Homework 2 - mySolution

******### Q1.

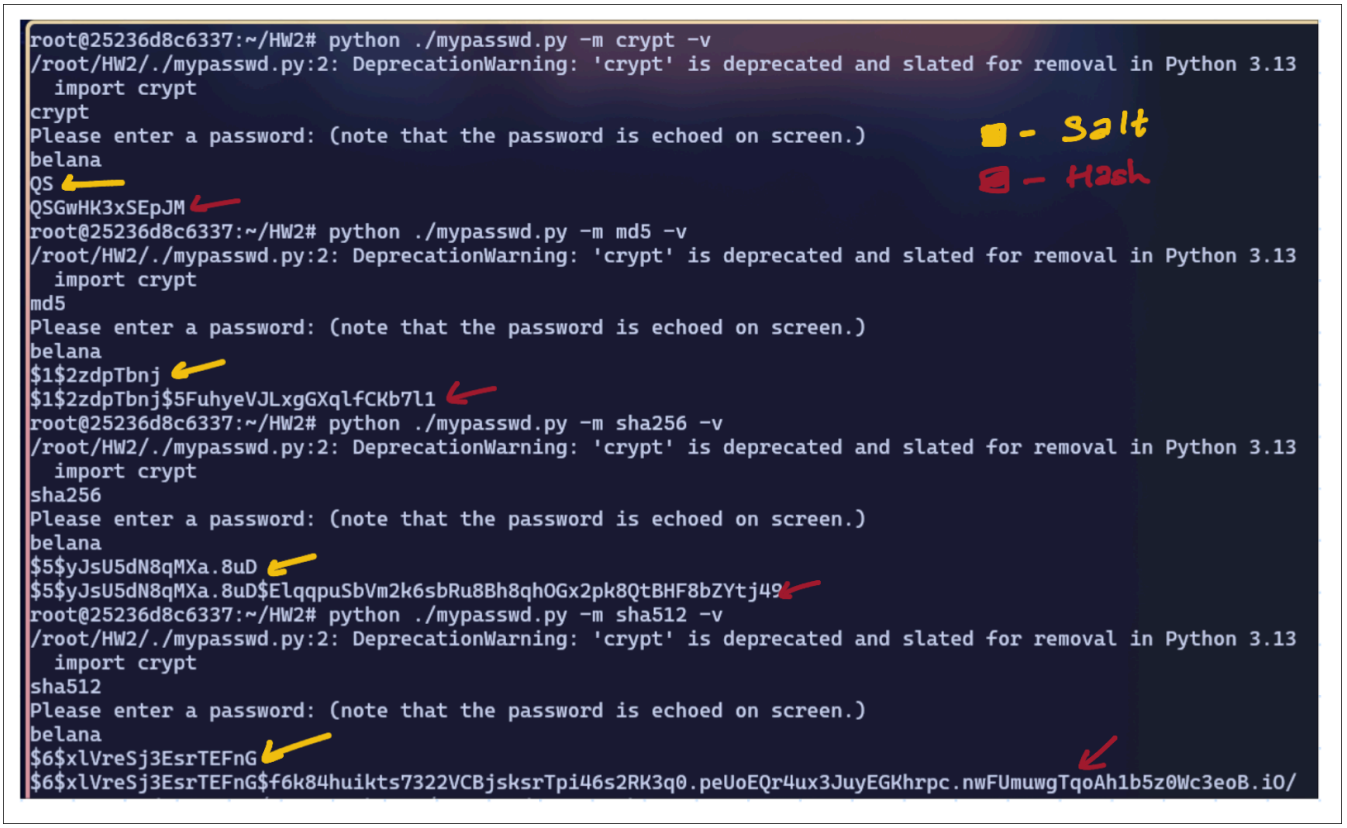
Answer:
Yes, both Google Chrome and Firefox offer built-in password management features. However, they are encrypted using the OS's encryption mechanism and stored locally on your device.

