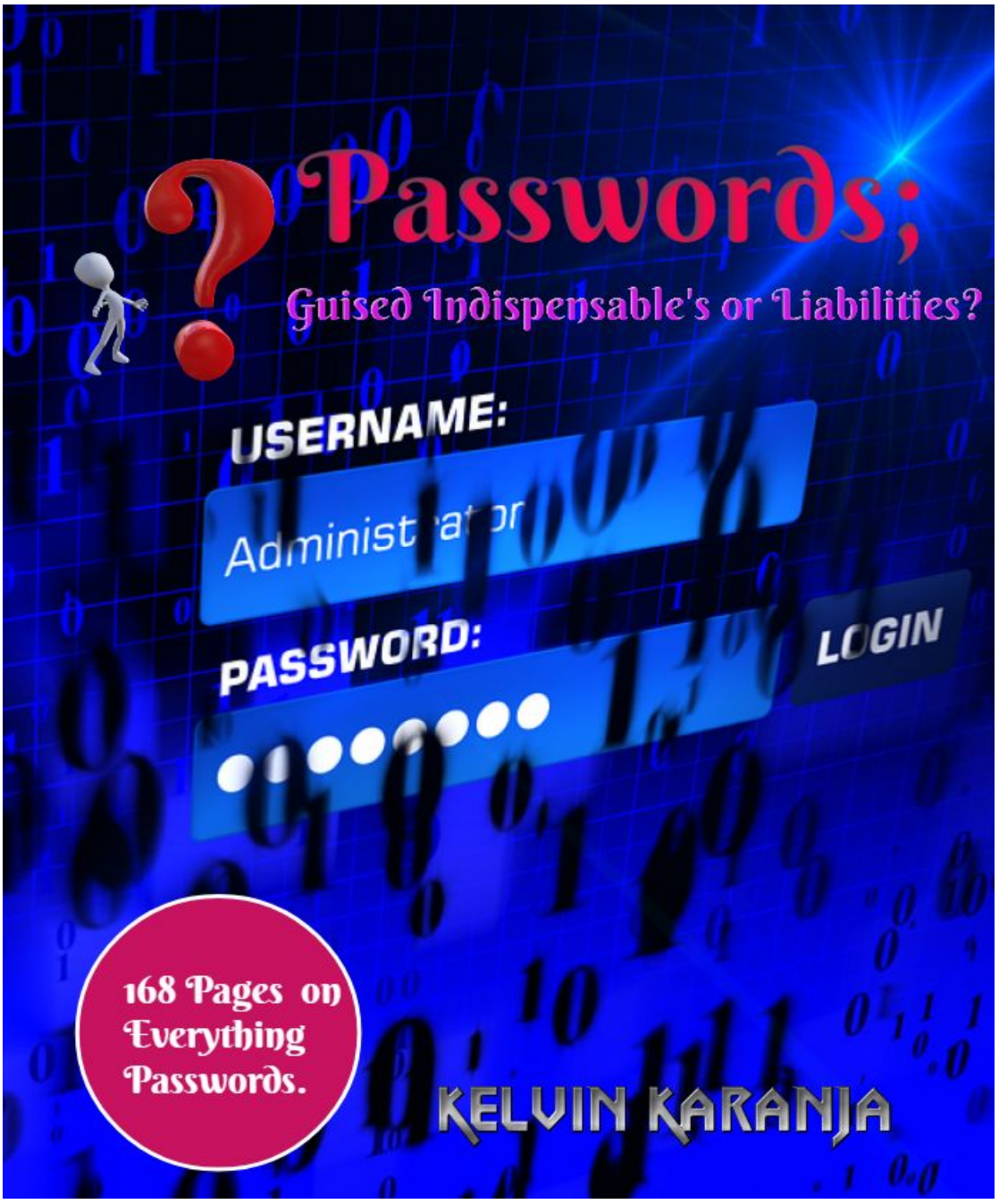

Passwords;
Guised Indispensable's or Liabilities?
USERNAME:
Administrator
PASSWORD:
LOGIN
168 Pages on Everything Passwords.
KELVIN KARANJA

CONTENTS

DISCLAIMER

Every attempt has been made to verify the information provided in this ebook.Every effort has been made to ensure the content of the ebook is as complete and accurate as possible.The author shall not be responsible for any errors,inaccuracies or omissions.

Follow Tech Bytes at Tech Bytes
for more tech news and information.

