



# EECS 3482

## Introduction to Computer Security

---

Assignment Project Exam Help

<https://powcoder.com>  
**Password Cracking**

Add WeChat powcoder

# TIME IT TAKES A HACKER TO BRUTE FORCE YOUR PASSWORD

Number of characters	Number only	Lower case letters	Upper and lowercase letters	Numbers, upper and lowercase letters	Numbers, upper and lowercase letters, symbols
4	Instantly	Instantly	Instantly	Instantly	Instantly
5	Instantly	Instantly	Instantly	Instantly	Instantly
6	Instantly	Instantly	Instantly	1 sec	5 sec
7	Instantly	Instantly	25 secs	1 min	6 min
8	Instantly	5 secs	22 mins	1 hour	8 hour
9	Instantly	2 mins	13 hours	3 days	3 weeks
10	Instantly	58 mins	1 month	7 months	5 years
11	2 secs	1 day	5 years	41 years	400 years
12	25 secs	3 weeks	300 years	2k years	34k years
13	4 mins	1 year	16k years	100k years	2m years
14	41 mins	51 years	800k years	9m years	200m years
15	6 hours	1k years	43m years	600m years	15bn years
16	2 days	34k years	2bn years	37bn years	1tn years
17	2 weeks	800k years	100 bn years	2tn years	93tn years
18	9 months	23m years	6tn years	100tn years	7qd years

Go to [howsecureismypassword.net](https://howsecureismypassword.net) for more information



**BEAUCERON**  
SECURITY

# Introduction

- **Password** – a secret word/string of characters used to authenticate a user into a system
  - ◆ critical (often only) defense against intruders
  - ◆ ~~critical (often only) defense against intruders~~ easy to remember, hard to 'crack'  
<https://powcoder.com>
  - ◆ Google (2013) released a **list of common password types which are insecure** as they are too easy to guess / get off social media
    - name of a pet, child, family member, spouse
    - names of birthplaces, favorite sports teams
    - birthdays, anniversary dates
  - ◆ **overly complex passwords are as dangerous as very simple ones**
    - the user likely to write it down or to reuse it

In 2019, the UK's **National Cyber Security Centre (NCSC)** has released a list of the 100,000 most common passwords to appear in breached accounts.

Using data from [Have I Been Pwned](#) (HIBP), a website that allows users to check if their email addresses or passwords have appeared in a known data breach, the United Kingdom's [National Cyber Security Centre \(NCSC\)](#) [has found](#) that 23.2 million user accounts worldwide were “secured” with ‘123456’.

Most used in total	Names	Premier League football teams	Musicians	Fictional characters
--------------------	-------	-------------------------------	-----------	----------------------

123456 (23.2m)

ashley (432,276)

liverpool (280,723) blink182 (285,706)

superman (333,139)

123456789 (7.7m)

michael (425,291)

chelsea (288,697) 50cent (291,153)

naruto (242,749)

qwerty (3.8m)

daniel (368,227)

arsenal (179,095) eminem (167,983)

tigger (237,290\_)

password (3.6m)

jessica (324,125)

manutd (59,440) metallica (140,841)

pokemon (226,947)

111111 (3.1m)

charlie (308,939)

everton (46,619) slipknot (140,833)

batman (203,116)

Assignment Project Exam Help

<https://powcoder.com>

Add WeChat powcoder



[Home](#)[Notify me](#)[Domain search](#)[Who's been pwned](#)[Passwords](#)[API](#)[About](#)[Donate !\[\]\(17413706fd4997a1a4bdf85c6864eee1\_img.jpg\)](#)

# ';--have i been pwned?

Check if you have an account that has been compromised in a data breach

Assignment Project Exam Help

<https://powcoder.com>

Add WeChat powcoder

## Pwned Passwords

Pwned Passwords are 555,278,657 real world passwords previously exposed in data breaches. This exposure makes them unsuitable for ongoing use as they're at much greater risk of being used to take over other accounts. They're searchable online below as well as being downloadable for use in other online systems. [Read more about how HIBP protects the privacy of searched passwords.](#)

Oh no — pwned!

