, y_{i+1}, x_{i+2}, \dots, x_n$. So we say that $x_0, x_1, \dots, x_{i-1}$ can be picked arbitrarily. Suppose the internal state of the hash is b_i after the processing of these blocks, so we can have $b_{i+2} = f(f(b_i, x_i), x_{i+1}) = f(f(b_i, y_i), y_{i+1})$ and it will make sure that internal state b_{i+2} will be identical for the two different files. Similarly, as above, the rest of the blocks $x_{i+2}, \dots, x_n$ can be selected arbitrarily. By writing simple program we can compare two blocks having same MD5 hash. We show one example of two different block of 256 hex characters (1024 bits or 128 bytes) having the same hash.



```
D131DD02C5E6EEC4693D9A0698AFF95C2FCAB58712467EAB4004583EB8FB7F89
55AD340609F4B30283E488832571415A085125E8F7CDC99FD91DBDF280373C5B
D8823E3156348F5BAE6DACD436C919C6DD53E2B487DA03FD02396306D248CDA0
E99F33420F577EE8CE54B67080A80D1EC69821BCB6A8839396F9652B6FF72A70
----------------------------------------------------------------
D131DD02C5E6EEC4693D9A0698AFF95C2FCAB50712467EAB4004583EB8FB7F89
55AD340609F4B30283E4888325F1415A085125E8F7CDC99FD91DBD7280373C5B
D8823E3156348F5BAE6DACD436C919C6DD53E23487DA03FD02396306D248CDA0
E99F33420F577EE8CE54B67080280D1EC69821BCB6A8839396F965AB6FF72A70

79054025255FB1A26E4BC422AEF54EB4
```

Figure 3. Showing two different blocks having the same hash.

The first four lines of the above figure 3 represent one block and last four lines denote another block. The first and third line of each block differs only in one position. Similarly the second and fourth line of each block differs in two positions shown by red color. Both block produces same MD5 hash. So now it is clear that MD5 hash authentication is insecure and it can put the security of entire network into danger. We discuss some of the existing solutions now.

3.1 Salting: A salt can be understood as a random data that is used to enhance security **[24]**. It can be cascaded with the input to calculate hash. Suppose we want to enhance the security of passwords and we use username as a salt to the corresponding password. So $username + password \rightarrow hash\ digest$. Naturally it provides some security against password guessing attacks like dictionary attacks. It has another benefit for authentication. Suppose two different users select the same password then also their hash string will be different because of different usernames.

3.2 Problems of salting: The first problem with salting is storing problem. It is always difficult to store many salts **[25]**. Any symmetry, as mentioned above that one can use username as a salt, can be predicted which degrades the security. Generating random salts is similar to OTP (One Time Pads) which is an expensive procedure in cryptography **[26]**. One has to generate thousands of random numbers which is a load on computational overheads.

3.3 Migrate to other algorithms: One may think that it is very easy and a good option to migrate to other algorithms like SHA-1 or SHA-2 (SHA-2 is a family of algorithms having different hash digest size as SHA-224/256/384/512, among all of them SHA-256 is most popular) **[27].**

3.4 Problems of migrating to other algorithms: There are many problems and it is never an optimum solution to migrate to other algorithms. SHA-1 provides 160 bit or 20 byte hash value (or 40 hex digits). SHA-1 is not secure against well equipped intruders. Researchers already suggested replacing SHA-1. In 2017, CWI and Google together worked on a project and announced that they have found a successful collision attack against SHA-1 and provided two different PDF files having the same SHA-1 digest **[28]**. Talking about SHA-2 family, it is not yet adopted in many systems. So replacement with SHA-2 is not a feasible option. Suppose one entity is providing authentication in MD5 and server provides authentication in SHA-2, then it will result as authentication mismatch. So for replacement, all the routers or entities must follow the same algorithm which is a very difficult task. With the ever increasing computational power, it is not too much to say that suppose some algorithm say SHA-256 in all the entities, then also intruders would perform attack within 2-3 years down the line **[29]**. It will waste lots of resources as well as we need to change the algorithm again.

