Digital Innovations
& Contemporary Research in SCIENCE,
ENGINEERING & TECHNOLOGY
Vol. 10. No. 4, December 2022 – Special Issue on Cryptography & Security Mechanisms

Article Citation Format
Kpieleh, F. (2022): Cryptographic Hash Functions For Digital Stamping. Journal of Digital Innovations & Contemporary Research in Science, Engineering & Technology.
Vol. 10, No. 2. Pp 65-72
DOI: dx.doi.org/10.22624/AIMS/DIGITAL/V10N4P9

Cryptographic Hash Functions For Digital Stamping

Kpieleh Ferdinand
School of Technology
Ghana Institute of Management & Public Administration
GreenHills, Accra, Ghana
E-mail: ferdinand_kpieleh@yahoo.com
Phone: +233502024517

ABSTRACT

The current study's objectives are to analyze a broad overview of hash function applications in cryptography and investigate the connections between digital signature applications and cryptographic hash functions. Applications of the hash function are widespread and used for a variety of purposes, including password hashing, file integrity verification, key derivation, time stamping, rootkit detection, and digital signatures. Cryptographic hash functions are a crucial tool used in many sections of data security. A digital signature is a code that is electronically associated with a document and includes the sender's information. As a result, the usefulness of the digital signature in validating digital messages or documents is great. Without mathematics, there would be no cryptographic hash functions. Mathematics is credited with computer science's success, or, to put it another way, it is because of mathematical science that computer science is understood and can be explained to everyone. The study's main goals are to explain hash functions to the reader, as well as some of their uses, including digital signatures, and to provide detailed examples of some hash functions and their creation.

Keywords: Hash Function, Cryptography, Digital Stamping

1. INTRODUCTION

The TIFF, JPG, and PNG forms of the digital stamp used in scrapbooking, stamping, and crafting are printed on the paper. Because they can be enlarged, flipped, conveniently stored, and rotated, digital stamps have several advantages over rubber stamps (Salem et al., 2019). Additionally, if the paper is sealed, digital stamps can be printed using a variety of colors, including watercolours, Copic markers, and colored pencils. There are numerous businesses that create digital stamps worldwide (Ladani & Gazanchaei, 2014).

Except for being inside the computer, the digital stamp used in philately and mail is identical to the postal stamp. However, the digital stamp can be downloaded and printed. Some artistamp releases have survived in the digital realm as images. For straightforward authorisation and data exchange, the digital stamp can be changed and replicated (Haber & Massias, n.d.). The cryptographic hash performs a mathematical operation.

The input and output of hash functions are typically both fixed lengths. Message passing and security features are integrated with the cryptographic hashing function (Bao Fumin et al., n.d.). Information input into computing systems, such as authenticating data and ensuring message integrity, is done using hash functions. It is challenging to decode the message information thanks to function cryptographic hash, which adds a security component to the hash functions (Pei Yin et al., n.d.).