- **Google Chrome** doesn't offer a master password feature. Once we login to OS account, accessing saved passwords in Chrome doesn't require additional authentication.
- **Firefox** provides and optional `Primary Password` option. When it is enabled, it requries the user to enter this password to access the stored credentials, adding an extra layer of security.

Feature	Google Chrome	Firefox
Master Password	Not Available	Yes (Optional)
Preventing Unauthorized Access	anyone with access to your user account can view passwords	Master password ensures that only individuals who know this password can access the credentials
Cloud Sync	Enabled to sync across devices - signed in	Can Sync password across devices - signed in
Server Knowledge of Plaintext passwords	They are encrypted. Google claims it cannot access your plaintext credentials	Encrypts passwords before syncing them to mozilla's servers, ensuring Mozilla can't have access to them.

Q2

a)




```
root@25236d8c6337:~/HW2# python ./mypasswd.py -m crypt -v
/root/HW2/./mypasswd.py:2: DeprecationWarning: 'crypt' is deprecated and slated for removal in Python 3.13
  import crypt
crypt
Please enter a password: (note that the password is echoed on screen.)
belana
QS
QSGwHK3xSEpJM
root@25236d8c6337:~/HW2# python ./mypasswd.py -m md5 -v
/root/HW2/./mypasswd.py:2: DeprecationWarning: 'crypt' is deprecated and slated for removal in Python 3.13
  import crypt
md5
Please enter a password: (note that the password is echoed on screen.)
belana
$1$2zdpTbnj
$1$2zdpTbnj$5FuhyeVJLxgGXqlfCKb7l1
root@25236d8c6337:~/HW2# python ./mypasswd.py -m sha256 -v
/root/HW2/./mypasswd.py:2: DeprecationWarning: 'crypt' is deprecated and slated for removal in Python 3.13
  import crypt
sha256
Please enter a password: (note that the password is echoed on screen.)
belana
$5$yJsU5dN8qMXa.8uD
$5$yJsU5dN8qMXa.8uD$ElqqpuSbVm2k6sbRu8Bh8qhOGx2pk8QtBHF8bZYtj49
root@25236d8c6337:~/HW2# python ./mypasswd.py -m sha512 -v
/root/HW2/./mypasswd.py:2: DeprecationWarning: 'crypt' is deprecated and slated for removal in Python 3.13
  import crypt
sha512
Please enter a password: (note that the password is echoed on screen.)
belana
$6$xlVreSj3EsrTEFnG
$6$xlVreSj3EsrTEFnG$f6k84huikts7322VCBjsksrTpi46s2RK3q0.peUoEQr4ux3JuyEGKhrpc.nwFUmuwgTqoAh1b5z0Wc3eoB.iO/
```

my observations:

1. When running `md5`, `crypt`, `sha256`, `sha512`, we get a different Hash every time since the salt is randomly specified.
2. When in verbose mode `-v`, I see the salt keeps changing every time I run any of the methods. No matter the change in method, this program generates a random Salt.
3. If given a same salt using `-s`, the program generates the same hash value.

---

b)

`aA`:

```
root@25236d8c6337:~/HW2# python ./mypasswd.py -s 'aA'
/root/HW2/./mypasswd.py:2: DeprecationWarning: 'crypt' is deprecated and slated for removal in Python 3.13
  import crypt
Please enter a password: (note that the password is echoed on screen.)
abc123
aAMdEccyA3LP2
root@25236d8c6337:~/HW2#
```

hash: `aAMdEccyA3LP2`

`$1$lXyXHBaP`:

```
root@25236d8c6337:~/HW2# python ./mypasswd.py -s '$1$lXyXHBaP'
/root/HW2/./mypasswd.py:2: DeprecationWarning: 'crypt' is deprecated and slated for removal in Python 3.13
  import crypt
Please enter a password: (note that the password is echoed on screen.)
abc123
$1$lXyXHBaP$rSq48Yg0J9J8De4b/634x/
root@25236d8c6337:~/HW2#
```