IV. PROPOSED SOLUTION

Before going to the proposed solution, it is essential that in the introduction part we discuss some perquisite in a concise manner to understand this paper. Our basic ingredients are MD5 hash, steganography and AES so we discuss about them in very brief. The MD5 algorithm, which is an improvement of MD4 was developed by Ronald Rivest in RFC 1321 **[30]**. MD5 satisfies all the desirable hash algorithm properties like collision resistance, pre image resistance etc. MD5 takes arbitrary length input and produces a fixed length i.e. 128 bit output known as message digest. MD5 is capable of processing data as 512 bit blocks. These blocks are further divided into 16 words where each word consists of 32 bits. Steganography is all about methods and procedures of hiding a message file inside another file called as carrier file. The resultant is known as steganogram. Based on the type of carrier file used, steganography can be image steganography or video steganography etc **[31]**. Here it is important to mention that we are considering steganography as a supporting tool of cryptography not a substitute of it because cryptography provides secrecy, authentication, data integrity and non repudiation as security parameters. In steganography one can use LSB based algorithms or RGB based algorithms **[32-33]**. AES is a well known symmetric encryption algorithm and it is much faster than triple DES. AES is a block cipher algorithm which has 128 bit data (block of 16 bytes) and uses 128/192/256 bit key. AES has iterative structure which is based on substitution-permutation network as shown in figure 4. AES have variable number of rounds. If the key size is 128 bits, 10 rounds are there. For 192 bits and 256 bit keys, numbers of rounds are 12 and 14 respectively.

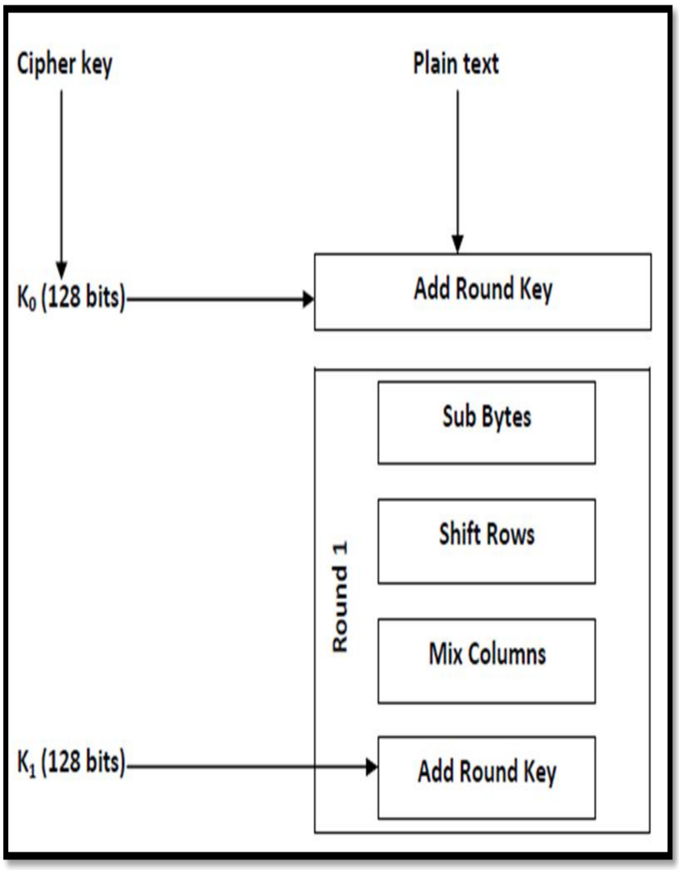
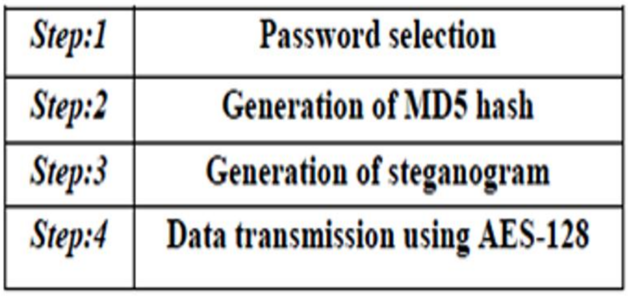


Figure 4. Representing steps involved in a round of AES

Our proposed solution is a simple four step procedure. We illustrate the procedure in one glimpse through figure 5 given below and after that we will explain all the steps individually.