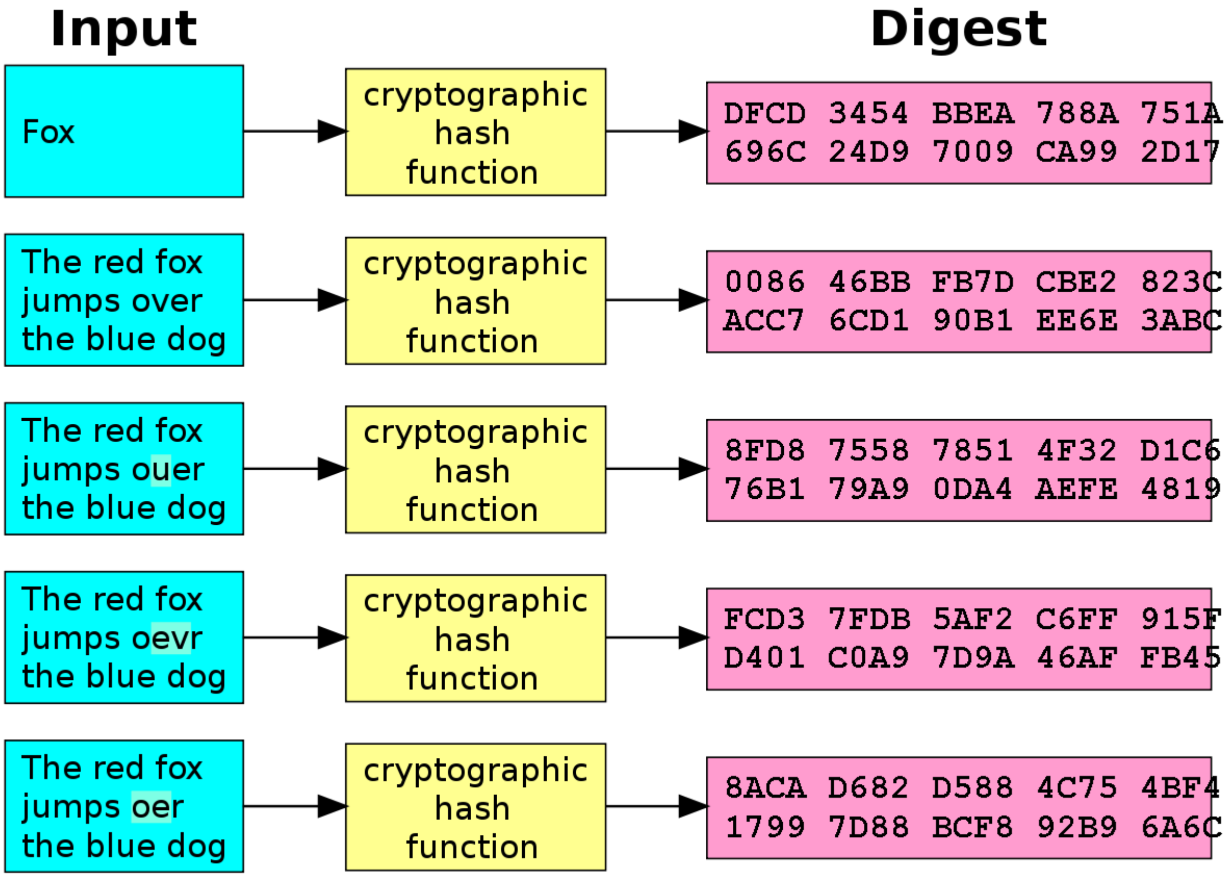
Input
Digest
Fox
cryptographic hash function
DFCD 3454 BBEA 788A 751A
696C 24D9 7009 CA99 2D17
The red fox jumps over the blue dog
cryptographic hash function
0086 46BB FB7D CBE2 823C
ACC7 6CD1 90B1 EE6E 3ABC
The red fox jumps ouer the blue dog
cryptographic hash function
8FD8 7558 7851 4F32 D1C6
76B1 79A9 0DA4 AEFE 4819
The red fox jumps oevr the blue dog
cryptographic hash function
FCD3 7FDB 5AF2 C6FF 915F
D401 C0A9 7D9A 46AF FB45
The red fox jumps oer the blue dog
cryptographic hash function
8ACA D682 D588 4C75 4BF4
1799 7D88 BCF8 92B9 6A6C

Fig 1: Cryptographic Hash Functions
Source: https://en.wikipedia.org/wiki/Cryptographic_hash_function

Three characteristics of cryptographic hash functions are:

- Two so-called collision-free input hashes that approximate output hashes.
- The so-called hidden output value determines how difficult it is to know the input value.
- It is impossible to select an input value that will provide a puzzle-friendly outcome (Rjaško, 2012).

The rest of the sections in this book are as follows, Literature Review, Design of Hashing Algorithms, Use of Cryptographic Hash Functions, The benefits and drawbacks of digital stamping and Conclusion.

2. LITERATURE REVIEW

All applications involving data security frequently use hash functions. It has mathematical properties. Values returned by a hash function are called hash values or message digests.

