A Practical One Way Hash Algorithm based on Matrix Multiplication

Mohammed Abu Taha
College of Administrative Sciences and Informatics
Palestine Polytechnic University
Hebron, Palestine

Mousa Farajallah
College of Engineering and Technology
Palestine Polytechnic University
Hebron, Palestine

Radwan Tahboub
College of Engineering and Technology
Palestine Polytechnic University
Hebron, Palestine

ABSTRACT
It is well known that Hash algorithm works in one way, and it cannot be reversed. We can build a new algorithm by using Hill cipher technique .Since its invention in 1929, Hill cipher algorithm which is one of the most famous symmetric cryptosystems .Hill cipher requires the inverse of the key matrix for decryption. This inverse not always exists, so we can use non-invertible matrices to propose a model for our new hash algorithm, and we proof the four requirements that needed to design a practical one way hash algorithm.

General Terms
Cryptographic algorithm, Practical One Way Function

Keywords
Hill cipher technique, Non-invertible matrix, hash algorithm, One-way hash function, plaintext, integrity.

1. INTRODUCTION
Cryptography is a mixture of mathematics and computer science. It is the study and the ability of hiding data. It is also used in other technologies and business applications such as payment. Cryptography has increasingly been used to secure information, But secure data of today could be broken in the future. Cryptography is the science of codes and ciphers. It includes many algorithms and techniques that transfer data safely. It is also inaccessible for non-permitted readers or writers. Computer Security aims to protect the automated information system in order to provide the goals of preserving the integrity, availability and confidentiality of information system resources and services. There are many attacks that harm computers and information security. There are two general methods that attack a symmetric encryption scheme. The first one , known as cryptanalysis, and it relies on the nature of algorithm and some information of the general characteristics of the plaintext message or even some plaintext samples. This kind of attacks exploits the characteristics of the algorithm in order to attempt to infer a specific plaintext or to infer the encryption used key. If the attack succeeds in inferring the key, all the messages plaintext and key are compromised. The second method is the brute-force, and it is used to try every possible key in apart of cipher text until plaintext translation is obtained [16].

Many approaches and countermeasures are set to protect systems' security. A countermeasure is an any mean or any technique that is used to prevent security attack. Ideally, a countermeasure can be devised to prevent a particular type of attacks from harming a computer or information security. If prevention is impossible, or fails in some cases, the goal is to detect the attack, then to recover from the effects of the attack. the countermeasure itself may infer new vulnerabilities. In such cases, residual vulnerabilities may remain after the imposition of countermeasures. Such vulnerabilities may be exploited by threat agents representing a residual level of risk to the assets. Systems owners will seek to minimize that risk by giving other constraints [16].

This paper contains five sections. Firstly, it compares between Symmetric and a symmetric encryption. Secondly, it talks about hash algorithm definition, description, applications and the requirements for one-way hash functions. thirdly, it handles the hill cipher encryption technique. Fourthly, contains our proposed model for one-way hash algorithm with mathematical representations and proves that the inverse of noninvertible matrix does not exist. Finally, is the conclusion and suggestions for future work. [16][7].

2. SYMMETRIC AND A SYMMETRIC ENCRYPTION
Asymmetric encryption uses two separate keys, in the contrary with the symmetric encryption which uses one key only. Symmetric encryption has five components [16], [7]:

• Plaintext: It is the message or any data inserted to algorithm as input.
• Encryption algorithm: It makes some of transformations and substitutions to the message.

• Secret key: One of the inputs of the algorithm and the encryption algorithm itself depend on key in the transformation and substitution process.

• Cipher text: The message that had been scrambled.

• Decryption algorithm: It reverses the encryption algorithm in execution.

A public-key encryption technique components [16],[7]:
• Plaintext: It is the message or any data inserted to algorithm as input.

• Encryption algorithm: It makes some transformations and substitutions to the message.

• Public and private key: A selected pair of keys. if one of the keys is used for encryption, the other one is used for decryption. All transformations and substitutions that are made by the encryption algorithm rely on the public or private key which submitted as input.

• Cipher text: The message that had been scrambled.

• Decryption algorithm: It produces the plaintext from the cipher by reversing the encryption algorithm.