Step:1	Password selection
Step:2	Generation of MD5 hash
Step:3	Generation of steganogram
Step:4	Data transmission using AES-128

Figure 5. Showing involved steps in the proposed method

Step 1: To generate the key we essentially need a password. When we create the symmetric key through randomly generated password, it will always enhance the security level of the cryptosystem. Here user can generate his or her own password randomly but in order to be more systematic we use a simple program which generates passwords on random basis. We use java.util.class package. It creates a password which is a random combination of small letters, capital letters, special symbols and numbers. The run time of the program is very small and we present some of the readings by table 1 below

S.N.	Run time (second)	Memory required (MB)	Created password
1	0.072	54.2	Ac9#@dbq
2	0.073	54.3	GRS$96*77
3	0.075	54.6	RPQnst@$91
4	0.082	54.9	FdymA%@78bj
5	0.086	55.0	pm^4@@7112%R
6	0.088	55.1	ZMlp@*r7r2q@%

Table 1: Showing generated passwords along with their run time

Step 2: In second step we generate the corresponding MD5 hash from random created passwords. The password length can be variable but MD5 message digest produces fixed output of 128 bits. We show message digest of passwords shown in table 2 below.

S.N.	Password	MD5 hash
1	Ac9#@dbq	8F 68 02 D5 EC 2A 9B 34 AC 8B EB A1 81 23 C2 DD
2	GRS$96*77	F2 48 B4 EA EF D7 BA 41 D8 E4 8B 18 94 BE D3 63
3	RPQnst@$91	DC DD F1 3C 61 87 E9 1B FD 48 FD 0D 5C 81 2E F6
4	FdymA%@78bj	46 77 7C 01 0C A4 A8 61 B2 40 ED 54 CE 8F 01 23
5	pm^4@@7112%R	70 30 82 32 7C 01 AD 82 11 A8 99 1F 58 17 8B 00
6	ZMlp@*r7r2q@%	3F 32 D6 1A 6F 5F CC 21 92 B9 6A 63 80 E5 59 B5

Table 2. Showing variable length passwords and their corresponding digests

Step 3: In these steps we hide the MD5 symmetric key inside the carrier file and generate the steganogram. We also provide password protection to steganogram. We talk about these steps in security analysis section in detail. In the below figure 6, we show the carrier file (left side) and the corresponding steganogram (right side) and we can see that there is no observable change.

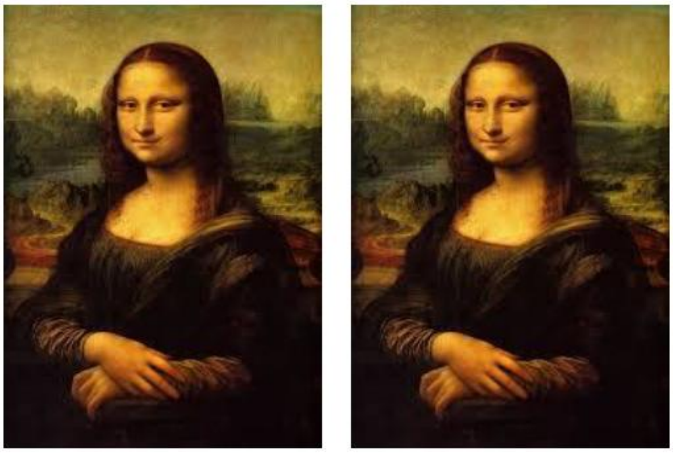
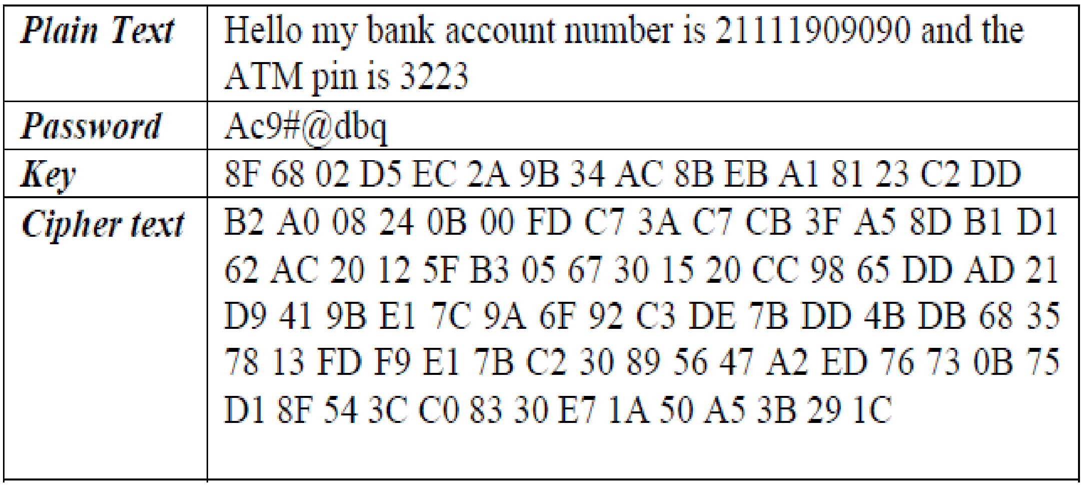


