ISSN 2347 - 3983
Volume 8. No. 8, August 2020
International Journal of Emerging Trends in Engineering Research
Available Online at http://www.warse.org/IJETER/static/pdf/file/ijeter89882020.pdf
https://doi.org/10.30534/ijeter/2020/89882020

NHAF-512: New Hash Algorithm Applying Feistel Cipher Structure

Christine Charmaine G. San Jose[1], Sabas G. Lazaro, Jr.[2]
[1]Isabela State University, Philippines, tinsanjose1112@gmail.com
[2]Isabela State University, Philippines, sabaslazaro1998@gmail.com

ABSTRACT

This paper aims to design, develop and test the New Hash Algorithm (NHAF-512) applying the feistel cipher structure. The role of hashing algorithm in cryptography is very vital particularly on online communication, transaction and e-commerce where data integrity and authentication is at high concern. The NHAF-512 adopts the substitution and permutation (S-P) concepts of feistel cipher with an increased rounds reaching to thirty-one rounds. The NHAF-512 has larger hash value of 512 bits compared to the well-known MD5 with 128 bits and SHA-1 with 160 bit hash value. This signifies that from the three algorithms, NHAF-512 has a higher security level which can be used to safeguard data integrity and authentication.

Key words : Block Cipher, Ciphertext, Cryptanalysis, Feistel Cipher, Hash Function, Plaintext.

1. INTRODUCTION

The hash algorithm had actually commence in as early as 1953, when a German inventor, Hans Peter Luhn who after working on a textile industry, had joined the IBM with his line of specialization on storage, communication, retrieval of information more particularly on text [1]. During his time, he had invented many mechanical devices and had 70 patented works. One of his many remarkable contributions is the creation of an algorithm known as “Luhn’s Method” with a main purpose to speed up the processing of searching of a telephone directory over a million of records by putting up all related information in a single “bucket”. This method is being performed by simply manipulating numbers using mathematical operations. A decade past, many computer scientists had made enormous improvement over Luhn’s method and had creatively thought of applying it into new uses such as in cryptography, this had paved the way to the development of hashing technology.

Several hash algorithms were developed [2] and among them are as follows: MD4 (Message Digest 4) developed in 1990, two years after, MD5 (Message Digest 5) was developed. It is followed by DMDC (Des-like Message Digest Computation) in 1994 and followed by SHA-1 (Secure Hash Algorithm 1) in 1995 and had several versions. Among the latest and noted as the strongest hash algorithm on the time being is SHA-3 (512).

From the year 1960 to 1971, a group from IBM led by Horst Feistel [2] had initiated a research project named it as ”Lucifer” for computer cryptography and became the first ever known block cipher operating 64 bits per block using 128 bit key size this algorithm was also known as “Feistel Cipher”. Another effort was again initiated by IBM in 1973, to produce a commercial encryption scheme and named it as: DES (Data Encryption Standard). This was led by Walter Tuchman. The DES is actually an improved version of the project lucifer which was noted as resistant to cryptanalysis. The DES was adopted as federal standard and was used by U.S. government communication in 1976. With a very strong internal structure of DES, it was used for over 20 years.

There are researches that had proposed for an improvement of Feistel Cipher, among these researches are [3], [4] and [5]. On the work of [3], the author had made revision on its structure by incorporating improvement on operation such as XOR operation with a Key and Shuffling, substitution, shifting of rows, mixing of columns. With the revisions made, it has shown positive changes in terms of its security. The study of [6], is a survey to review lightweight block cipher (LWC) through integration of cryptographic primitives into devices. The result displayed good performance and widely used for integrity check and authentication. The first hash algorithm that applied DES structure is the DMDC (Des-Like Message Digest Computation). It is one-way hash function that produces four different hash values (18, 32, 64 and 128). This was primarily designed and used in CDMA mobile communication.