The public key of the pair is made public for others to handle . But the private key is handled only by the owner. A public key cryptographic algorithm depends on a key for encryption and a different key for decryption.

3. HASH ALGORITHM

3.1 Definition, Descriptions and Applications

Algorithm changes messages and text into a fixed string of digits. It usually does so for systems security integrity, confidentiality and availability. The one-way means that it is hard to recover the original text from the hash value string. A one-way hash function is used to create digital signatures. Which in its turn identify and authenticate the sender and the distributed message digitally. One-way Hash functions have an important primitive cryptographic, and it can be used to solve any problems including authentication and integrity. Hash function is a well-defined procedure that converts a large data into a small one. The returned value from hash function is called hash code [6]. One-way hash function is a function that converts a variable string length into a fixed length binary sequence that cannot be reversed, [10],[15],[13]. The Microsoft cryptographic providers support three hash algorithms: MD4, MD5 and SHA [6]. An important element in many computer security services and applications is the usage of cryptographic algorithms .The first type is symmetric encryption like DES algorithm, which is used primarily in the widest variety of contexts. to provide confidentiality. Another type is a secure hash functions like SHA512, MD5 which are used in message authentication. The third type is public-key encryption like RSA. Asymmetric encryption and secure hash functions are combined together to produce an extremely useful tool; Hash functions are used in cryptography with digital signatures for ensuring data integrity when hash used with digital signatures. A public available hash function hashes the message and signs the resulting hash value. The part that receives the message hashes the message and checks whether the block size is authentic for the given hash value [16],[7].

One-way hash function is an alternative to the message authentication code (MAC), which accepts a variable size input and produces a fixed size message. Unlike the MAC, hash code does not require a key as an input to authenticate the message, but a message digest is sent with the message in an authenticated way. The message digest can only be encrypted by using symmetric key if the sender and the receiver share the key. In this way, the authenticity is satisfactory by using public key encryption that does not require the keys to be distributed to the parties [16].

3.2 Requirements for one-way hash function

The following properties required for hash function to be useful:

- Applied to any size of data.
- Hash function (H) produces a fixed-length output.
- $\mathrm{H}(\mathrm{X}) = h$ is relatively easy to compute for any given *x*.
- One-way property.

Computationally infeasible to find *x* such as $\mathrm{H}(\mathrm{X}) = h$ (h is a hash value generated).

- Weak collision resistance.

Computationally infeasible to find $y \neq x$ such that $\mathrm{H}(y) = \mathrm{H}(x)$

- strong collision resistance

Computationally infeasible to find any pair (*x*, *y*) such as $\mathrm{H}(y) = \mathrm{H}(x)$

The first three properties are requirements for a practical application of a hash function to message authentication [16].

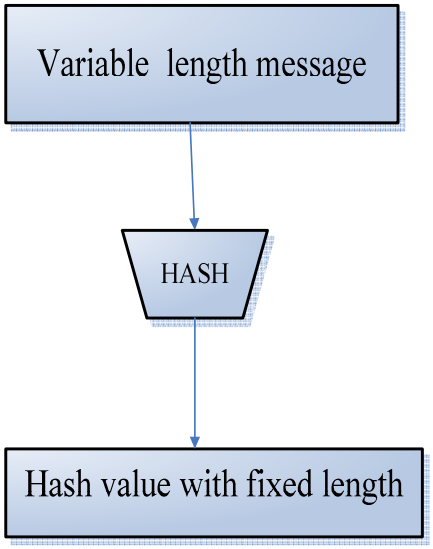

Figure1: secure hash functions [16].

4. HILL CIPHER

Hill cipher, invented by Lester S. Hill in 1929, uses matrix multiplication for mixing the plaintext [3]. The Hill cipher works on groups of letters in different ways [8], [9]. It works by displaying a group of letters as a vector. And encryption is done by matrix multiplication [7] [5].

Hill cipher satisfies properties that good cryptosystems would Have:

Diffusion: One change in plaintext character should affect as many characters as possible in cipher text. We know that hill cipher converts any plaintext character to number, and then inserts it in a matrix of column vector. If we take – be - as plaintext characters then it will be – 1, 4 -, the matrix of column vector will be $\begin{bmatrix}1\\4\end{bmatrix}$ then any change in plaintext must affect cipher text characters.