Figure 6. Showing carrier file (left side) and the steganogram (right side)

Step 4: In this step, we encrypt the message data using AES symmetric key and transmit it to the receiver. We show the corresponding encrypted message of the plain text in the below figure 7.



Plain Text	Hello my bank account number is 21111909090 and the ATM pin is 3223
Password	Ac9#@dbq
Key	8F 68 02 D5 EC 2A 9B 34 AC 8B EB A1 81 23 C2 DD
Cipher text	B2 A0 08 24 0B 00 FD C7 3A C7 CB 3F A5 8D B1 D1 62 AC 20 12 5F B3 05 67 30 15 20 CC 98 65 DD AD 21 D9 41 9B E1 7C 9A 6F 92 C3 DE 7B DD 4B DB 68 35 78 13 FD F9 E1 7B C2 30 89 56 47 A2 ED 76 73 0B 75 D1 8F 54 3C C0 83 30 E7 1A 50 A5 3B 29 1C

Figure 7. Showing plaintext, password, key and cipher text in a protocol run

V. SECURITY ANALYSIS

1. Analysis of steganogram: Since we are using MD5 hash as a key which is always of fixed size i.e. 128 bits only. This small size will have almost no effect on the steganogram which looks like a carrier file. We analyze this using histogram in the figure below **[34]**.