Another primitive and widely known cipher algorithm is the Caesar Cipher. It is considered as one of the conventional encryption which is also referred as symmetric encryption using single-key encryption. It uses the substitution technique, for this reason, Caesar cipher was also known as “Shift Cipher”. The authors [7] had improved the Caesar Cipher algorithm through using the Goldbach Code Compression which made the algorithm more efficient. A symmetric key encryption was also used in the study of [8] to provide security. It is a novel secret key generation scheme

used in Mobile ad-hoc Network (MANET) communication. This paper will engage towards the design, development and testing of the new hash algorithm applying feistel cipher structure with 512 bit hash value.

2. FEISTEL CIPHER STRUCTURE

The Feistel Cipher is a block cipher developed by Horst Feistel which is based on Shannon's substitution – permutation (s-p) concept. It takes any amount of data and process it into certain bits per block and each of the block will be divided into two equal part making L0 and R0 an equal part. The figure below shows the Feistel Cipher structure [2].

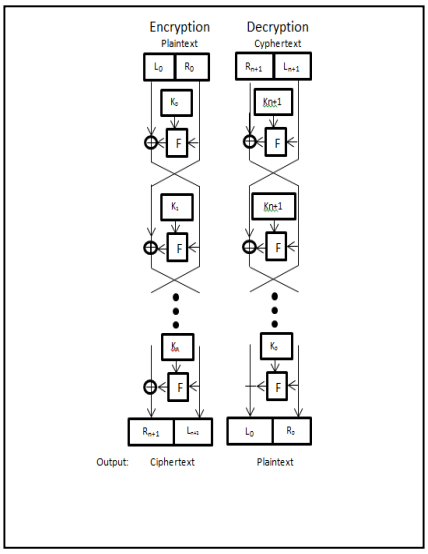

Figure 1: Feistel Cipher Structure.

It primarily divides block input data into halves and processes it into multiple rounds such as substitution (S-box) and permutation swapping (P-box). The fiestel cipher is based on the following parameters and design: Block size, Key size and number of rounds. The larger the block size and key size means more secure but with one disadvantage which affects the speed of processing time. Moreover, the greater number of rounds of iteration will also contribute to an increase of security.

3. NHAF-512 ARCHITECTURE

The development of the NHAF-512 (New Hash Algorithm applying Feistel Cipher) is based on careful planning through application of design tool particularly on its algorithm. The Feistel cipher structure was also simulated to determine the different mathematical calculations involved in its processes. For the development phase, the author had considered the Java programming language and Sublime text editor. After debugging errors and incorporating revisions, the NHAF-512 was developed. The testing and simulation is necessary in order to check whether the correct calculations involved in the design are achieved.

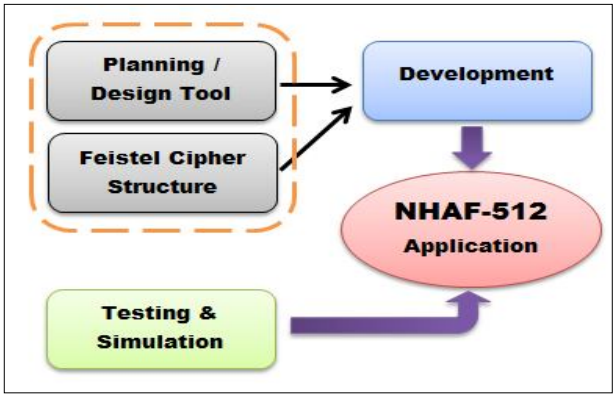

Figure 2: NHAF-512 Architecture

3.1 NHAF-512 Schemes

The study proposed for a new hash algorithm applying the feistel cipher structure and named it as NHAF-512 which stands for New Hash Algorithm applying Feistel - 512. The output of NHAF will produce a 512 bits hash value. The processing of the plaintext is divided into 512 bits per block, each block will undergo several process.

The NHAF-512 incorporates the feistel cipher of the first part of the algorithm, after which several mathematical computations will follow. Below is the pseudo code of the NHAF-512 algorithm.

1- Process plaintext 512 bit per block
2- Each 512 bit per block is divided into 256 equal parts (PL and PR)
3- PL1 is equal to the XOR of F(PL0) and PR0
4- Substitute PL0 to PR1
5- The process will loop for 31 Rounds

The NHAF-512 structure on figure 3 shows how feistel cipher structure is applied.