This password has been seen 23,547,453 times before

This password has previously appeared in a data breach and should never be used. If you've ever used it anywhere before, change it!

<https://haveibeenpwned.com/Passwords>

# Introduction (cont.)

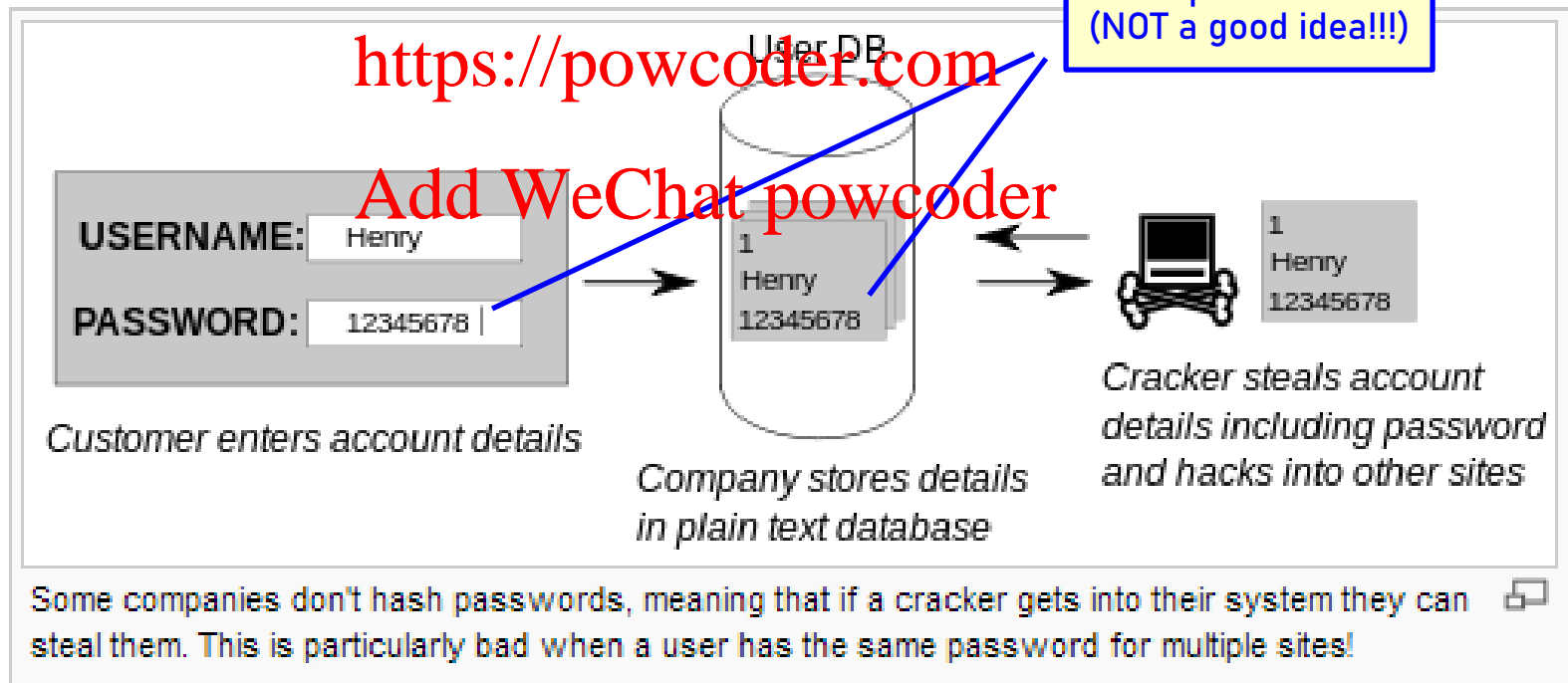
## How are passwords stored in a computer/system???

Assignment Project Exam Help

password is stored  
in plain-text  
(NOT a good idea!!!)