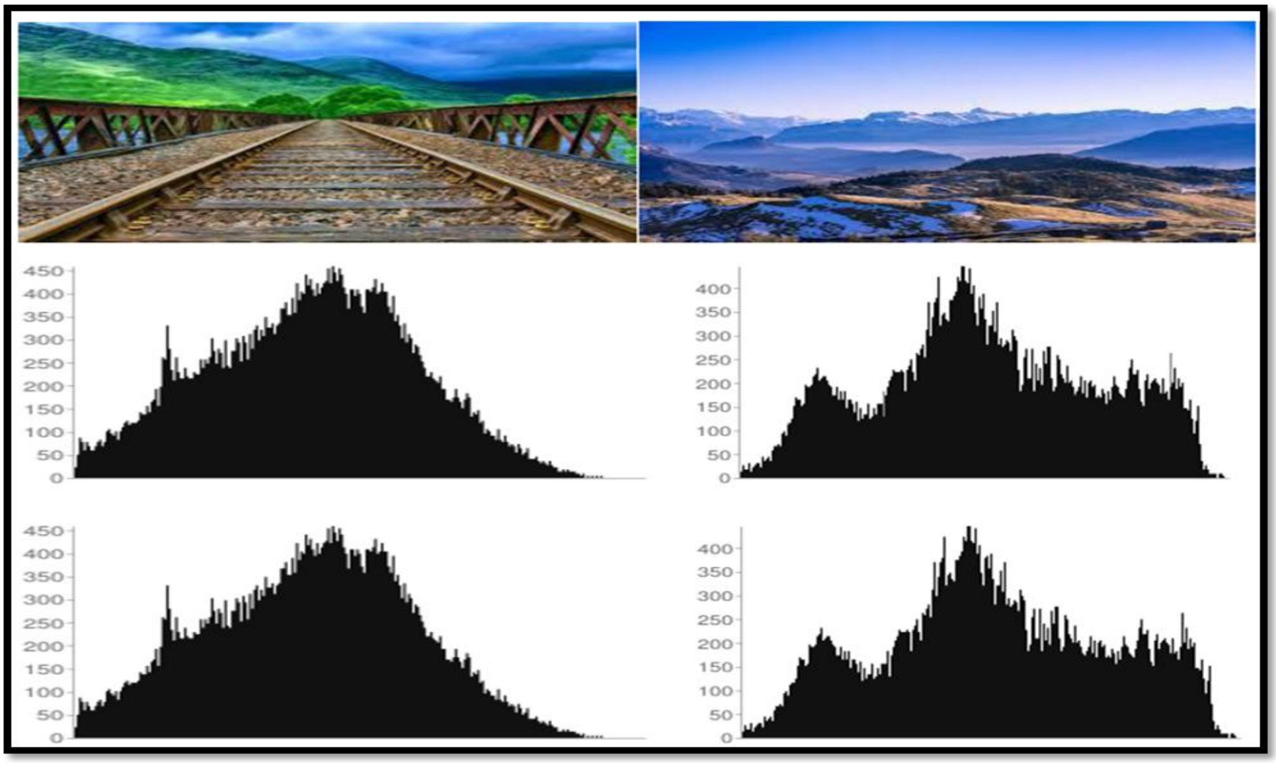
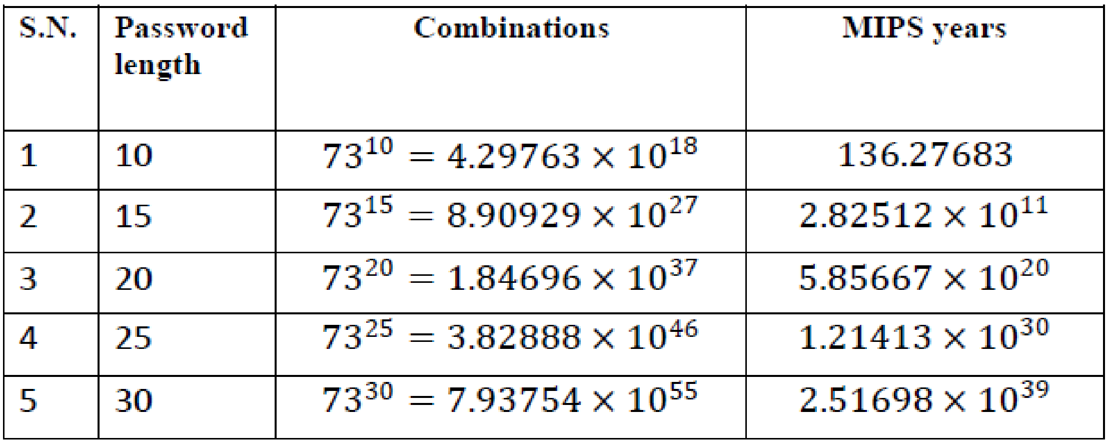


Figure 8. Histogram analysis of the carrier file and the steganogram

In this above figure 8 we have used two different carrier files (in the first row) and their respective histograms (in the second row). We have also shown the histograms of corresponding steganogram (in the third row) generated from these carrier files and one can observe that there is no visible change.

2. Password protection: We generate our key from random passwords. Suppose we have 30 digit password (because it is very easy as we have to change only one line in the program), then the total possible combinations are 73^{30}. If a intruder has computational strength of 1000 MIPS (Million Instructions Per Second) then also it will take the time which is computationally infeasible as shown in table 3 given below.

So this password based key serve as an OTP (OTP based security is assumed hardest in cryptography **[35]**) as well as there is no chance to predict the output of MD5. In case of a new session or in time stamping based method, the key changes and the intruder has to revise the entire procedure again which is computationally very expensive.