1] The Password

Foreword

The password is a phenomenal that has being in existence since the dawn of the web,in fact passphrases were used by ancient societies as a security measure,and this just goes to show the innovative nature of mankind throughout the ages.The password is a mechanism that provides a secure gateway or a loophole to ***CyberSecurity****;whichever way you look at it as there are two sides to a coin(****others say 3****).With the passing of time,it has become easier to compromise passwords and therefore there is no guarantee of security by having a password,it has to be a secure one and the online service you sign up for should also offer an environment that maintains that level of security and even improves the level of security rather than diluting it and making the user's vulnerable.Many of us have been culpable of numerous password flaws which compromises our Cyber Security.The statement 'Do anything and everything and even hire a Cyber Security team but if your password is weak,none of it will matter' says a great deal about the many underlying* ***issues*** *relating to Passwords other than say password length and to an extension the whole Cyber Security Challenges.The aim of this eBook is to try shed some light,understand and resolve most of these issues,because in the words of* ***Calvin Coolidge*** *(****30th US President****)....'We cannot do everything at once,but we can do something at once'.I believe that we'll definitely have made an important step forward.*

Why Use a Password?

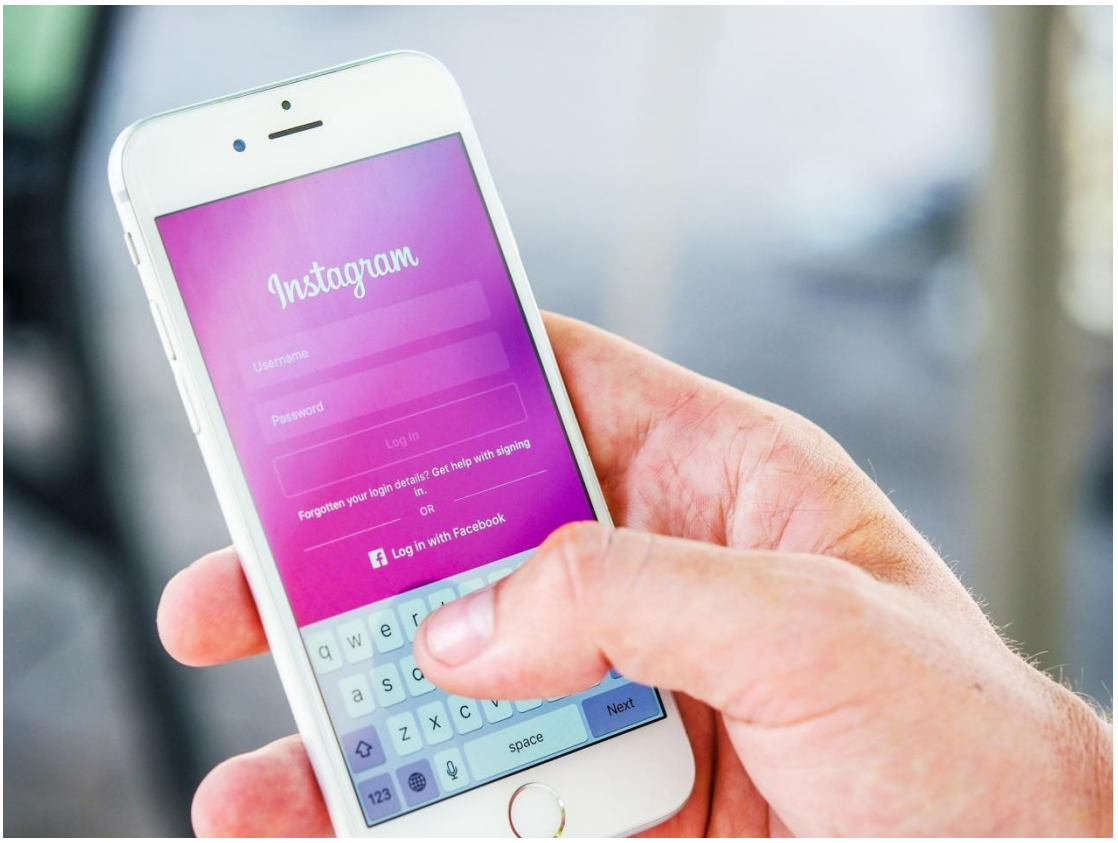
Everyone in the world who is tech savvy has used and interacted with a system that requires him to have and use a password.In fact due to phenomenons such as social networking,passwords have become something of a household name.A password is basically a word or string of characters used for user authentication to prove identity and access a resource or login to an online account.A typical computer user of the 21st Century has a Password(**s**) for various purposes:

I. Logging Into Accounts
II. Retrieving E-mails
III. Securing Devices e.g Phones,PCs,Tablets etc
IV. Databases
V. Websites
VI.Networks

There are many factors which have necessitated the use of the usage of the Password and it is hard to now imagine a world without them.Some of these factors might vary from one user to another,depending on many things-

I.Privacy and Protection of Private Data(the Main Reason)

II.Other Attacks



Passwords are nonetheless prone to physical security issues;from simple vulnerabilities like bystanders prying at what you're typing,shoulder surfing in crowded workstations to complex threats like video cameras and keyboard sniffers being mounted on your PC to spy on you and try stealing your password,writing your password on a sticky note and placing it on your monitor especially in the workplace is not a good practice either.All of these loopholes should be **sealed** at all costs to maintain the integrity of the Password.

Most computer systems have the option of showing or obscuring(**masking**) using * and • ,as the password is being typed.While,this is good practice other users want to be allowed to chose whether to obscure or not because obscuring will likely lead to stressing the user since he will not clearly see what he is typing which could result to selection of weak Passwords to avoid such struggle and stress.Weighing in on this issue,I believe that its better that the user is provided with the option of obscuring the password or not,depending on the preferences of the user.However,the user should exercise caution when doing this to ensure he does not fall prey to Physical Security Threats.

Password Security Mechanisms

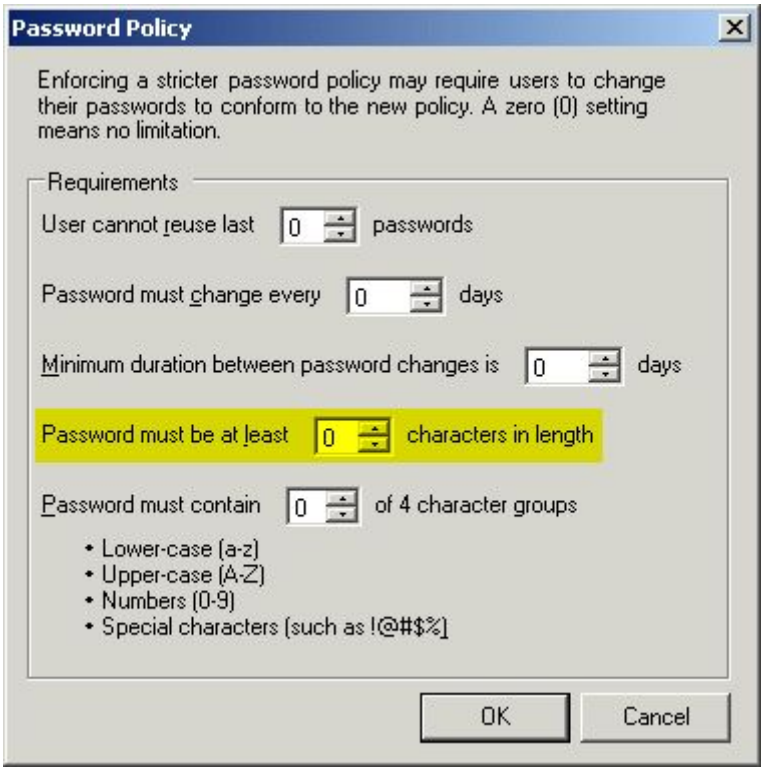
This is how computer systems have being designed to ensure that the passwords employed by the user,do serve their purpose which is providing security and that this is done in a manner that leaves little or no room for vulnerabilities.Some of these may fall into the bracket of **Password Policy**(**see chapter 4**).Most Computer systems are structured to do the following:

I. **Not displaying the password on the display screen as it is being typed.Often times obscuring or masking it using bullets(•) and asterisks(*).**
II. **Allowing passwords of adequate length.**
III. **Using two-factor authentication; such as sending a text message, an email or alert via a third-party app whenever a login attempt is made.**
IV. **Requiring characters from various character classes in a password such as "having at least one uppercase letter and also at least one number" Etc.**

However,despite having such measures aimed at providing an optimal level of security in place,some measures are considered by users as being too stringent and thus people tend to treat them with hostility and drag their feet at abiding by them and in the long run;the security level will have decreased.