<https://powcoder.com>

Add WeChat powcoder



# Introduction (cont.)

- **Passwords in a System**

- ◆ in most systems, passwords are stored in a protected (hash) form  $\Rightarrow$  snooper that gains internal access to system cannot easily retrieve/steal passwords

Assignment Project Exam Help

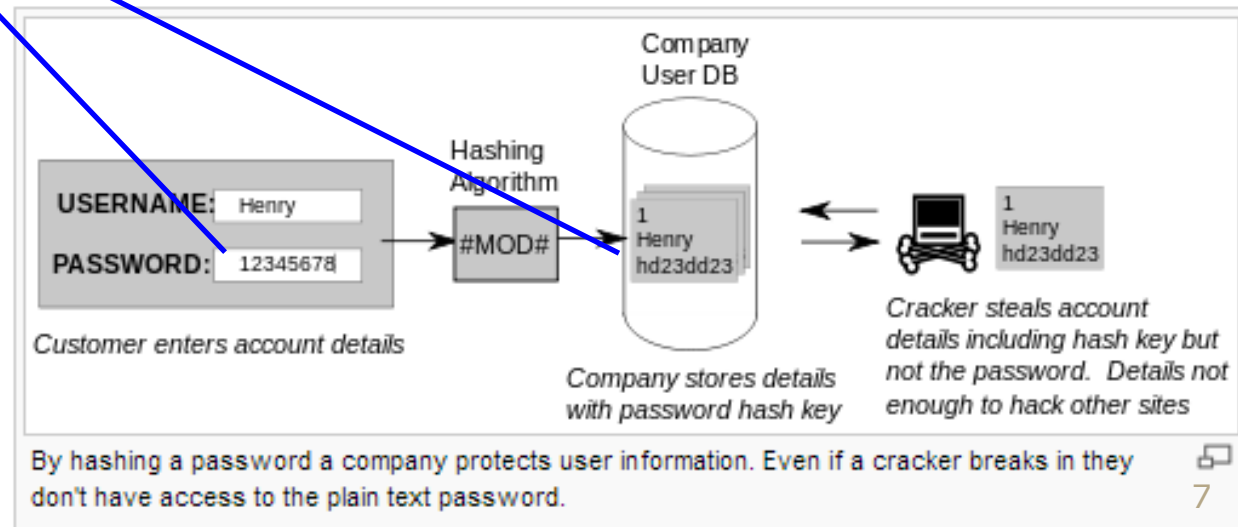
- every time a user logs in, password handling software runs the hash algorithm

password is stored in a 'hashed form'

<https://powcoder.com>

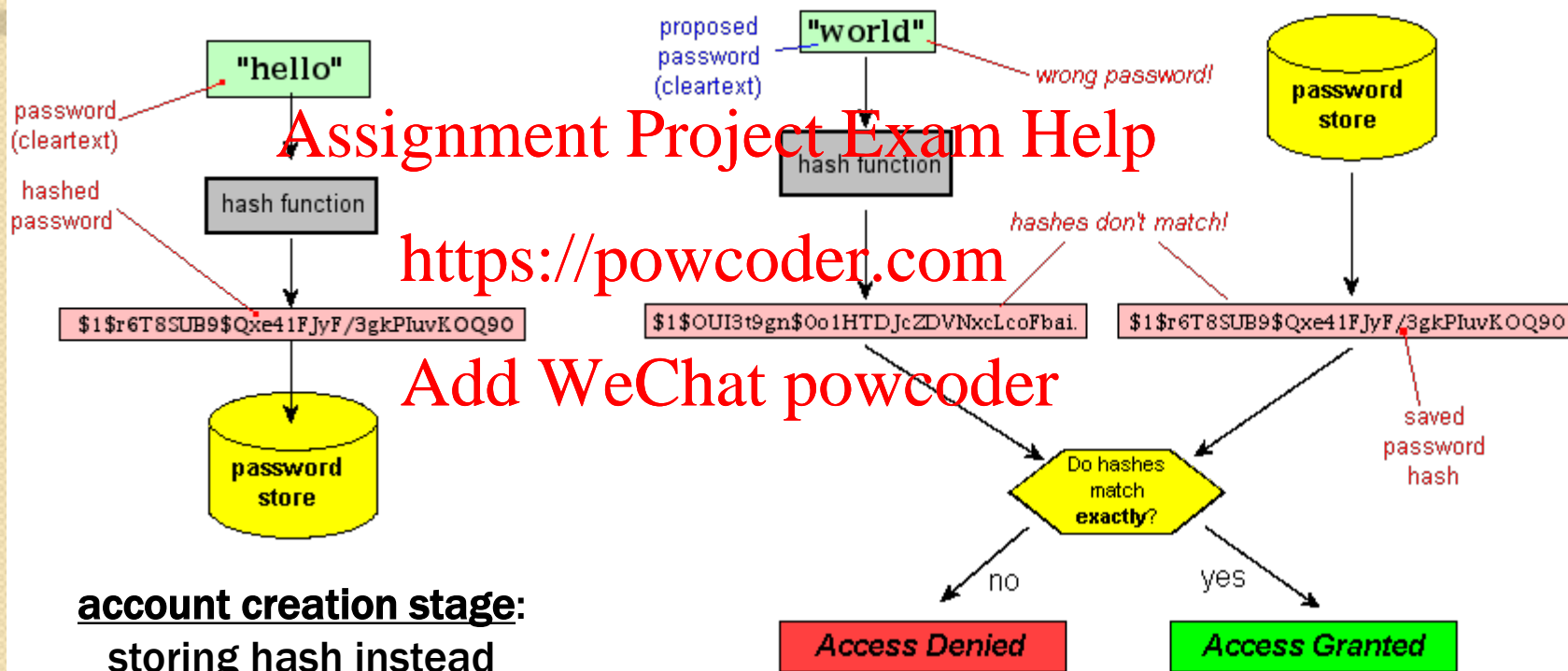
- if (new hash = stored hash), access is granted

