© CSVTU Research Journal: Swami Vivekanand Technical University All Rights Reserved.

CSVTU Research Journal

Vol. 10(1), 33–36 2021 ISSN: 0974-8725

S-HASH: A Crack Towards Cryptographic Hash Functions

Kaushal Jangid[1], Vidushi[2]

[1]Chhattisgrah Swami Vivekanand Technical University**,** Chhattisgarh-491107, India
[2]Department of Computer Science and Engineering, HMR Institute of Technology and Management Bakoli HMRITM Rd, Hamidpur, New Delhi, Delhi 110036, India.
kaushaljangid10@gmail.com; vidushi.mtech@gmail.com

Received May 24, 2021; received in revised form June 18, 2021; accepted June 2021; Available online August 2021

Abstract

S-HASH is tool based on Perl, is used to hack/crack the cryptographic hash function, which is a combination of message which is defined to be of arbitrary length and a message digest defined of fixed length. For cracking the hash values two techniques namely: dictionary attack and the brute-force attack are used. This paper presents the reviews on several hashing function (like MD5, and various types of SHA) along their cracks.

Keywords: Cracking, HASH functions, MD5, SHA1, SHA224, SHA256, SHA384, SHA512.

Research Article

1. Introduction

Hashing is a function which is required for creating a fixed-size digest from the variable message. Hash value, hash sums, hash code are the value which are returned by the hash function. Hash table is used in computer software's data structure to look up the data and are known as one way encryption. No key is required in hashing function and only encryption can be done whereas Decryption is not possible. The properties of Hashing function include Pre image resistance, collision resistance and the second- pre image resistance.

1.1 Hash

MD: Its stands for message digest algorithm given by Ron Rivet referred as MD2, MD4 and MD5. MD5 is the latest version and the strength-end versions of the MD4 that create a 128-bit digest from 512 bits. According to [1], it is found as too small in resisting collision attack.

SHA (Secure Hash Algorithm): -SHA is a standard algorithm which was developed by (NIST) National Institute of Standards and Technology and was published as a processing standard towards federal information [2]. It was based on Message digest 5, which was revised in 1995 under FIP 180-1. That has also included SHA-1. However, FIPS-2 has declared four new versions, t+hat is, defines four new versions SHA-224, SHA256, SHA-384, and SHA-512. Simply collision attack is use to break the whole version of hashes because there is no way of reversing it.

SHA -1 is not considered as a secure hash, as in 2005, the cryptanalysts has found the attacks and have suggested that the algorithm is not secure. In 2010, the researchers have recommended that to replace the SHA-1 through SHA-2 or SHA-3as produced in [3]. Although SHA forms are the widely used and

well-defined security applications and protocols,
including TLS and SSL, PGP, SSH, S/MIM E, and IPsec, as produced in [4].

1.2 S-HASH

The s-hash may run on any operating system as Perl is a cross platform and is a high-level language designed by Larry Wall.

System requirement:

i. Linux operating system any version.
ii. Perl

Hardware requirement:

i. 1 GHZ processor.
ii. 512 RAM.
iii. 100 MB of available disk space for the application Perl.

Procedure of using of S-HASH

Open the terminal and type the command for the Perl script
>Perl<name-of-your-script.pl>

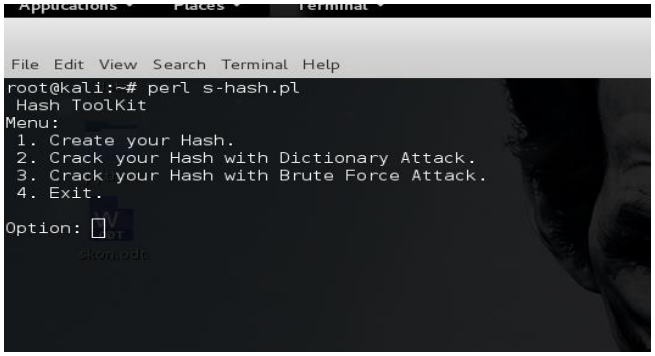

Fig. 1 Creating the Hash Code towards the initializing of Hash Tool kit.