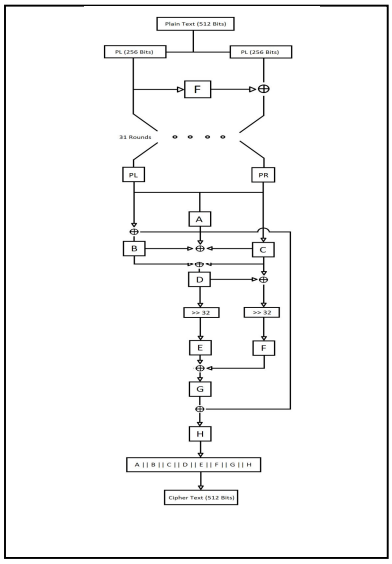

Figure 3: NHAF-512 Structure

3.2 NHAF-512 Development

The system, following the proposed NHAF-512 Scheme as seen on figure 3 was developed using Java Programming Language and sublime as the text editor. Java is one of the most popular programming languages at the time being [9] that works on many platforms. It is used in many application such as mobile, desktop and web application, game, database connection and many others. The sublime text [10] is a source code editor that supports many programming languages and markup languages. The figures below are the sample java code using sublime text of the developed system.

3.2.1. Development

The figures below are the sample Java source code of the developed System. The figure 4 shows the sample java class file while figure 5 shows the header file of the developed system. The figure 6 shows the sample java source code of the system.