Add WeChat powcoder



# Introduction (cont.)

## Example: Password hashes



**account creation stage:**  
storing hash instead  
of password

**logging into an existing account:**  
testing a password against stored hash



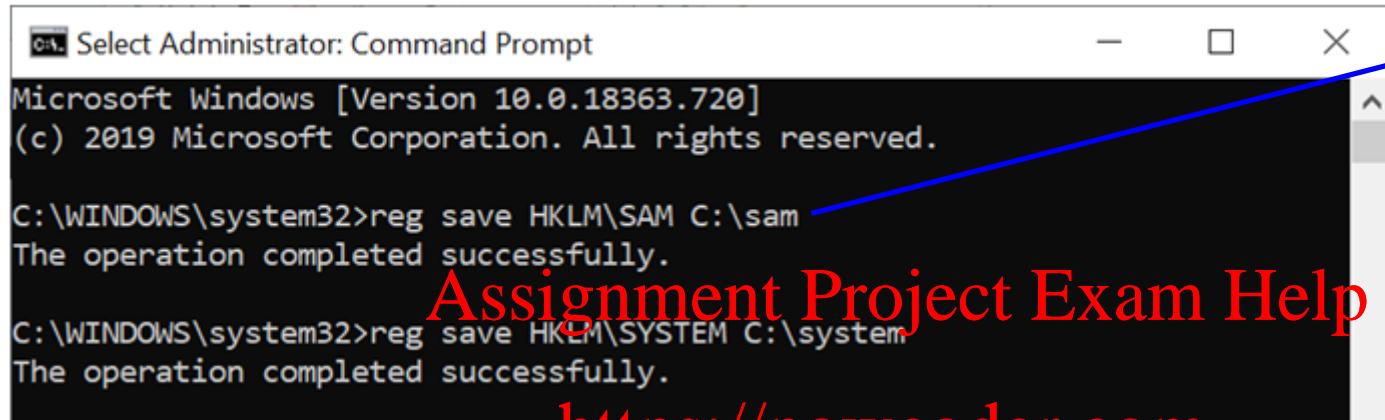
# Introduction (cont.)