Password Policy

A password policy is a set of rules or measures designed to ensure strong passwords are selected and used properly.The policy may apply to an institution or company.The **main** goal is to enhance computer security.The best password policy is one that helps users in creating secure passwords rather than try to strongarm and force users to do so.Using Technology and policy to make passwords stronger and secure might not necessary be enough because the weakest element in the system is the human element;some security players have even suggested that it would be better to do away with the human element by generating random passwords.However,although this is in theory a very good idea,practically it is impossible to completely do away with the human element even if you generate random passwords.You can sideline human beings from the generation but not from the use of these passwords;which presents other challenges.Selecting good passwords requires education;for both users and system administrators so that they can be able to educate and help the users.Complex Password requirements have usually been proven to be off-putting and according to many reports,over half of users queried abandon creation of online accounts,another around 55% **abandon a login page** because they have forgotten a password or incorrectly answered a security question.



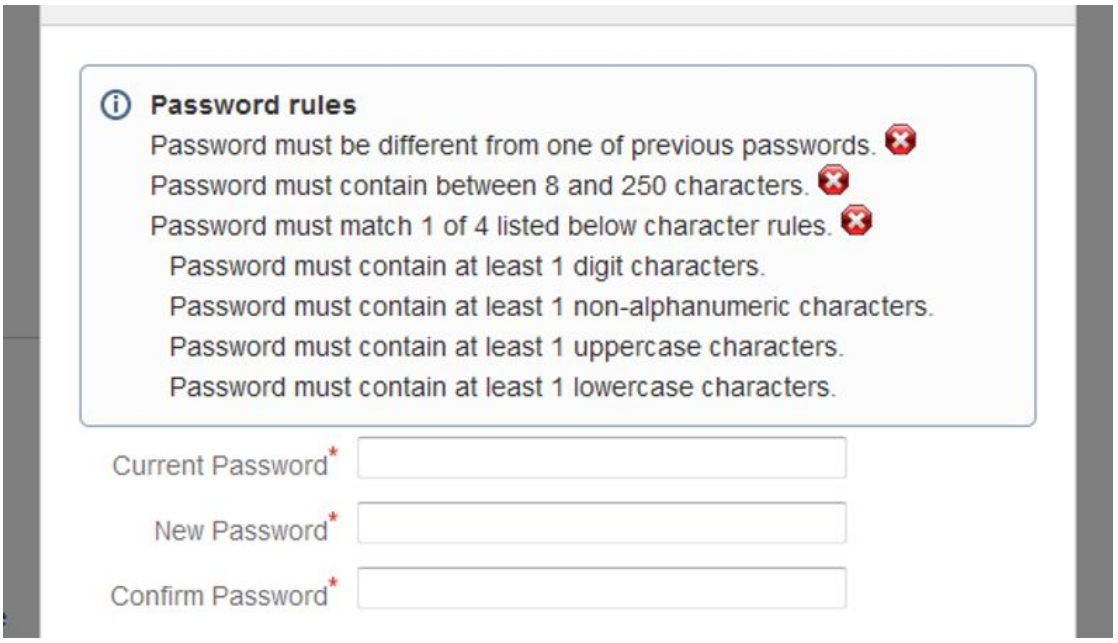
Aspects of Password Policy

The aspects of password policies may vary from organization to organization depending on their threat assessment of possible vulnerabilities;irrespective of these differences the bottom line is **security** to the firm,its resources and the users.

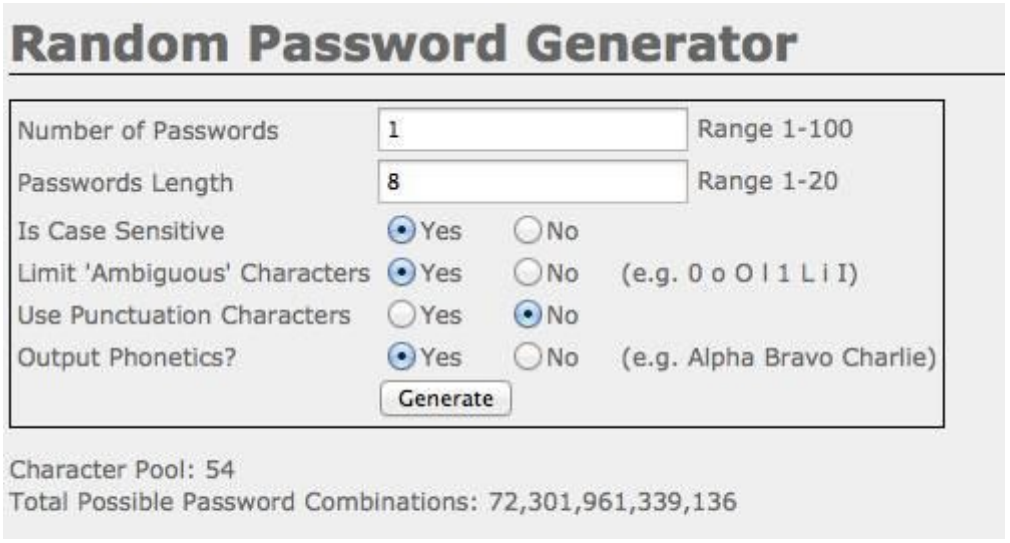
There are many things that a password policy ought to do;It should Assist users to choose strong passwords,prescribe the constitution of characters which passwords must contain,ensure the passwords are suited to the target users,provide recommendations for users with regard to the handling of their passwords,prompting users to change passwords which have been lost or compromised and ensuring that passwords don't last beyond a certain period of time among things.To achieve such goals it is important that a good password policy has a training program where users are trained on the basics of **password selection** and also train those who face challenges (**lost passwords**) or fail to follow the password policy(**inadequate passwords**),Rewarding users of strong passwords by reducing the rate of password change(to an extent asking users to change strong passwords is not a very wise thing to do because they may end up selecting a weaker password than the previous one).