I. Hash function types

1. Fixed Length Output

- As part of the process of hashing data, length (arbitrary) is converted to a fixed length.
- The input data reduces the hash value: Hash functions call compression functions.
- When compared to enormous data, a digest indicates that the hash is little data.
- The hash function values ranged from (160 to 512) bits.

2. The Effectiveness of the System

- Fast operation means that the input represents h when using the hash function (x).
- where h stands for the hash function and x for the input.
- Hash functions are faster than symmetric encryption (Andreeva et al., n.d.), (Hussein et al., 2019).

II. Hash Function Specifications

Resistance to Pre-Image

Reverse engineering a hash function is challenging. Finding the final input value when the hash function generates a hash value is particularly challenging (x). That guards against an intruder.

- Resistance to the second pre-image

Finding the input value with the same hash is challenging. This stops an attacker from trying to modify a hash value after obtaining it and its input.

- Resistance to Collision

Two inputs cannot have the exact same hash value. Using the has function, find the two inputs (x) and (y).

3. DESIGN OF HASHING ALGORITHMS

A hash code is produced by the mathematical operation of hashing using two specified sizes. The block size typically consists of (128–512) bits. Block cipher is one of the numerous hashes functions that are included in the hashing algorithm. Every round starts with a fixed-size input, a mix of message blocks, and the results from the previous round. The process required repeating numerous rounds and hashing each message.

I. Hashing operations

- Initial Message Digest

A hash function like MD5 has been in use for a while. There were MD2, MD4, MD5, and MD6 in it. Typically, file servers offer MD5. In an hour, the analytical attack's success was established. The MD5 collision attack results.

- Secure Hashing Technique

It had four different SHA types: SHA-3, SHA-2, SHA-1, and SHA-0. Despite being a member of the same family, it can take many different forms depending on the structure. The first version of (SHA-0) has (160) bits; in 1993 and 1995, SHA-1 was created to address SHA-0's shortcomings and is now the most widely used.

- RIPEMD

These hashing operations have proven to be effective. RIPENED instances include RIPEMD-160 and RIPEMD-128. There are two variations: 256-bit and 320-bit.

- Whirlpool

It consists of a hash function with 512 bits. There are various varieties, three of which are WHIRLPOOL, WHIRLPOOL-T, and WHIRLPOOL-0.

II. Applications of Hash Function

- Password Keeping

The password is shielded by it. It stops passwords from being stored in plain text. The table with the password file included contains (Id, h) (P).

- Verifying the Data Integrity

It appears frequently in hash functions. From it, check sums for data files were produced. reassure users by confirming that the data in the program is accurate.

- Electronic Signatures

They serve as message authentication keys. The communications frequently include handwritten signatures. A digital signature is a method of connecting the named individual with the digital information.

III. The Process' General Description

- There are two keys for each user of this scheme (public and private).
- Signing and validating could be done using the two keys. Wherever the private key is used for signature and the public key is used for verification, encryption and decryption are different.
- The person who gave the hash function the data.
- The digital signature is created by feeding the signature algorithm the hash value and signature key.
- The verifier provides the verification algorithm with the verification key and digital signature that it produced some output value with.
- The user creates the hash value using the same data hash function.
- The verifier can tell the digital signature is false because of compression between the hash value and the verification algorithm's output.
- The user's private key is used to create a digital signature.

IV. The significance of digital signatures

An essential tool for handling data security is the public key. Message authentication and data integrity are provided by the digital signature.

- Data Integrity

The digital signature is useless if the attacker is successful in obtaining the data. The output and the modified data do not agree.

- Message authentication, second

The public key is used to reveal the digital signature to the user.

- Non-Repudiation

The user only has access to the signature key and can only use it to generate a singular signature.

V. Use of a digital stamp for encryption.

Only the holder of the key that permits decryption can read a document that has been encrypted. Information secrecy is provided by the digital stamp's encryption. If a communication or document is encrypted such that only a specific user can decrypt it and read it, the sender must have a certificate for that person on hand since encryption uses the public key. The user's smartcard is required for decryption because encryption relies on the private key. It is possible to combine encryption and a digital signature: a document can first be signed, and then it can be encrypted to ensure both authorship and secrecy.