(a) Java Class File

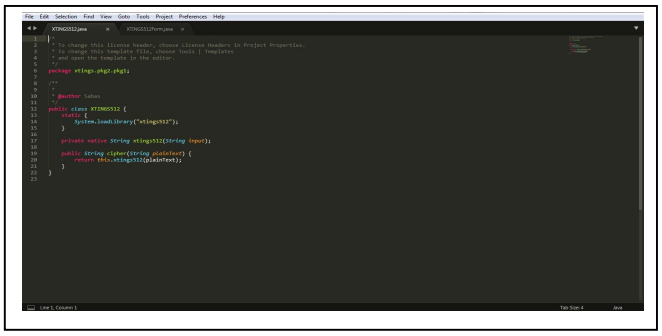

Figure 4: Sample Class File

(b) Sample Header File

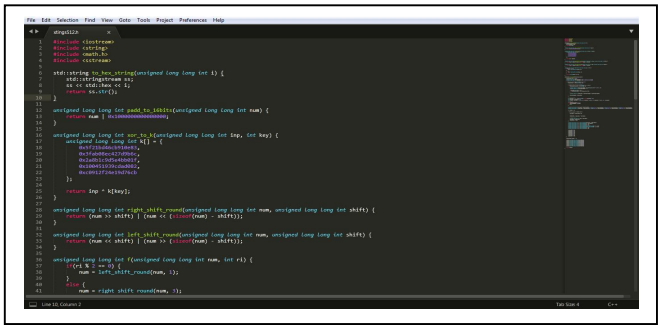

Figure 5: Sample Header File

(c) Sample Source Code of the System

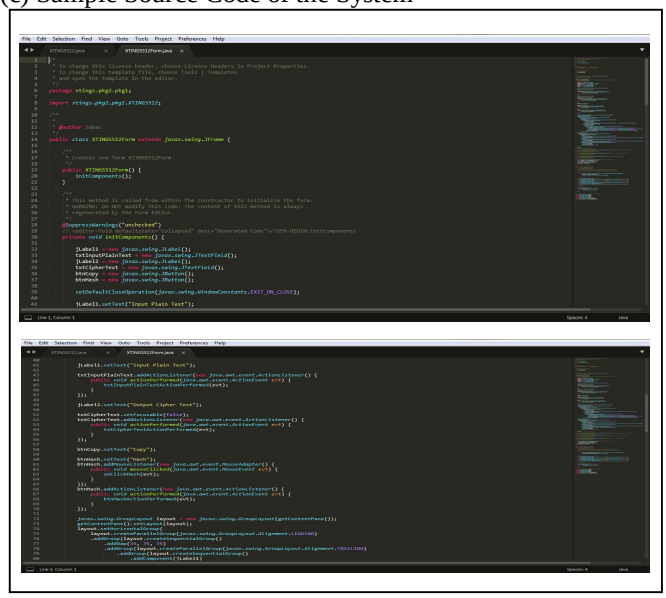

Figure 6: Sample System Source Code

3.2.2. System Screenshots

The developed system is a desktop application which consists of two textboxes and two command buttons. This can be seen on figure 7. The first textbox is labeled “Plain Text” and is primarily used for user to enter any text/plaintext to be hashed. The second textbox, labeled “Cipher Text” is used to display the hashed value of the plaintext. There were two command buttons, the first command button is labeled “Hash” and the other is labeled “Copy”. The Hash command button is simply used to hash any entered plaintext while the Copy command button is used to copy the hashed value to any desired place.

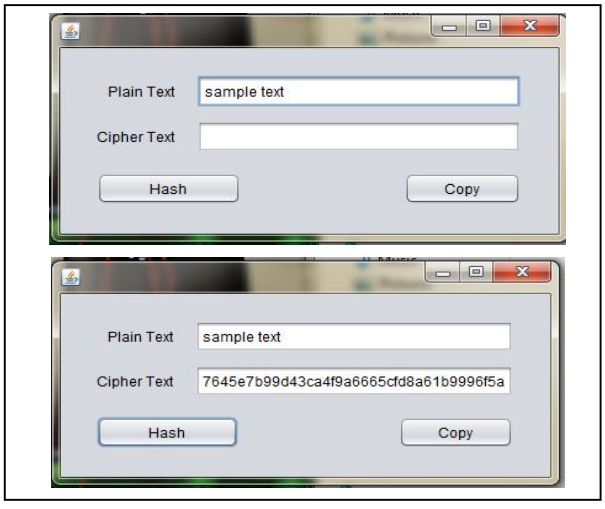

Figure 7: NHAF-512 Main Page

3.2.3. Testing NHAF-512

The developed NHAF-512 applying feistel cipher structure will produce a 512 bit hash value. The table1 shows the sample hash value of the three plaintexts. The entered plaintexts are as follows: “ISUCCSICT”, “Philippines” and “Mysterious”. The corresponding hash values for this plaintext are displayed on the third column displaying the 512 bit hash value of each plaintext.

Table 1: NHAF-512 Hash Value

No.	Plaintext	Hash Value
1	ISUCCSICT	b36eb0cf0a66893c94eba2797644cc4d378512b67c224571b36eb0cf0a66893c54cc4d0084eba2791a66893c00a36eb05eaac43c8448ccc9fdc474f38e2e45f5
2	Philippines	1f48664f5a27980ff69c029881f66961f9d464d7dbd1f16e1f48664f5a27980ff6696100e69c02985a27980f000f4866bc4ef90fe6934afeb3069f40bcb4d2f1
3	Mysterious	f72cf3c81f63ca3ffc8e40bb376ec95d1ba2b373280d0362f72cf3c81f63ca3f7ec95d00ec8e40bb1f63ea3f00e72cf371aab73fec696c48968664f7f30aa677

HASH ALGORITHM	HASH VALUE	NUMBER OF BITS
MD5	f9c2838a76dcf9cdced88ef121cb1532	128 bits
SHA-1	03b109b8258553e3b10bc25bd808bfe6edd4045e	160 bits
NHAF-512	b36eb0cf0a66893c94eba2797644cc4d378512b67c224571b36eb0cf0a66893c54cc4d0084eba2791a66893c00a36eb05eaac43c8448ccc9fdc474f38e2e45f5	512 bits

Table 2: Hash Comparison of Plaintext “ISUCCSICT”

The table 2 shows the hash value of the plaintext ”ISUCCSICT” when tested to MD5 [11], SHA-1 [12] and NHAF-512 with corresponding number of output in bits. It can be seen on the table that the NHAF-512 has the largest number hash value.