1)Length and Details/Constitution

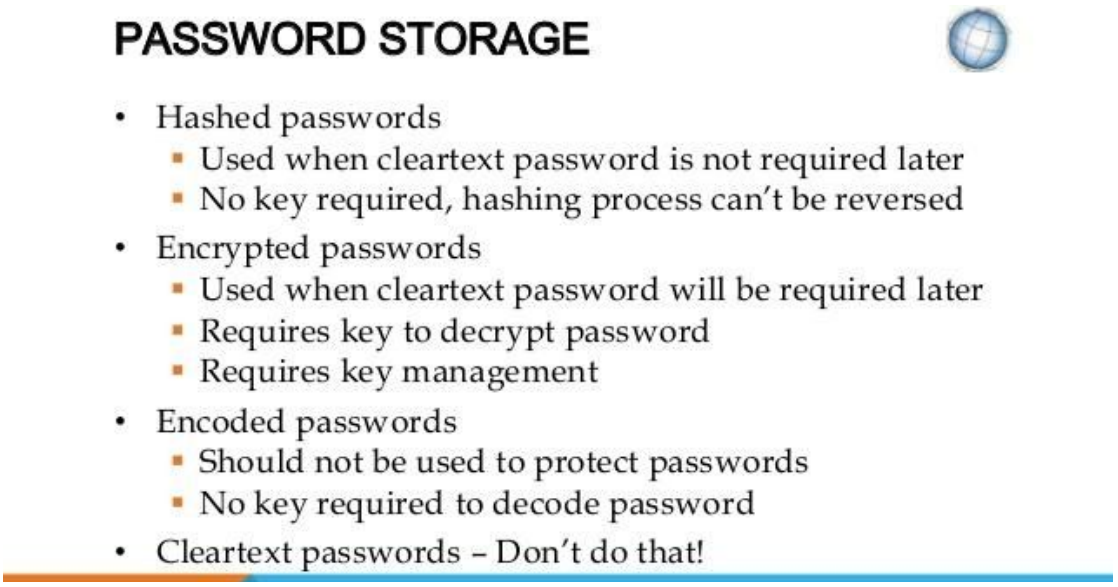
I. A minimum password length of 8 characters
II. Prohibition of words found in a password blacklist
III. Case Sensitivity - using of both uppercase and lower-case letters.
IV. Prohibition of words found in the user's personal information (e.g social media bio,statuses,profiles etc)
V. Prohibition of use of Company Name or an Abbreviation (Mnemonics)
VI. Inclusion of Special Symbols/Characters such as #,$,@
VII. Prohibition of passwords that match the format of mobile/telephone numbers,calendar dates,license plate numbers or other common numbers.
VIII. Reference to blacklists and using blacklists to block common,weak and easily guessed passwords.
IX.Password Expiration- The password becomes inactive after a certain period of time.



2)Random Generators - Here,the user will not come up with the password but systems following a certain set criteria(of a password policy) create the password for him.The Random Generators could also let the user to select a password from a limited number of choices.