S.N.	Password length	Combinations	MIPS years
1	10	$73^{10} = 4.29763 \times 10^{18}$	136.27683
2	15	$73^{15} = 8.90929 \times 10^{27}$	2.82512×10^{11}
3	20	$73^{20} = 1.84696 \times 10^{37}$	5.85667×10^{20}
4	25	$73^{25} = 3.82888 \times 10^{46}$	1.21413×10^{30}
5	30	$73^{30} = 7.93754 \times 10^{55}$	2.51698×10^{39}

Table 3. Showing different password lengths and corresponding MIPS years

3. AES Security: Our method enjoys security of AES also. AES is a secure encryption scheme and no such attacks are presented till now in computationally feasible time **[36]**.

4. High randomness: Here it is important to mention avalanche property of hash functions **[37]**. The property says that if we change only a bit in the input of hash, output changes dramatically. Here in our case we are changing the entire password in every run so it is not possible to predict the hash output.

5. Resistance against DoS attack: When we use regular cryptographic methods, an intruder can intentionally provide delay or DoS (Denial of Service) attack in order to degrade the QoS (Quality of Service) **[38]**. In our case, it is not the problem because the encrypted message and key goes separate and one never knows that there is a hidden key there.

VI. ADVANTAGES

1. New key for every session: The salient feature of proposed method is that one can use new session key in every run. It makes any kind of prediction very difficult because an intruder has to perform cryptanalysis again.

2. Time stamping of a key is possible: Another method to provide uniqueness of key is to employ time stamping in key. A key expires after a certain predefined time period even if the session is in running mode. It makes cryptanalysis very difficult because intruder has to perform attack within the lifetime of the key.

3. Brute force attack is not possible: This is a very obvious point. From the above table it is clear that to try all possible combinations is not possible in computationally infeasible time. The security further increases when the key has specific lifetime or valid for a particular session only.

4. A unique solution keeping MD5 algorithm intact: As we have claimed in part 1 that we will not change the algorithm because it is an expensive and difficult task. So we have provided a new method keeping the algorithm intact.

5. Cascaded encryption is also possible: Our method is flexible enough so that one can apply cascaded or chain encryption in order to enhance the security. Double AES encryption will enhance the security level.

6 Authentication and encryption both at a time: The proposed method provides authentication and encryption in one run. If any alteration is done with the image, there is a change in password and any change in password will produce a different key and authentication goes fail. One can decrypt the data only in case of successful authentication. So in a nutshell, in a very first run, you can send a message which is encrypted and provides authentication too.

VII. CONCLUSION & FUTURE SCOPE

So from the above discussion it is clear that we have given a new solution for the vulnerability of dynamic routing protocols. The method is robust enough to resist various security attacks. The protocol provides many advantages and at the same time, it is simple enough so that anybody can use that. The future scope of the proposed method is very rich as one can apply other algorithms like IDEA, Blowfish etc. The proposed method can be customized in various aspects by making password length variable, applying time stamping etc. The method can also be useful in medical information security, defense applications or in various peer to peer applications.

The method can be extended to group communication as well as one can use five different keys (generated from five different passwords) in order to transmit same message to five different persons using different networks.

REFERENCES

1. A.J.Menezes, P.C.V.Oorschot, S.A.Vanstone, Handbook of applied cryptography, fifth edition, CRC press Inc., USA, ISBN: 9780849385230, 2001.
2. W.Stallings, Cryptography and network security, principles and practices, seventh edition, Prentice Hall, 2005, ISBN-13:978-0134444284, ISBN-10:0134444280.
3. D-I.Trunog, B.Jaumard, Recent progress in dynamic routing for shared protection in multidomain networks, IEEE communications magazine, volume 46, issue 6, June 2008, pp.112 - 119, DOI: 10.1109/MCOM.2008.4539474