4. USE OF CRYPTOGRAPHIC HASH FUNCTIONS

- Message Digest: A function frequently referred to as irreversibility, which does not produce output values from input values.
- Password Verification: Password verification includes password verification.
- There are numerous computer languages that have been utilized in data structures. The primary goal is to produce unique key-value pairs, and the keys can include Hash Set, C++, and Java hash maps.
- Compiler operation: Where the compiler preserves all keywords in implemented groups, the distinction between a programming language's keywords and other identifiers.
- Rabin-Karp Algorithm: Wherever the compiler saves all keywords in implemented groups, it distinguishes between a programming language's keywords and other identifiers.
- The file's name and path together: When observing files, we learn that they consist of two parts: the file path and the file name. A hash table is utilized to implement the map, which is used to store the file's name and path.
- Digital stamp: the same postage stamp used in mail but saved electronically. It is downloadable and printable for use on packaging.

I. Electronic documents (Text, Audio, Video)

The hashing approach is becoming more significant as video and graphics are used so frequently. A method used to stop any hacker user from obtaining multimedia material is called digital fingerprinting. Additionally, it employs wireless networking and mobile computing strategies; multimedia data is frequently transmitted via shaky wireless networks where packet losses or mistakes are possible.

The employment of hash functions is common in the digital world. It is used to find related files (such as for spam and virus detection). Additionally, it processes high-dimensional data using picture classification. Hashing is utilized for picture representation learning, compact binary codes, high search speed, and low storage cost.

II. A Basic Scheme Considering a Third Party

To stop a fraudulent user from utilizing the public key, it is crucial to authenticate the public key. Without authentication, a hacker might intercept, decrypt, and utilize all messages sent between the sender and receiver. A digital signature like the CA signature is used to provide the certificate. The assumption cannot be maintained if the CA is destroyed due to a system failure, a conflict, or acts of terrorism. We should come up with a workable and straightforward method for independently authenticating the public key. The approach employed the message authentication code to obtain a quick value for authenticating public keys.

III. Utilize the Merkle Tree when digitally stamping.

Merkle trees are still trees. The Merkle tree or hash trees enable efficient data verification. Hash chains and hash lists make up hash trees. The leaf node is displayed as a section of a hash tree that needs a certain number of hashes. All sorts of stored data could be verified by hash trees. On a peer-to-peer network, it can receive data blocks. The hash trees are also utilized by Btrfs, ZFS and IPFS, the Apache Wave protocol, the Dat protocol, the Tahoe-LAFS backup system, and Zeronet.

The benefits and drawbacks of digital stamping

I. Benefits of Electronic Signatures

For use in cardmaking, scrapbooking, and paper, digital stamps can be printed. TIFF, JPG, and PNG are just a few of the many formats that the digital stamps accept. It can be scaled, rotated, and readily stored. Additionally, it can take any color when it is heated to seal. The application of its digital stamp is simple.

Authorized individuals might print and download a digital stamp to put on shipments or envelopes. Additionally, it might be encoded as commenting or nodding in approval on a digital copy of the material. The digital paper stamp can be customized when initialed, signed, or noted (Shay Gueron, 2017), (Paar & Pelzl, 2010).

II. Drawbacks of Digital Stamping

The restrictions on digital stamps only apply to projects using printed images. This indicates that it employs digital stamp images to decorate non-printable surfaces. Therefore, it is challenging to utilize digital stamps on cardstock, cloth, pre-formed boxes, very thick or thin paper, and enormous pieces of paper.

In addition to the ever-expanding stamping family, many of the functions of digital stamps are also used with conventional stamps (Alharbi & Abdullah, 2019), (MacCormick, 2011), (B. Thigale et al., 2019), (N. Mohammed et al., 2019).