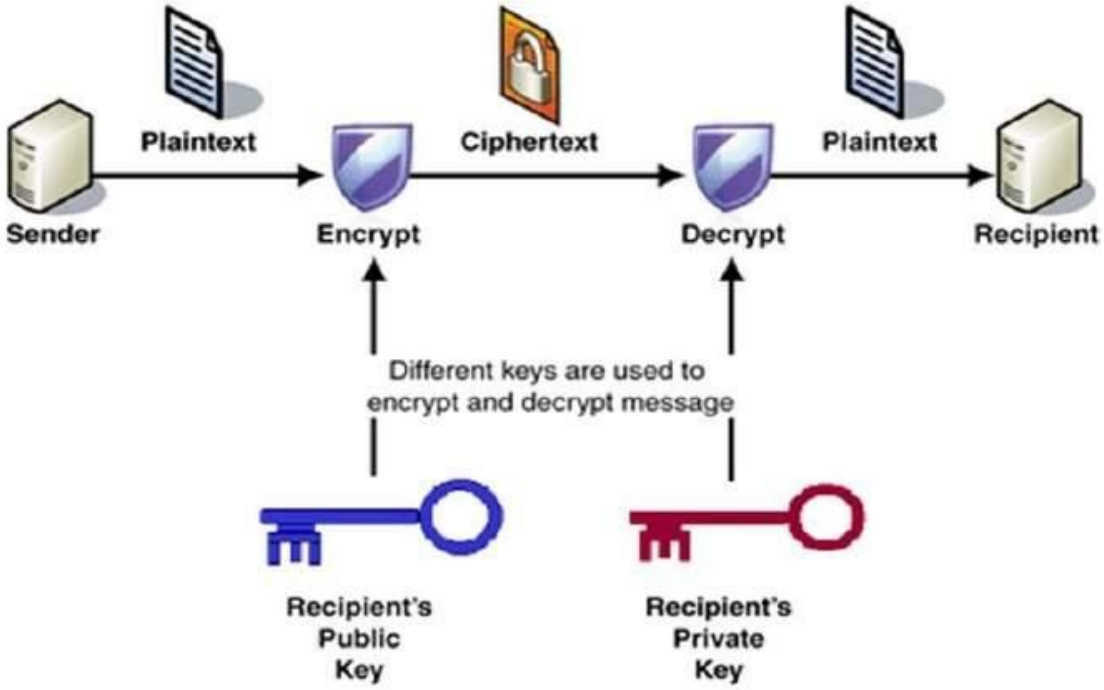


Storage Of Passwords



Back in the early infancy stages of Computer Science,websites stored user passwords as **plain text**.Password cracking was not as big as it is today,the protection and security mechanisms were also designed to deal with such lower-level threats.In order to verify that the user sent in the correct password a copy of the passwords were stored in a file somewhere, and was used to check the user's submitted password against the list.As time went by,attackers devised methods of accessing the database files(Through Deception like politely asking for permission to access such files)that had passwords.The security players needed to do something different,and quickly.Fast forward some time later,Hashing was born.A hash function is a piece of code that takes a piece of information and scrambles it up mathematically into a fixed-length piece of gibberish.This is called 'hashing' the data.What's so cool and unique about them is that **they only go in one direction;they are irreversible**.It's fairly easy to take a piece of information and figure out its unique hash but quite tasking to take a hash and find a piece of information that generates it.An attacker,can use commercially available tools to have a go at guessing the Passwords.Such tools work by hashing possible passwords and comparing the result of each guess to actual password hashes.If a match pops up they definitely know that their guess is the actual password.Hashes have some really useful properties for password applications.Now,instead of storing the password,you store the hashes of the passwords.When you want to verify a password,you hash it, delete the original, and check it against the list of hashes.Hash functions all deliver the same results, so you can still verify they submitted the correct passwords.Crucially,the actual plaintext passwords are never stored on the server.So,when hackers gain access to the server,they can't steal any passwords – only hashes.The hackers response to this was to spend a lot of time and come up with really clever ways to reverse hashes.There are various forms in which Passwords on a computer system can be stored.Oftentimes they are stored as plaintext,against which to compare user log on attempts.These ones are not secure since if an attacker gains access to such an internal password store,all passwords and by obviously all

user accounts will be compromised.In fact storing passwords as plaintext is one of the biggest mistakes any online service can ever make.