Confusion: The key should not relate to the cipher text. Hill cipher uses key matrix to encrypt the message and key inverse to decrypt it.

Hill Cipher example with Key Matrix 2×2 uses math equation with Condition: The key matrix has to be invertible relative to 26.

Given Plaintext: $p1p2p3p4.....pn-1pn$ Given Key

Matrix: $k=\begin{pmatrix}a_{11} & a_{12}\\ a_{21} & a_{22}\end{pmatrix}$

Encryption:

1. Form vectors as follows:

$$\begin{pmatrix}p_1\\p_2\end{pmatrix}\begin{pmatrix}p_3\\p_4\end{pmatrix}\begin{pmatrix}p_5\\p_6\end{pmatrix}\cdots\begin{pmatrix}p_{n-1}\\p_n\end{pmatrix}$$

2. Multiply each vector by k to obtain a pair of cipher text letters:

$$k\begin{pmatrix}p_1\\p_2\end{pmatrix}=\begin{pmatrix}a_{11} & a_{12}\\ a_{21} & a_{22}\end{pmatrix}\begin{pmatrix}p_1\\p_2\end{pmatrix}=\begin{pmatrix}c_1\\c_2\end{pmatrix}(\text{mod } 26)$$

$$k\begin{pmatrix}p_3\\p_4\end{pmatrix}=\begin{pmatrix}a_{11} & a_{12}\\ a_{21} & a_{22}\end{pmatrix}\begin{pmatrix}p_3\\p_4\end{pmatrix}=\begin{pmatrix}c_3\\c_4\end{pmatrix}(\text{mod } 26)$$

....

$$k\begin{pmatrix}p_{n-1}\\p_n\end{pmatrix}=\begin{pmatrix}a_{11} & a_{12}\\ a_{21} & a_{22}\end{pmatrix}\begin{pmatrix}p_{n-1}\\p_n\end{pmatrix}=\begin{pmatrix}c_{n-1}\\c_n\end{pmatrix}(\text{mod } 26)$$

3. The cipher text message is: $c1,c2...cn$

Decryption:

1. Calculate k^{-1}

2. For each pair of cipher text find a plaintext by:

$$k^{-1}\begin{pmatrix}c_1\\c_2\end{pmatrix}=\begin{pmatrix}p_1\\p_2\end{pmatrix}(\text{mod}\,26)$$

$$k^{-1}\begin{pmatrix}c_3\\c_4\end{pmatrix}=\begin{pmatrix}p_3\\p_4\end{pmatrix}(\text{mod}\,26)$$

.....

$$k^{-1}\begin{pmatrix}c_{n-1}\\c_n\end{pmatrix}=\begin{pmatrix}p_{n-1}\\p_n\end{pmatrix}(\text{mod}\,26)$$

5. PROPOSED MODEL

The main point of one-way hash function is that any encrypted text cannot be decrypted. From this point ,we need to choose the noninvertible matrix from the hill cipher to use it inside the practical one- way hash algorithm. First we take non-invertible matrix, multiply it by plaintext as column vector with modular

value n to generate the hash value H. The sender of the message calculates the hash value or message digest by using the model. After that the message and the hash value are sent to the receiver who makes the same calculations by using the model to generate a message hash value. Finally, the receiver compares between the messages digest from the sender and the hash value that he calculated.

5.1 Mathematical model

$H(V) = V \times R \bmod N$.

$H(V)$ = **hash value generated.**

V =**plaintext message as column vector**.

R = **non-invertible matrix.**

N = **modular value.**

We use the R as a non-invertible matrix that cannot be reversed, which is used to generate hash value using this formula:

$$H(V) = V \times R \bmod N .$$

R cannot be reversed, If we Calculate the determinant of this matrix d where $d = |R|$, then doesn't relatively prime to N, so R^{-1} doesn't exist and we can't calculate the value of $(H(V))^{-1}$.

Rushdi A. Hamamreh and Mousa Farajallah in their research paper "Design of a robust cryptosystem algorithm for non-invertible matrices based on Hill cipher" have proved that if the non-invertible matrix was used then the encrypted text can never be decrypted [5] and this what we need in our model in order to this satisfy the one way property .