5. CONCLUSION

It's crucial to use hash algorithms while encrypting data, especially when using a digital stamp. The cryptographic hash function is used in file integrity verification, key derivation, password hashing, and digital timestamping, and it has major advantages in information security across the board. It offers the highest level of security for messages and documents. A digital code called a "digital stamp" is added to messages to give them high authority and to verify the sender's identity.

Data security is being developed by using digital stamps. Verifying the sender's and receiver's identities is essential for all forms of digital security. More people will utilize computer applications safely and without issues as digital stamps are developed.

REFERENCES

Alharbi, E., & Abdullah, M. (2019). Asthma attack prediction based on weather factors. *Periodicals of Engineering and Natural Sciences (PEN)*, *7*(1), 408. https://doi.org/10.21533/pen.v7i1.422

Andreeva, E., Neven, G., Preneel, B., & Shrimpton, T. (n.d.). Seven-Property-Preserving Iterated Hashing: ROX. In *Advances in Cryptology – ASIACRYPT 2007* (pp. 130–146). Springer Berlin Heidelberg. https://doi.org/10.1007/978-3-540-76900-2_8

B. Thigale, S., Pandey, R. K., Gadekar, P. R., Dhotre, V. A., & Junnarkar, A. A. (2019). Lightweight novel trust based framework for IoT enabled wireless network communications. *Periodicals of Engineering and Natural Sciences (PEN)*, *7*(3), 1126. https://doi.org/10.21533/pen.v7i3.624

Bao Fumin, Li Aiguo, & Qin Zheng. (n.d.). Photo Time-Stamp Recognition Based on Particle Swarm Optimization. *IEEE/WIC/ACM International Conference on Web Intelligence (WI'04)*, 529–532. https://doi.org/10.1109/WI.2004.10167

Haber, S., & Massias, H. (n.d.). Time-stamping. In *Encyclopedia of Cryptography and Security* (pp. 616–620). Springer US. https://doi.org/10.1007/0-387-23483-7_431

Hussein, K. A., Mehdi, S. A., & Hussein, S. A. (2019). Image Encryption Based on Parallel Algorithm via Zigzag Manner with a New Chaotic System. *Journal of Southwest Jiaotong University*, *54*(4). https://doi.org/10.35741/issn.0258-2724.54.4.29

Ladani, M. J., & Gazanchaei, A. K. (2014). *Erratum to: Using Asynchronous Hot Standby Spare in Time-Stamped, Fault-Tolerant, Real-Time System* (pp. E1–E1). https://doi.org/10.1007/978-3-642-53751-6_66

MacCormick, J. (2011). *Nine Algorithms That Changed the Future*. Princeton University Press. https://doi.org/10.2307/j.ctt7t71s

N. Mohammed, G., Abdul Hassan Al-Fatlawi, A., & Talal Kamil, A. (2019). Combined DWT-DISB based image watermarking optimized for decision making problems. *Periodicals of Engineering and Natural Sciences (PEN)*, *7*(3), 1009. https://doi.org/10.21533/pen.v7i3.633

Paar, C., & Pelzl, J. (2010). *Understanding Cryptography*. Springer Berlin Heidelberg. https://doi.org/10.1007/978-3-642-04101-3

Pei Yin, Xian-Sheng Hua, & Hong-Jiang Zhang. (n.d.). Automatic time stamp extraction system for home videos. *2002 IEEE International Symposium on Circuits and Systems. Proceedings (Cat. No.02CH37353)*, II-73-II–76. https://doi.org/10.1109/ISCAS.2002.1010927

Rjaško, M. (2012). *Black-Box Property of Cryptographic Hash Functions* (pp. 181–193). https://doi.org/10.1007/978-3-642-27901-0_14

Salem, I. E., Salman, A. M., & Mijwil, M. M. (2019). A Survey: Cryptographic Hash Functions for Digital Stamping. *Journal of Southwest Jiaotong University*, *54*(6). https://doi.org/10.35741/issn.0258-2724.54.6.2

Shay Gueron, N. M. (2017). SPHINCS-Simpira: Fast Stateless Hash-based Signatures with Post-quantum Security. *IACR Cryptol. EPrint Arch.*, *2017*, 645.