4. A.K.Jain, A.Ross, S.Pankanti, Biometrics: a tool for information security, IEEE transactions on information forensics and security , volume 1, issue 2, June 2006, pp.125-143, DOI: 10.1109/TIFS.2006.873653
5. S.M.Lajevardi, A.Arakala, S.A.Davis, K.J.Horadam, Retina verification system based on biometric graph matching, IEEE transactions on image processing, volume 22, issue 9, September 2013, pp.3625-3635, DOI: 10.1109/TIP.2013.2266257
6. S.Arya, N.Pratap, K.Bhatia, Future of face recognition: A review, Procedia computer science, volume 58, 2015, 578-585, DOI: https://doi.org/10.1016/j.procs.2015.08.076
7. Y.Yinhui, Z.Lei, Research on a provable security RFID authentication protocol based on hash function, The journal of china universities of posts and telecommunications, volume 23, issue 2, April 2016, pp.31-37, DOI: https://doi.org/10.1016/S1005-8885(16)60018-3
8. F. A. Alsulaiman , A. El Saddik, Three-dimensional password for more secure authentication, IEEE transactions on instrumentation and measurement, volume 57, issue 9, 2008 ,pp. 1929 -1938, DOI: 10.1109/TIM.2008.919905

N.Datta, Zero knowledge password authentication protocol, New paradigms in internet computing, (Part of the Advances in Intelligent Systems and Computing book series (AISC, volume 203)), pp.1-79, DOI https://doi.org/10.1007/978-3-642-35461-8_7 10

9. J.Moon, Y.Lee, J.Kim, D.Won, Improving an anonymous and provably secure authentication protocol for a mobile user, Security and communication networks, volume 2017, article ID 1378128, pp.1-13, DOI: https://doi.org/10.1155/2017/1378128
10. I.Fitigau, G.Toderean, Network performance evaluation for RIP, OSPF and EIGRP routing protocols, Proceedings of the international conference on electronics, computers and artificial intelligence - ECAI, 2013, pp.1-4, DOI: 10.1109/ECAI.2013.6636217
11. G. Huston , M. Rossi, G. Armitage, Securing BGP -a literature survey, IEEE communications surveys & tutorials , volume 13, issue 2, 2011, pp.199-222, DOI**:** 10.1109/SURV.2011.041010.00041
12. R.Perlman, A comparison between two routing protocols: OSPF and IS-IS, IEEE network, volume 5, issue 5, 1991, pp.18-24, DOI: 10.1109/65.121955
13. R.Rivest, The MD5 message-digest algorithm, Request for comments: 1321, 1992, DOI: doi>10.17487/RFC1321
14. K.Shahbazi, M.Eshghi, R.F.Mirzaee, Design and implementation of an ASIP-based cryptography processor for AES, IDEA, and MD5, Engineering science and technology, an international journal, volume 20, issue 4, 2017, pp.1308-1317, DOI: https://doi.org/10.1016/j.jestch.2017.07.002
15. K. Bok, Y. Lee, J. Park and Jaesoo Yoo , An energy-efficient secure scheme in wireless sensor networks, Journal of sensors, volume 2016, Article ID 1321079, pp.1-11, DOI: http://dx.doi.org/10.1155/2016/1321079
16. M.Harran, W.Farrelly,K.Curran, A method for verifying integrity & authenticating digital media, Applied computing and informatics, volume 14, issue 2, 2018, pp.145-158, DOI: https://doi.org/10.1016/j.aci.2017.05.006
17. X.Wang, H.Yu, How to break MD5 and other hash functions, EUROCRYPT'05- Proceedings of the 24th annual international conference on theory and applications of cryptographic techniques, pp.19-35 , 2005, DOI: doi>10.1007/11426639_2
18. T.Xie, D.Feng, Construct MD5 collisions using just a single block of message, Cryptology ePrint archive, 2010, available at https://eprint.iacr.org/2010/643.pdf accessed at 16 March 2019
19. M.Stevens, Single-block collision attack on MD5, Cryptology ePrint archive, 2012, available at https://eprint.iacr.org/2012/040.pdf accessed at 16 March 2019
21. G.C.Kessler, The impact of MD5 file hash collisions on digital forensic imaging, Journal of digital forensics, security and law, volume 11, number 4 , article 9, DOI: https://doi.org/10.15394/jdfsl.2016.1431 22.
21. Z.E.Rasjid, B.Soewito, G. Witjaksono, E. Abdurachman, A review of collisions in cryptographic hash function used in digital forensic tools, Procedia computer science, volume 116, 2017, pp.381-392, DOI: https://doi.org/10.1016/j.procs.2017.10.072
22. Ongoing MD5 support endangers cryptographic protocols, available at https://www.computerworld.com/article/3020066/security/ongoing-md5-support-endangers-cryptographic-protocols.html accessed at 12 March 2019
23. S. Contini, Method to protect passwords in databases for web applications, Cryptology ePrint archive, 2015, available at https://eprint.iacr.org/2015/387.pdf accessed at 14 March 2019
24. W. Luo, Y. Hu, H. Jiang, J. Wang, Authentication by encrypted negative password, IEEE Transactions on information forensics and security (Early Access), June 2018, DOI: 10.1109/TIFS.2018.2844854
25. F.Busching, L.Wolf, The rebirth of one-time pads—secure data transmission from BAN to sink, IEEE internet of things journal , volume 2, issue 1, February 2015, DOI: 10.1109/JIOT.2014.2378783
26. B. Preneel, The first 30 years of cryptographic hash functions and the NIST SHA-3 competition, CT-RSA 2010: topics in cryptology - CT-RSA 2010 , 2010, pp.1-14, DOI: https://doi.org/10.1007/978-3-642-11925-5_1