- **Password Management in Windows** – password hashes are stored in **Security Account Manager (SAM) file**
  - ◆ stored in C:\Windows\System32\config or HKEY\_LOCAL\_MACHINE\SAM registry
  - cannot be accessed on normal boot up of the OS (i.e., while computer running) – file used by OS
- **Accessing SAM File in Windows** – requires administrative privileges to be copied / dumped

Just open the Command Prompt as Administrator, and then run the following commands:

```
reg save HKLM\SAM C:\sam  
reg save HKLM\SYSTEM C:\system
```

# Introduction (cont.)



```
Microsoft Windows [Version 10.0.18363.720]
(c) 2019 Microsoft Corporation. All rights reserved.

C:\WINDOWS\system32>reg save HKLM\SAM C:\sam
The operation completed successfully.

C:\WINDOWS\system32>reg save HKLM\SYSTEM C:\system
The operation completed successfully.
```

Copy of SAM file is now stored on C drive as a file named 'sam'. However, this file is encrypted using SysKey!!! So, a dump of SYSTEM hive/file is also needed!

Assignment Project Exam Help

<https://powcoder.com>

Add WeChat powcoder

The SAM file is encrypted with the **SysKey** which is stored in %SystemRoot%\system32\config\system file.

During the boot-time of Windows the hashes from the SAM file get decrypted using the SysKey and these hashes are then loaded to the registry and used for authentication purpose.

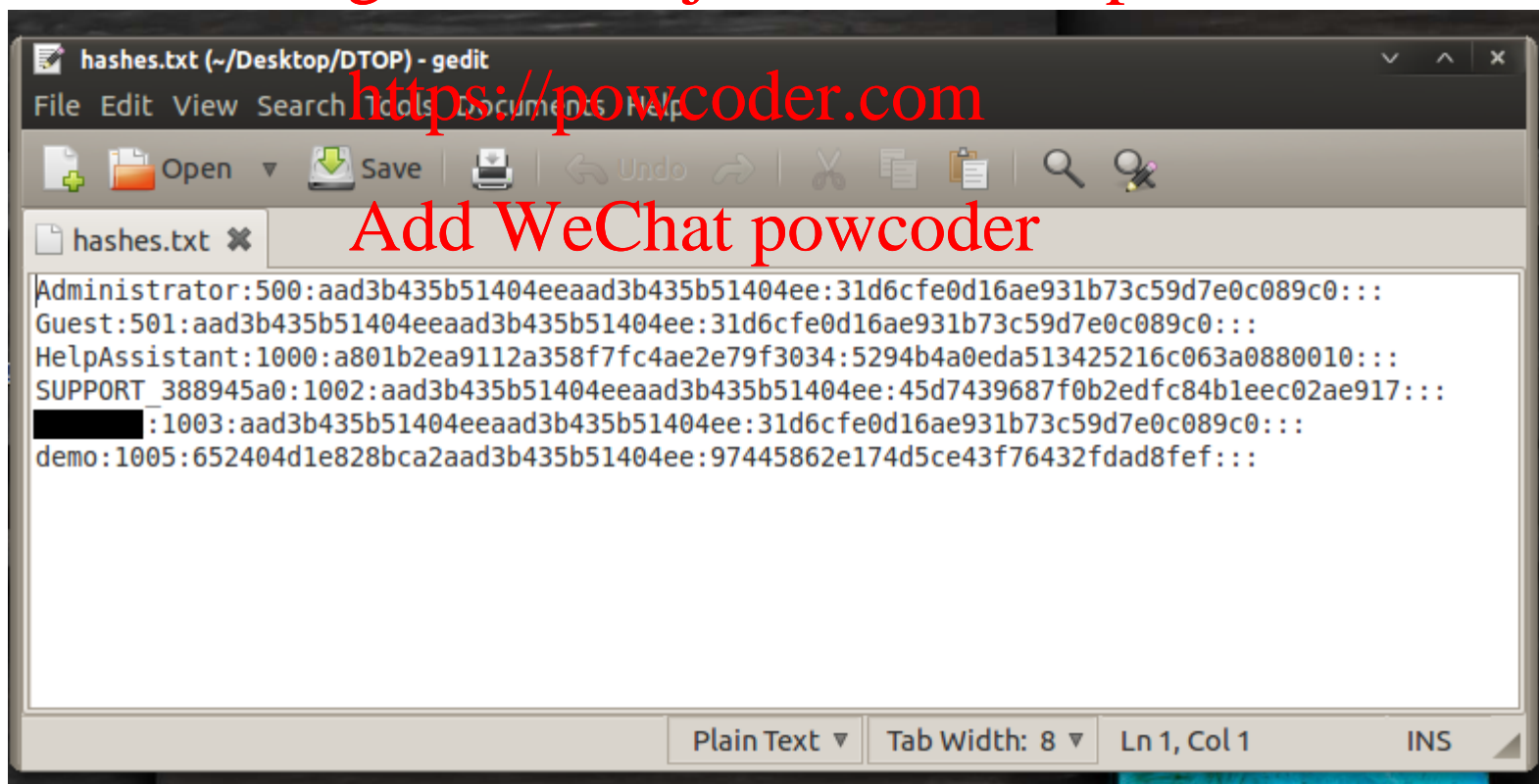
Both system and SAM files are unavailable (i.e., locked by kernel) during Windows' runtime.