4. CONCLUSION

The role of hashing algorithm in cryptography is very vital. As such, we cannot deny the astounding relevance of cryptography in the present day where on-line transactions, e-commerce, social media, mobile application as a domino effect due to the availability of internet technology is uncontrollably rearing. An improved version of previous security scheme was continuously being developed producing a more secure cryptographic algorithm. The Luhn’s method was the first to perform simple manipulation of numbers using mathematical operations to speed up business process, and a decade after, the “Lucifer” or Feistel Cipher was developed - the first ever known block cipher that became the basis of the development of the famous DES (Data Encryption Standard) algorithm. Years thereafter gives birth to the development of stronger algorithm with robust computation. The brilliant minds of previous inventor had placed us in a situation that technology is made available for utilization of today’s generation. Stronger and faster computer will be produced, continues improvement on security scheme is indeed necessary.

This paper was able to achieve its objective in the design, development and testing of the new hash algorithm applying the Feistel Cipher Structure. The NHAF-512 is a desktop application developed using Java programming language and Sublime text editor following the scheme on figure 3. The sample code of the developed application can be seen on figure 4, 5 and 6. The running applications as seen on figure 7 consist of two textboxes and two command button. With the application, the user can enter any plaintext and will produce a fixed 512 bit hash value. To test the NHAF-512, on table 1, three plaintexts were entered. It can be seen on the table the hash value of each of the plaintext. The hash value of each of the three plaintexts produces a fixed 512 bit or 128 characters. The 512 bit hash value of NHAF-512 is far much larger than the well-known MD5 with 128 bit and SHA-1 with 160 bit value. This signifies that the NHAF-512 has higher security level which can be used to safeguard data integrity and authentication.

ACKNOWLEDGEMENT

The authors wish to thank Research Development Extension and Training Office of Isabela State University, Echague Main Campus, Philippines in financing this research.

REFERENCES

1. Stevens, **Hans Peter Luhn and the Birth of the Hashing Algorithm**, *IEEE Spectrum, 2018*, Available at: https://spectrum.ieee.org/tech-history/silicon-revolution/hans-peter-luhn-and-the-birth-of-the-hashing-algorithm
2. M. Rhee, **Internet Security, Cryptographic principles, algorithms and principles**, *John Wiley & Sons, Ltd* ISBN 0-470-85285-2, 2003.
3. Sastry and A. Kumar. **A Modified Feistel Cipher Involving Substitution, shifting of rows, mixing of columns, XOR operation with a Key and Shuffling**, *(IJACSA) International Journal of Advanced Computer Science and Applications*, 2012.
4. E. Al-Bahrani and R.Kadhum. **A New Cipher Based on Feistel Structure and Chaotic Maps**, *Ghana Social Science Journal*, Vol.16(1):270-280, 2019.
5. F. Noorbasha, K.Kishore. **Implementation of modified Feistel block cipher for OTP generation using Verilog**

HDL, *Computer Science International journal of engineering and technology*, 2018.

6. G. Hatzivasilis, K. Fysarakis, I. Papaefstathiou and C. Manifava. **A review of lightweight block ciphers**, *Journal of Cryptographic Engineering* ,8(2):1-44, 2017.
7. J.C. Arroyo and A.J. Delima, **Caesar Cipher with Goldbach Code Compression for Efficient Cryptography**, *International Journal of Emerging Trends in Engineering Research* (IJETER) Vol. 8, No.7, 2020,
8. K. Shibu K and P. Suji, **A Novel Secret Key Generation Scheme for MANETs using Traffic Load to Avoid Active Attackers**, *International Journal of Emerging Trends in Engineering Research (IJETER),* Vol. 8, No.5, 2020.
9. W3schools.com, Java Tutorial, available at: https://www.w3schools.com/java/java_classes.asp
10. Wikipedia.org,Sublime Text, available at: https://en.wikipedia.org/wiki/Sublime_Text
11. Dan's Tools, **MD5 Hash Generator**, 2019, https://www.md5hashgenerator.com/.
12. SHA-1 and other Hash Functions Online Generator, available at: http://www.sha1-online.com/.