Cryptanalysis is a science of data encryption and is mostly used by computer scientists and cryptanalysts to recover Passwords from data that has been stored in or transmitted by a computer system.Therefore,more secure computer systems store each password in a cryptographically protected form making it a tall order for someone who gains internal access to the system getting the password,whilst still leaving room for user validation.Other computer systems have gone a notch higher and don't store passwords at all,which is quite good.They store one-way derivation like an advanced hash or a polynomial modulus.(The salt must be saved for each user and is usually stored beside the username and password hash, so the information is available during each user login.Salt is rarely kept apart from the hash.Even when known,its virtue lies in its uniqueness,which defeats pre-computation of results.)

Cryptanalysis is the science and study of methods for breaking encryption schemes. A cryptographic system is said to be **breakable** if plaintext can be obtained from ciphertext without knowing the key, or if the key can be deduced from observed ciphertexts and corresponding plaintext information. There are three main lines of attack:

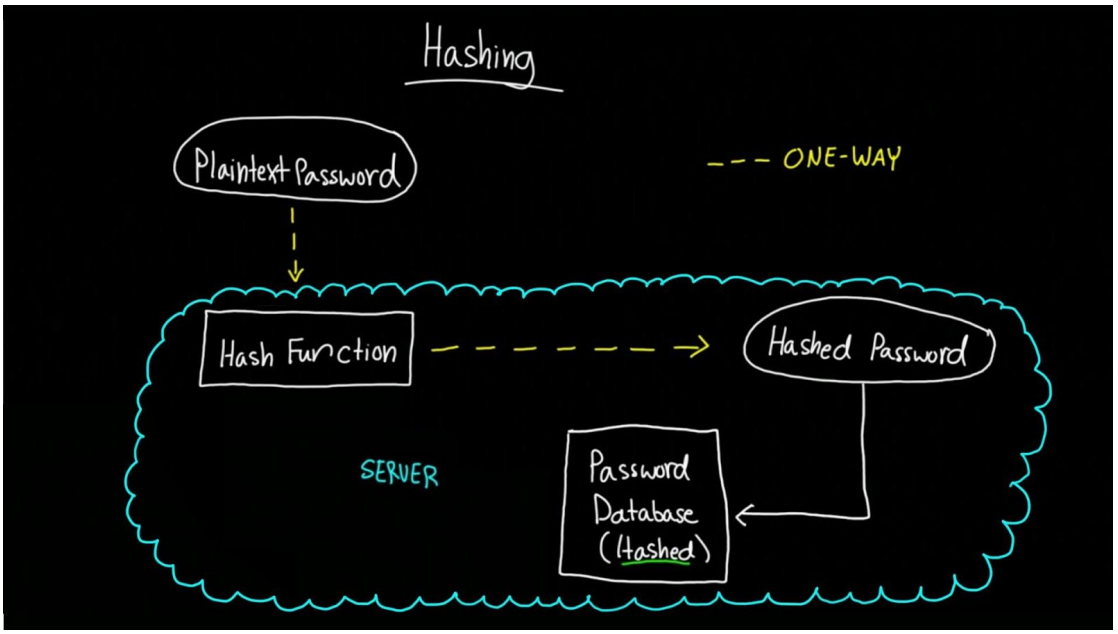
- **Ciphertext-only attack**. The cryptanalyst has several pieces of ciphertext that were all encrypted using the same encryption algorithm. The goal is to recover as many plaintexts as possible or, better yet, to deduce the key(s) used for encryption and/or decryption.
- **Known-plaintext attack**. The cryptanalyst is able to obtain several plaintext-ciphertext pairs. The goal is to deduce the key(s) used for encryption and/or decryption, so that any further messages encrypted with the same key(s) can be decrypted.
- **Chosen-plaintext attack**. The cryptanalyst can choose plaintexts and obtain the corresponding ciphertexts. The goal is to choose the plaintexts such that the resulting plaintext-ciphertext pairs make it as easy as possible to deduce the encryption and/or decryption key(s).

User details are stored in the following way and usually separated from each other using colons:
1)The Username(on the left)
2)The Number Identifier of the hashing algorithm used (on the right after the colon)
3)The Salt(after the Hashing algorithm number identifier)
4)The very long hash
5)Details about when the password was last modified,how old it is,when the account will expire among other details.