Tools like **samdump2** can be used to dump password hashes from sam file. Tools like **Cryptool** or **John the Ripper** can be used to 'crack' hashed passwords extracted from sam file ...

# Introduction (cont.)

- **Accessing Hash File in Unix** – text file: `/etc/shadow` (`/etc/passwd`)
  - ◆ readable by system administrator (root) only

Assignment Project Exam Help



hashes.txt (~/Desktop/DTOP) - gedit

File Edit View Search Tools Documents Help

Open Save Undo

hashes.txt

```
Administrator:500:aad3b435b51404eeaad3b435b51404ee:31d6cfe0d16ae931b73c59d7e0c089c0:::  
Guest:501:aad3b435b51404eeaad3b435b51404ee:31d6cfe0d16ae931b73c59d7e0c089c0:::  
HelpAssistant:1000:a801b2ea9112a358f7fc4ae2e79f3034:5294b4a0eda513425216c063a0880010:::  
SUPPORT_388945a0:1002:aad3b435b51404eeaad3b435b51404ee:45d7439687f0b2edfc84b1eec02ae917:::  
[REDACTED]:1003:aad3b435b51404eeaad3b435b51404ee:31d6cfe0d16ae931b73c59d7e0c089c0:::  
demo:1005:652404d1e828bca2aad3b435b51404ee:97445862e174d5ce43f76432fdad8fef:::
```

Plain Text Tab Width: 8 Ln 1, Col 1 INS


<https://powcoder.com>

Add WeChat powcoder

# Introduction (cont.)

## Example: passwd vs. shadow

cd /etc

 indigo.cs.yorku.ca - PuTTY

```
indigo 28 % ls -l passwd
-rw-r--r-- 1 root root 1266 May 16 16:20 passwd
```

```
indigo 29 % ls -l shadow
-rw----- 1 root root 70669 Mar 7 22:50 shadow
```

When any user is created in Linux it affects 4 files

- /etc/passwd
- /etc/group
- /etc/shadow
- /etc/gshadow

/etc/passwd file is essentially the *user account database* in which Linux stores valid accounts and related information about these accounts; typically has file system permissions that allow it to be readable by all users of the system

/etc/shadow file contains hashed passwords and bookkeeping information; accessible only by the super user

# Introduction (cont.)

## Example: entry in etc/shadow

vivek:\$1\$fnfffc\$PgteyHdicpGOfffXX4ow#5:13064:0:99999:7::

1 2 3 4 5 6

Annotations:  
- Red circles around \$1\$, \$fnfffc\$, and \$PgteyHdicpGOfffXX4ow#5:  
- Blue box labeled "salt" under \$fnfffc\$  
- Blue box labeled "hashed password" under \$PgteyHdicpGOfffXX4ow#5:  
- Blue arrows pointing from the boxes to the list of hashing algorithms.