M. Stevens , E. Bursztein , P. Karpman , A. Albertini , Y. Markov, The first collision for full SHA-1, available at https://eprint.iacr.org/2017/190.pdf accessed at 14 March 2019 29.

28. M. Stevens , E. Bursztein , P. Karpman , A. Albertini , Y. Markov, The first collision for full SHA-1, available at https://eprint.iacr.org/2017/190.pdf accessed at 14 March 2019
29. R.Rivest, The MD5 message-digest algorithm, network working group, Request for comments: 1321, available at https://www.ietf.org/rfc/rfc1321.txt
30. M.Douglas, K.Bailey, M.Leeney, K.Curran, An overview of steganography techniques applied to the protection of biometric data, Multimedia tools and applications, volume 77, issue 13, July 2018, pp.17333–17373, DOI: https://doi.org/10.1007/s11042-017-5308-3
31. P.Li, A.Lu, LSB-based steganography using reflected gray code for color quantum images, International journal of theoretical physics, volume 57, issue 5, May 2018, pp.1516–1548, DOI: https://doi.org/10.1007/s10773-018-3678-6
32. M.Jain, A.Kumar, RGB channel based decision tree grey-alpha medical image steganography with RSA cryptosystem, International journal of machine learning and cybernetics, volume 8, issue 5, October 2017, pp.1695–1705, DOI: https://doi.org/10.1007/s13042-016-0542-y
33. G. Swain, High capacity image steganography using modified LSB substitution and PVD against pixel difference histogram analysis, Hindawi security and communication networks, volume 2018, article ID 1505896, pp.1-14, DOI: https://doi.org/10.1155/2018/1505896
34. P.Laka, W.Mazurczyk, User perspective and security of a new mobile authentication method, Telecommunication systems, volume 69, issue 3, pp.365–379, November 2018, DOI: https://doi.org/10.1007/s11235-018-0437-1
35. A.A.Thinn, M.M.S.Thwin, Modification of AES algorithm by using second key and modified sub bytes operation for text encryption, Computational science and technology, lecture notes in electrical engineering, volume 481, Springer, Singapore, 2019, pp.435-444, DOI: https://doi.org/10.1007/978-981-13-2622-6_42
36. Y.M.Motara, B.Irwin, SHA-1 and the strict avalanche criterion, 2016 information security for south africa (ISSA), August 2016, pp.35-40, DOI**:** 10.1109/ISSA.2016.7802926
37. S.Fowler, S.Zeadally, N.Chilamkurti, Impact of denial of service solutions on network quality of service, Security and communication networks, volume 4, issue 10, pp.1089-1225, October 2011, DOI: https://doi.org/10.1002/sec.219