Then, S-hash provides four options:

i. Create hash.
ii. Dictionary attack.
iii. Brute-force attack.
iv. exit

While creating the hash, a string is taken by the user which is converted in to fixed length of hash code. Fig 1 shows the creation of your hash code example shown below:
The given string is apple and the hash code of apple is as follows:

MD5:
1f3870be274f6c49b3e31a0c6728957f

SHA1:
347f437d65829303cf6c49b0989dd218f3fyh w3

SHA224:
b7bbfdf1a1012999b3c466fdeb906a629caa5 e3e022428d1eb702281

SHA256:
55562347f437d65829303cf6307e71acf8b84 a020989dd218f31586eeafd01a9

SHA384:

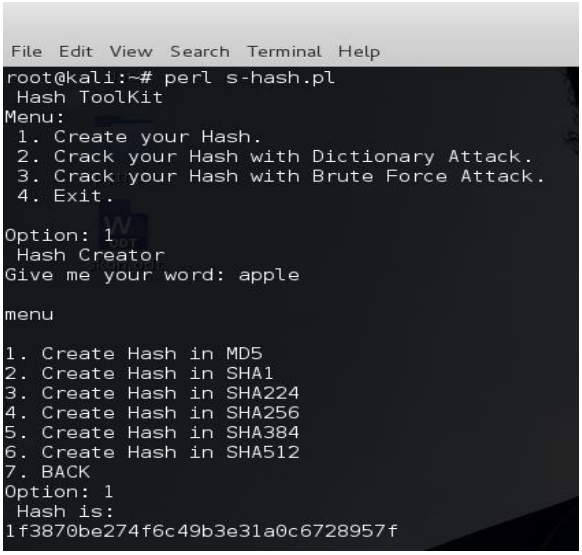

Fig. 2 Hash Tool Kit

3d8786fcb588c93348756c6429717dc6c374a 14f7029362281a3b21dc10250ddf0d057805 2749822eb08bc0dc1e68b0f

SHA512:
844d8779103b94c18f4aa4cc0c3b447405858
0a991fba85d3ca698a0bc9e52c5940feb7a65
a3a290e17e6b23ee943ecc4f73e7490327245
b4fe5d5efb590feb2

2. **Flow chart for creating of hash:**

In this flow chart the flow of data can be seen very easily. The string is taken by the user which is converted in the form of hash code. It provides seven steps in which the condition will be checked for which type of hashing is required by the user with the help of a simple if statement.

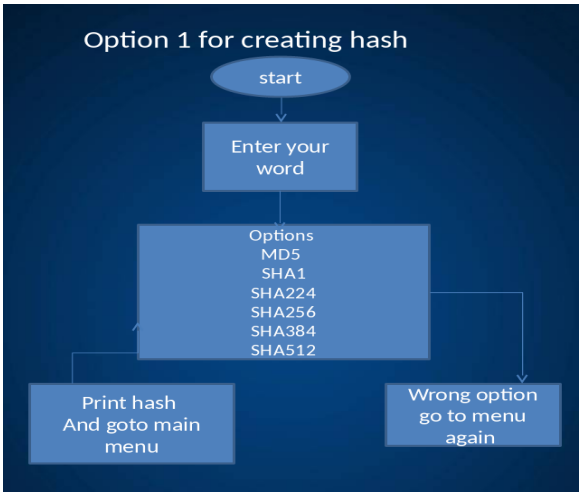

Fig. 3 Option- creating hash

Also, we can crack the hash using dictionary attack which takes hash code as input by the user and the location of dictionary. (Please Note: the dictionary is basically a password list).

3. **Flow chart of dictionary attack:**

This flow chart shows that the hash code is given by the user and then it is matched with the dictionary words one by one, in a loop which goes upto the end of the dictionary.

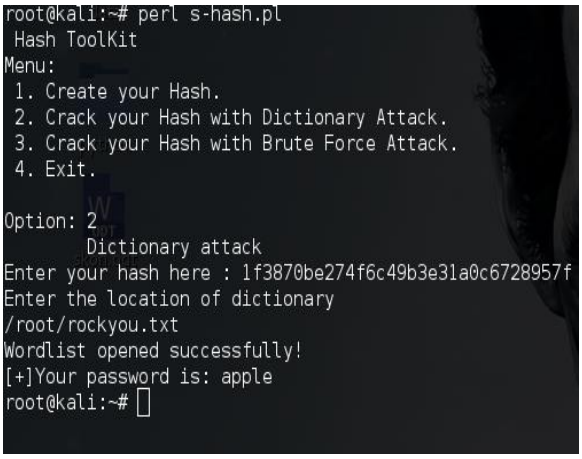

Fig. 4 Option- dictionary attack.

It stops when a collision for the hash is found. It takes a word from the dictionary, converts it into hash and then matches with the hash code given by the user.