5.2 Proof of practical one way property hash algorithm requirements:

5.2.1 Applied To Any Size of Data

For any input data **v**, let the square matrix has **x** dimension, then the system can convert the input data into vector(s) of **x** length, so if the number of integers consists the input vector less than **x** , then the system will make padding into vector **v** to make the new model applying to any size of data, but if the number of integers consists the input vector **v** more than **x** , the new model will make more than one round in order to applying to any size of data.

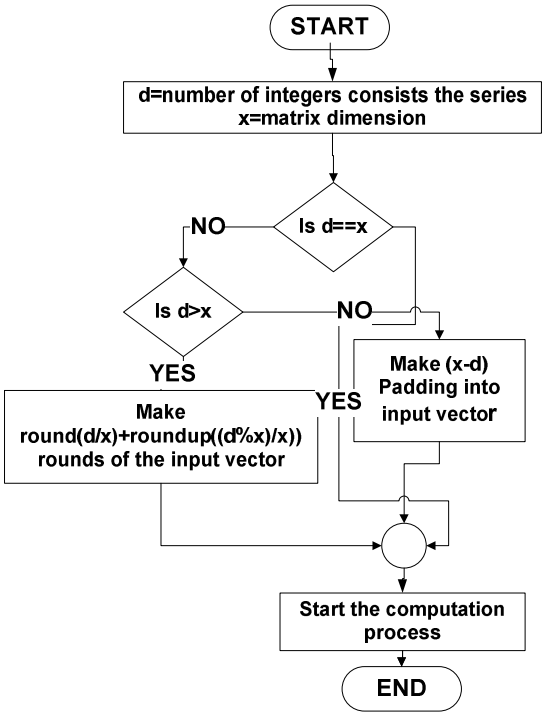

Figure2: steps to make new model applying to any data size

5.2.2 H Produces a Fixed-Length Output

The new model will be able to process an arbitrary-length message into a fixed-length output. this can be achieved by dividing up the input vector into a series of equally sized x vector(s) from a previous point, and operating on them in sequence.

5.2.3 H Relatively Easy To Compute for Any Given X

This property is easy to be found in any mathematical model If and only if the input is known and that makes the output easy to be calculated, and the new model has all the needed input parameters in order to calculate the output.

5.2.4 One-Way Property

The new model based on the following mathematical equation $H(V) = V \times R \bmod N$, where V is the input vector at any round, R is the non-invertible matrix, and N is the modular value of the system, if any user has $H(V)$, and let us assume also he has R and N then he can only formulate the following model $V = H(V) \times R^{-1} \bmod N$, but since R is not invertible matrix he can't solve this equation, so the proposed model is one way function.

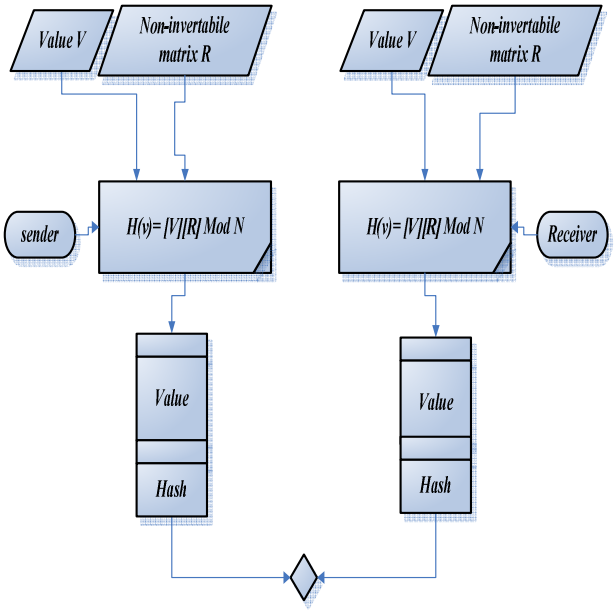

Figure3: practical one way hash algorithm

6. CONCLUSIONS AND FUTURE WORK

This paper proposes a technique to design a practical one-way hash algorithm by using non-invertible matrix that cannot be reversed to produce hash value. We proof the four requirements that a practical one way hash algorithm need. In Future works we need to design an algorithm that convert any invertible matrix into non-invertible one, and then design one way hash algorithm to generate hash value.