ID of used  
hashing  
algorithm

1. \$1\$ is MD5
2. \$2a\$ is Blowfish
3. \$2y\$ is Blowfish
4. \$5\$ is SHA-256
5. \$6\$ is SHA-512

- <https://powcoder.com>
- Add WeChat powcoder
1. **Username** : It is your login name.
  2. **Password** : It is your encrypted password. The password should be minimum 6-8 characters long including special characters/digits and more.
  3. **Last password change (lastchanged)** : Days since Jan 1, 1970 that password was last changed
  4. **Minimum** : The minimum number of days required between password changes i.e. the number of days left before the user is allowed to change his/her password
  5. **Maximum** : The maximum number of days the password is valid (after that user is forced to change his/her password)
  6. **Warn** : The number of days before password is to expire that user is warned that his/her password must be changed
  7. **Inactive** : The number of days after password expires that account is disabled
  8. **Expire** : days since Jan 1, 1970 that account is disabled i.e. an absolute date specifying when the login may no longer be used.

Typically  
set to 0.



# Introduction (cont.)

## Example: 'encrypted' password

```
$6$5H0QpwprRiJQR19Y$bXG0h7dIfOWpUb/Tuqr7yQVCqL3UkrJns9.7msfvMg4Z0/PsFC5Tbt32P
| 1 | ----- 2 ----- | ----- 3 -----
```

1. Hash Algorithm: This field denotes the hashing algorithm used to create the hashed password. The digit 6 describes that, SHA-512 algorithm is used, in this case. Some more of them are enlisted below:

```
-----
| 1 | MD5 |
-----
| 2 | Blowfish |
-----
| 2a | eksBlowfish |
-----
| 5 | SHA-256 |
-----
| 6 | SHA-512 |
-----
```

2. Salt Value: Salt values are used to make the hash value stronger. These are the random type of data that is used to combine with the original password and then the hashed version of that is used as the encrypted password.

3. Password: This field stores the hashed version of the combination of original password and salt value.

Assignment Project Exam Help

<https://powcoder.com>

Add WeChat powcoder

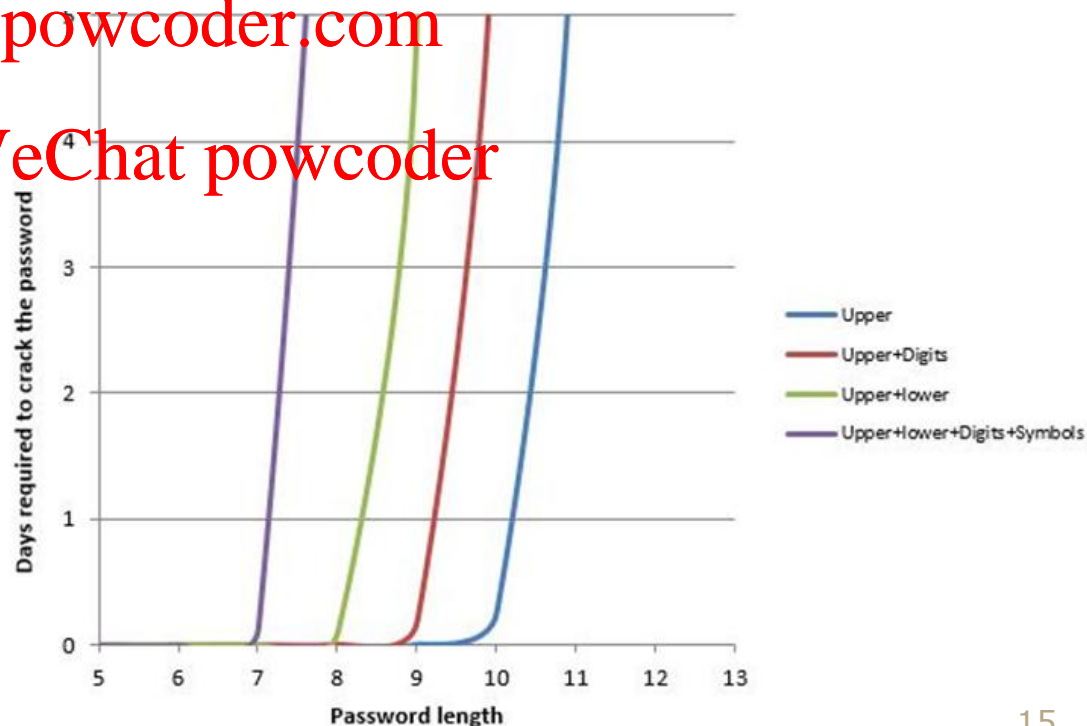
# Password Cracking

- **Password Cracking (Guessing)** – a method of gaining unauthorized access to a computer system by trying different passwords

Assignment Project Exam Help  
cracking difficulty – size of password space

<https://powcoder.com>

Add WeChat powcoder



# Password Cracking (cont.)

- **Online vs. Offline Password Cracking**

- ◆ **online cracking**

- try every password at the login prompt in real time

➤ very slow!