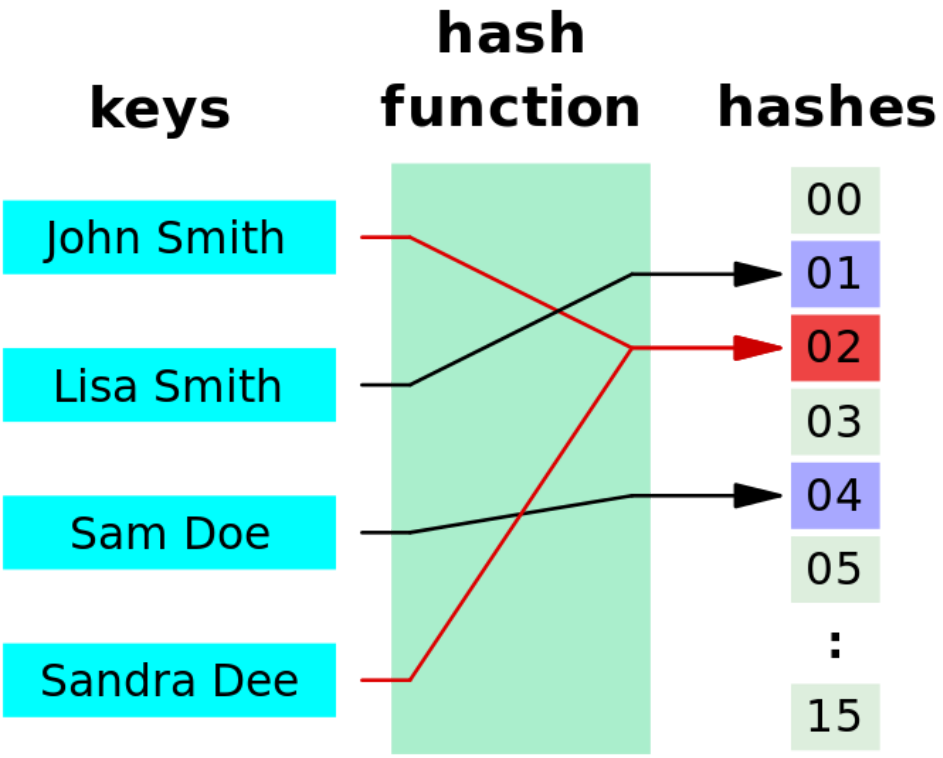
Example of a Stored Password:

testuser:$6$2lvEhpi5$KnVn901C4Y23zsVZK1/UILbTkKIU6hA6V/0pXZ3yQU.EhVxQS6/KjaO2bH7VZOOr/DTGko9LjqWOi7CrU.Ggy0:15569:0:99999:7:::

The line is broken up by colons—first comes the username,then the lengthy password section,then data about when the password was last changed,how old it is,when the account expires,and more.



Hash- Hashing is the transformation of a string of characters into a usually shorter-fixed length value or key that represents the original string.Roger Needham is credited for inventing the common approach of storing only a hashed form of the plaintext Password.This system allows the user to type in a Password on such a system,the password handling software then runs through a cryptographic hash algorithm,and if the hash value generated from the user's entry matches the hash stored in the password database, the user is then permitted access.The hash value is created by applying a cryptographic hash function to a string consisting of the submitted password and,in many implementations,another value known as a salt.A salt prevents attackers from easily building a list of hash value or simply guessing them.Main storage methods for passwords are text,hashed and salted and reverse encryption.If an attacker gains access to the Password file,it is stored as a plain text and no much work for him such as cracking is necessary because its plain text and the password is crystal clear.If it is hashed but not salted,then it is vulnerable to rainbow table attacks(**more efficient than Cracking**).If it is reversibly encrypted,the attacker needs only get the decryption key and the file...If he does get them,nothing can save you now because,no cracking is necessary.However,if he fails to get the key cracking is not possible.



Rainbow Table Attacks- A precomputed table for reversing cryptographic hash functions,usually for cracking password hashes.Tables are usually used in recovering a plaintext password up to a certain length consisting of a limited set of characters.

An attacker,can use available tools-especially commercially available ones to have a go at guessing the Passwords.Such tools work by hashing possible passwords and comparing the result of each guess to actual password hashes.If a match pops up they definitely know that their guess is the actual password.

Authentication of Passwords

When logging into your online account and you type your password,how is the password retrieved from the server and verified? There are a few methods such as Cryptographic Protection which uses Transport Layer Security (**TLS**),previously known as **SSL**.It is a feature built into browsers and the TSL/SSL feature is shown by a closed lock icon displayed at the beginning of the address bar(top left).Another mode of verification is the hash-based method;A client ought to prove to a Server that they know what the shared secret(the password) is and the Server then has to obtain the shared secret from its stored form.The shared secret during remote authentication in most Operating Systems like **Unix-type** systems is the Hashed form;in case of attack,the attacker will only need the hash rather than the original password to authenticate.