7. REFERENCES

[1] Bibhudendra. A, and et al, (2006): " Novel Methods Of Generating Self-Invertible Matrix For Hill Cipher Algorithm ". International Journal of Security, Vol (1), pp:14-21.

[2] Charlie, O, and Behzad, S, (2007): "A Parallel Algorithm for determining the inverse of a matrix for use in block cipher encryption/decryption". The Journal of Supercomputing, Vol (39), pp: 113-130.

[3] Chu-Hsing, L, and et al, (2004): " Comments On Saeednia's Improved Scheme For The Hill Cipher". Journal of the Chinese Institute of Engineering, Vol (27), pp: 743- 746.

[4] DaniloGligoroski†, Smile Markovski†† and Svein J. Knapskog†(2006):"A Secure Hash Algorithm with only 8 Folded SHA-1 Steps", IJCSNS International Journal of 194 Computer Science and Network Security, VOL.6 No.10

[5] Farajallah. M and Hamamreh. R (2009) " Self Generating Multi Keys Cryptosystem Model for Non-Invertible Matrices based on Hill Cipher ", Security and Management 2009, IET SAM09 Conference, Las Vegas, Nevada, USA, 665-672.

[6] Forouzan – Behrouz (2008) .A "Cryptography and Network Security",McGraw Hill..

[7] Hill S. L, (1929): "Cryptography in an algebraic alphabet". American Math. Monthly, Vol (36), pp: 306-312.

[8] Ismail, I. A, and et al, (2006): " How to repair the Hill cipher". Journal of Zhejiang University SCIENCE, copublished with Springer-Verlag GmbH, Vol (7), pp: 2022- 2030.

[9] Jeffrey, O, and et al, (January, 2005): "On the Keyspace of the Hill Cipher". Cryptologia, Vol (29), pp: 59-72.

[10] Johannes Mittmann, (may ,2005): "One-Way Encryption and Message Authentication".

[11] KimmoJrvinen, MattiTommiska and JormaSkytt (2005): "Hardware Implementation Analysis of the MD5 Hash Algorithm", Proceedings of the 38th Hawaii International Conference on System Sciences.

[12] Menezes. A. J and et al, (2001): "Handbook of Applied Cryptography-Discrete Mathematics and Its Applications", Fifth Edition. CRC Press, New York, Inc. USA.

[13] Murray Eisenber (1999): "Hill Ciphers and Modular Linear Algebra".

[14] Rushdi A. Hamamreh, Mousa Farajallah(2009), "Design of a Robust Cryptosystem Algorithm for Non-Invertible Matrices Based on Hill Cipher", International Journal of Computer Science and Network Security; pp 11-16.

[15] Victor Shoup, (2000): " A Composition Theorem for Universal One-WayHash Functions".

[16] William Stallings (2006.), "Cryptography and Network Security Principles and Practices", Prentice Hall.

[17] Yi-Shiung. Y, and et al, (1991): "A New Cryptosystem Using Matrix Transformation". Proceedings of IEEE International Canahan Conference on Security Technology, 1-3 – October – 2008, Taipei, Taiwan pp: 131-138.

[18] Yi-Shiung. Y, and et al, (1993): " HAVAL — A One-Way Hashing Algorithm with Variable Length of Output". Appeared in "Advances in Cryptology — AUSCRYPT'92," Lecture Notes Computer Science, Vol.718, pp.83-104, Springer-Verlag

Mousa Farajallah received the B.S. degree in Computer Systems Engineering from Palestine Polytechnic University (PPU) in 2006, and his M.S degree from AL-Quds University in Jerusalem, now he is lecturer at College of Engineering and Technology at PPU, his research interests are in cryptography and algorithms.

Mohammed Abutaha received the B.S. degree in information Technology from Palestine Polytechnic University (PPU) in 2007, and his M.S degree from PPU University in Hebron, now he is lecturer at College of Applied Professions at PPU, his research interests are in cryptography and information security applications.