8-character password of 76 possible characters (upper & lower case, digits, common symbols) =  $1.1 \times 10^{15}$  possibilities

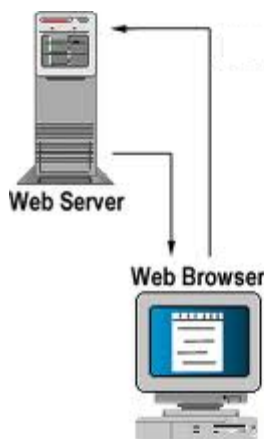
2 to 3 passwords a second  $\Rightarrow$  5,878,324 years to guess a password

- **extremely noisy!**

most systems block the victim account after several failed login attempts

- ◆ **off-line cracking**

- assumes the possession of passwd/hash file



Assignment Project Exam Help

<https://powcoder.com>

Add WeChat powcoder

# Password Cracking (cont.)

- **Brute-Force Password Cracking** – aka exhaustive password search
  - ◆ **entire password space is ‘tried’**
  - ◆ starts by using simple combinations of characters, and then gradually moves to more complex/longer ones
  - ◆ (may be) effective for passwords of small size, but too time consuming for long passwords
  - ◆ examples of brute-force crackers
    - **Cryptool**
    - **Cain and Able**
    - **John the Ripper**
    - **Ophcrack**

Assignment Project Exam Help

<https://powcoder.com>

Add WeChat powder

# Password Cracking (cont.)

In the case of brute-force password cracking, there is no particular strategy when generating password guesses. The entire possible space of passwords is explored.



123456

*hacker makes a password guess*

hash function

Assignment Project Exam Help

<https://powcoder.com>

*stolen password hash*

\$1\$OUI3t9gn\$0o1HTDJeZDVNxcLcoFbai.

\$1\$r6T8SUB9\$Qxe41FJyF/3gkPluvKOQ90

Add WeChat powcoder

Do hashes  
match  
exactly?

no

yes

*try another password*

*cracking successful !*



# Password Cracking (cont.)

## What is Password Search Space in Brute-Force Attacks?

a) On 26-letter alphabet, password of length 1/2/n:

?  $S_{1\text{-Letter}} = 26^1$   
? ?  $S_{2\text{-Letter}} = 26 * 26 = 26^2$   
? ? ... ?  $S_{n\text{-Letter}} = 26 * 26 * ... * 26 = 26^n$

Assignment Project Exam Help

<https://powcoder.com>

Add WeChat powcoder

b) On A-character alphabet (lett. + numb.), passw. of length n:

$$S_{n\text{-character}} = A^n$$

c) On A-character alphabet, passwords up-to n characters

$$S_{\text{varying-size}} = \sum_{i=1}^n A^i = \frac{A^{n+1} - 1}{A - 1}$$

# Password Cracking (cont.)

## Example: Brute-Force Password Search Space (2)

Tina has to create a password for the security of a software program file. She wants to use a password with 3 letters.

How many passwords are allowed if no letter is repeated and the password is not case sensitive?

<https://powcoder.com>

L<sub>1</sub> L<sub>2</sub> L<sub>3</sub> : A (B-Z) (C-Z)

26 25 24

$$26 * 25 * 24 = 15,600$$

# Password Cracking (cont.)

## Example: Brute-Force Password Search Space (3)

A system allows passwords consisting of 4 lower-case letters followed by 3 digit numbers.

How many passwords are possible if there are no restrictions.

<https://powcoder.com>

$L_1 L_2 L_3 L_4 D_1 D_2 D_3$   
Add WeChat powcoder  
any combination any combination

$$26^4 * 10^3 = 456,976,000$$