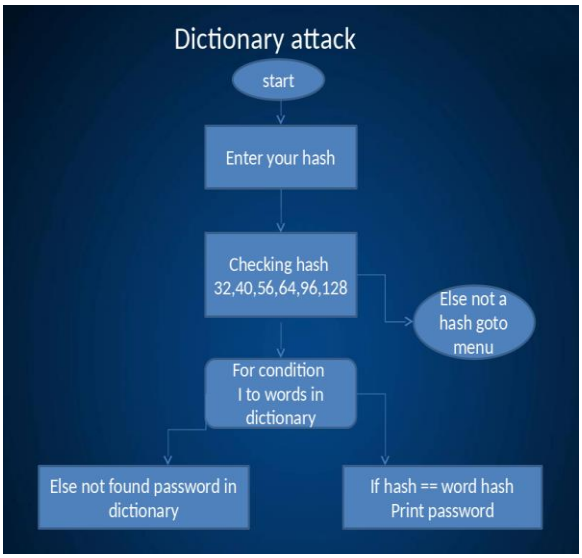

Fig. 5 Dictionary Attack

Thirdly, what we have is a brute-force attacking technique which will take an input of hash and then asks us for the type of characters it may contain.

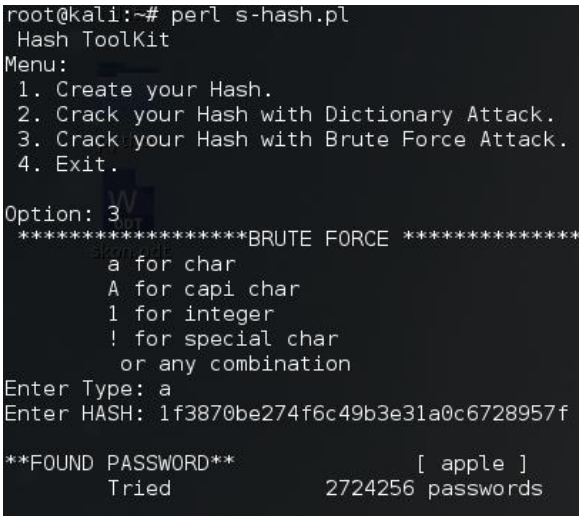

Fig. 6 Perl s- hash.

It is basically a hit and trial technique which is contains all the characters, numbers and special characters. If the password contains 5 characters, then the brute-force technique will try 26*26*26*26*26=11881379 keys of find the password zzzzz.

Flow of brute-force attacking technique

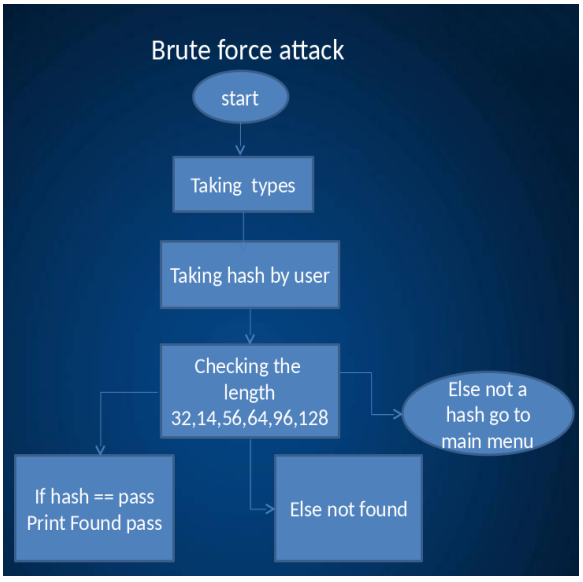

Fig. 7 Brute force Attack

4. Future Scope

In the future, the scope to reverse the hash or find the other way to crack the hash code or may be improve the algorithm of brute-force to crack faster than any other algorithm exists because hash is only a one way function and the super computer can do 38,360,000,000,000,000 keys per second right now. If we talk about normal computer then it will take 120 hours using cloud as a platform.

Conclusion

The work presents the focus on our concern on minimizing the brute-force attacking, for this several algorithms are made such as MD5**, SHA1, SHA224, SHA256, SHA384, SHA512**and after performing several attacks which encounters the part of collision. Final result has shon that out of all define algorithm it is possible to break all anyhow, so still a new revolution is still about to come in the era of cryptography hash function.

Conflict of interest

The author declares no conflict of interest.

References

1. Forouzan, B. A., & Mukhopadhyay, D. (2015). Cryptography and network security. New York, NY: Mc Graw Hill Education (India) Private Limited.
2. Dang, Q. H. (2015). Secure hash standard.
3. Barker, E. B. (1995). Secure hash standard (shs).
4. NIST.gov - Computer Security Division - Computer Security Resource Center.
5. Gallagher, P., & Director, A. (1995). Secure hash standard (shs). FIPS PUB, 180, 183.