**Tittle**

Estimation of time required for brute-force search  
attack on the password-based encryption

Ayodele Esho

Student ID: 201499108

Contents

[Abstract 3](#_Toc97129276)

[Introduction 3](#_Toc97129277)

[Password storage 3](#_Toc97129278)

[Password Algorithms 3](#_Toc97129279)

[Password length 4](#_Toc97129280)

[Methodology 4](#_Toc97129281)

[Conclusion 5](#_Toc97129282)

[References 5](#_Toc97129283)

# Abstract

  The first line of defence against unauthorized access to your computer and personal information is a password. Millions of services require a password for user protection. This doesn’t only mean digital services, it also means physical services such as; a bank, School login, Gmail and more. Passwords, should be complex and uncommon to prevent breaches. Almost 80 percent of data breachers, are the result of a poor or reused password. Poor passwords simply leads to easy access. This is why its important, users think clearly before setting a password for access that behold important information. In this report, I will be expressing the different ways to safeguard passwords (C.J.Fairfeild 2021).

# 

# Introduction

The security of your passwords can be improved in many different ways. One way, is Hashing. Hashing, is the act that converts passwords into an unreadable strings of characters. This means if a hacker has gained access to someone’s computer, instead of easily finding a set a of passwords they mind find a set of random characters and strings. Therefore, even if the hacker has the password, they will not be able to use it directly into a website. This makes it harder as they would have to personally decrypt each password. The success rate for this is uncommon. I recommend hashing passwords that hold important information (A.Greenberg 2016)

# 

# Password storage

An effective way to store all of the passwords that u have created is a password manager. A password manager, allows users to create and store passwords. All passwords are listed and would be protected. To access this, a master password would be created. This makes it easier to remember all of the key passwords that u have created. Password manager has many features such as, extensions that will autofill logins for you (A.Johnson 2021).

# 

# Password Algorithms

Encryption algorithm are divided into three classes. Symmetric, Asymmetric and hash functions, example of some of the algorithms are; DES, 3DES,AES,SHA. Each are a form of ciphers to encrypt data.

Data Encryption Standard (DES), is a symmetric-key block cipher used to encrypt and decrypt data in blocks sizes of 64 bits. 64 bites of plain text is inputted into DES and it returns 64 bits of ciphertext. A block cipher is used to take amount of data in bits and encrypts that data, making it into data unreadable for users to read (G.Geeks 2021).

Another algorithm similar is DES. 3DES (Triple Data Encryption Standard) is an updated version of DES. Once DES weaknesses were unrevealed 3DES was made. The difference between DES and 3DES, is that the key size is tripled to provide extra security, for total key length of 168 bits. This means that 3DES encrypts the inputted data three times (Techopedia 2011).

AES (Advanced Encryption Standard) algorithm was previously known as Rijndael is also a block cipher but converts individual blocks using keys of 128,192 and 256 bits. The ciphertext is formed by combining them once they are encrypted (Simplilearn 2022)

SHA (Secure hashing algorithm) is a hashing algorithm, that shortens data into a smaller version that cannot be read. This means that the server would only have to remember hashes instead of passwords. So if there is an attack the user will only gain access to hashes and will not be able to directly use them (E.Consultancy 2018)

# 

# Password length

The length of the password will determine the time needed for hackers to be able to encrypt it. As mentioned before it is important to use the mentioned maximum length for the password. By using the maximum length, and also adding special characters, capital letters / lower case letters makes it harder for the hackers to succeed. To improve this, you can also use salt (S.Gibbs 2016)

Salting is a procedure that adds a unique string characters to the addition of a password. For example a password could be “cat”. Salting would change this to “catp#2z”. This goes from a standard password to a more unique password. It is important to salt passwords because it safeguards it from being reversed engineered by hackers. As a result by using this, the hashing process is further complicated. Changing even the smallest aspect of a password can make it more complicated (T.MEZQUITA 2020)

Another is iteration count. An interaction occurs when a password has been hashed several times prior to being stored. A password can be iterated as many times as a user wants. Iterating a password improves its security as it makes it more harder for the password to be found in its original state. Nevertheless a password should not only be iterated it should also be salted and addition to a selection of numbers, capital/lower letters and special characters (S.Saubar 2018)

# 

# Methodology

Brute forcing passwords

I have now tested the time it would take to decrypt a standard predefined password “Mypassword”.

Graphical user interface

Description automatically generated with medium confidence

To brute force this password the time taken would take 1month. Having a standard plaintext password could lead to easy hacking. However I have found out that depending on the iteration count will determine how fast a password can be encrypted and decrypted.

Here the iteration count is set to 1024. This means the password will be hashed 1024 times.



The outcome is

Text

Description automatically generated with medium confidence

However if its changed to 5000



The outcome is

A black background with white text

Description automatically generated with medium confidence

Now if the salt was changed to



With the iteration count of 5000 the outcome becomes

Text

Description automatically generated

# 

# Conclusion

In conclusion it is important to create a complex password to defend against hackers. To do this I recommend using the hashing algorithm and also applying an iteration count and salting that password to safeguard you’re password as much as possible. Plaintext passwords is not a smart choice to use when creating a password. It can potentially be instant for a hacker to be able to decrypt your password depending on the text.

# References

Consulting, T. B. E., 2018. [Online]   
Available at: https://www.encryptionconsulting.com/education-center/what-is-sha/

Fairfeild, C., 2021. [Online]   
Available at: https://www.crn.com/news/channel-programs/logmein-poor-or-reused-passwords-responsible-for-83-percent-of-breaches

GeeksforGeeks, 2021. [Online]   
Available at: https://www.geeksforgeeks.org/data-encryption-standard-des-set-1/#:~:text=DES%20is%20a%20block%20cipher,and%20decryption%2C%20with%20minor%20differences

Gibbs, S., 2016. [Online]   
Available at: https://www.theguardian.com/technology/2016/dec/15/passwords-hacking-hashing-salting-sha-2

GREENBERG, A., 2016. [Online]   
Available at: https://www.wired.com/2016/06/hacker-lexicon-password-hashing/

Johnson, A., 2021. [Online]   
Available at: https://us.norton.com/internetsecurity-how-to-how-to-store-passwords.html

MEZQUITA, T., 2020. [Online]   
Available at: https://cyberhoot.com/cybrary/password-salting/

Sauber, S., 2018. [Online]   
Available at: https://scottsauber.com/2018/01/29/increasing-password-hashing-iterations-with-asp-net-core-identity/

Simplilearn, 2022. [Online]   
Available at: https://www.simplilearn.com/tutorials/cryptography-tutorial/aes-encryption

Techopedia, 2011. [Online]   
Available at: https://www.techopedia.com/definition/4144/triple-des

uOttawa, 2022. [Online]   
Available at: https://it.uottawa.ca/security/identity-authentication-theft#:~:text=Passwords%20provide%20the%20first%20line,all%20accounts%20on%20your%20computer