hash: `$1$lXyXHBaP$rSq48Yg0J9J8De4b/634x/`

`$5$sHsbaOklL9HZRKZA`:

```
root@25236d8c6337:~/HW2# python ./mypasswd.py -s '$5$sHsbaOklL9HZRKZA'
/root/HW2/./mypasswd.py:2: DeprecationWarning: 'crypt' is deprecated and slated for removal in Python 3.13
  import crypt
Please enter a password: (note that the password is echoed on screen.)
abc123
$5$sHsbaOklL9HZRKZA$b7zAzmguiDxSCFahS4sonX9fMdoihOLUryHLKQsFfh0
root@25236d8c6337:~/HW2#
```

hash: `$5$sHsbaOklL9HZRKZA$b7zAzmguiDxSCFahS4sonX9fMdoihOLUryHLKQsFfh0`

---

c)

`CUnRTj3ykJUkc`:

```
root@25236d8c6337:~/HW2# python  ./guess-password.py --number 'CUnRTj3ykJUkc'
/root/HW2/./guess-password.py:3: DeprecationWarning: 'crypt' is deprecated and slated for removal in Python 3.13
  import crypt
Trying numbers from 0 to 99999999...
736134
root@25236d8c6337:~/HW2#
```

Password is `736134`

`$1$2ewNLDoz$GxiXqiOZweZPTzh4spxzs0`:

```
root@25236d8c6337:~/HW2# python  ./guess-password.py --number '$1$2ewNLDoz$GxiXqiOZweZPTzh4spxzs0'
/root/HW2/./guess-password.py:3: DeprecationWarning: 'crypt' is deprecated and slated for removal in Python 3.13
  import crypt
Trying numbers from 0 to 99999999...
272002
root@25236d8c6337:~/HW2#
```

Password is `272002`

`$5$waAsZWO52fJSzE.x$.nl4eoocyyWHXoeNT.cIsb1ycO/comIfwT/GoIcav27`:

```
root@25236d8c6337:~/HW2# python  ./guess-password.py --number '$5$waAsZWO52fJSzE.x$.nl4eoocyyWHXoeNT.cIsb1ycO/comI
fwT/GoIcav27'
/root/HW2/./guess-password.py:3: DeprecationWarning: 'crypt' is deprecated and slated for removal in Python 3.13
  import crypt
Trying numbers from 0 to 99999999...
4400
root@25236d8c6337:~/HW2#
```

Password: `4400`

---

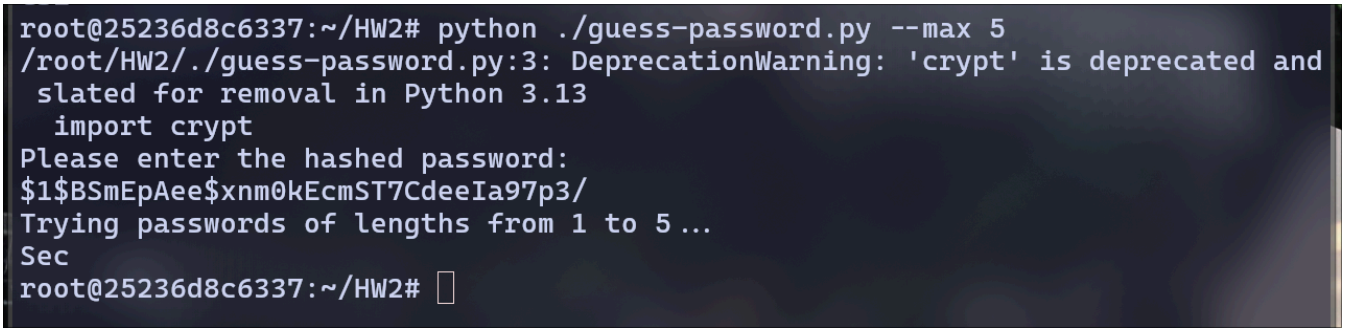
d)

`SehYy7JsbWXCk`:

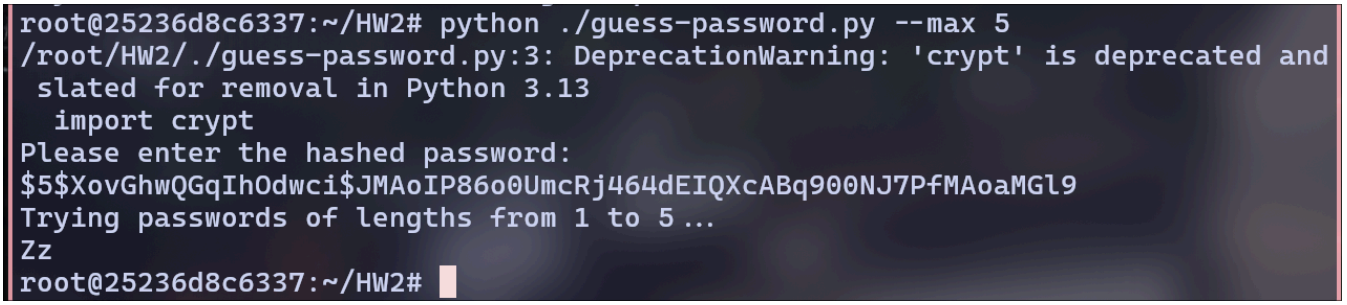
```
root@25236d8c6337:~/HW2# python ./guess-password.py --max 5
/root/HW2/./guess-password.py:3: DeprecationWarning: 'crypt' is deprecated and
 slated for removal in Python 3.13
  import crypt
Please enter the hashed password:
SehYy7JsbWXCk
Trying passwords of lengths from 1 to 5...
CSE
root@25236d8c6337:~/HW2#
```

Password: CSE

`$1$BSmEpAee$xnm0kEcmST7CdeeIa97p3/` :



Password: Sec



Password: Zz

---

e)

I used a number `91080` to create Hashes

Method	Hash
crypt	uqT5B1gakEpDY
md5	`$1$RNCymQDW$Z.GYbORbQCrSuDRrCLPH80`
SHA256	`$5$yuUPJgolmF.C/fC9$zqVJnysrosCGqjtdA/X4/z7N3tuuo.MacbwL2z0aRi6`

```
root@25236d8c6337:~/HW2# python ./mypasswd.py -m crypt
/root/HW2/./mypasswd.py:2: DeprecationWarning: 'crypt' is deprecated and slate
d for removal in Python 3.13
  import crypt
Please enter a password: (note that the password is echoed on screen.)
91080
uqT5B1gakEpDY
root@25236d8c6337:~/HW2# python ./mypasswd.py -m md5
/root/HW2/./mypasswd.py:2: DeprecationWarning: 'crypt' is deprecated and slate
d for removal in Python 3.13
  import crypt
Please enter a password: (note that the password is echoed on screen.)
91080
$1$RNCymQDW$Z.GYbORbQCrSuDRrCLPH80
root@25236d8c6337:~/HW2# python ./mypasswd.py -m sha256
/root/HW2/./mypasswd.py:2: DeprecationWarning: 'crypt' is deprecated and slate
d for removal in Python 3.13
  import crypt
Please enter a password: (note that the password is echoed on screen.)
91080
$5$yuUPJgolmF.C/fC9$zqVJnysrosCGqjtdA/X4/z7N3tuuo.MacbwL2z0aRi6
root@25236d8c6337:~/HW2# python ./mypasswd.py -m sha512
/root/HW2/./mypasswd.py:2: DeprecationWarning: 'crypt' is deprecated and slate
d for removal in Python 3.13
  import crypt
Please enter a password: (note that the password is echoed on screen.)
91080
$6$8iBvxX3mI9QMNNaz$O8YSN12mLaCVVOMx8WDVnTcxp7rC9KU1vPTq7RCyX6MQbpAbHSHJWhdvao
6fwxBtUImWKSHs/jTjziRBZRuWm/
root@25236d8c6337:~/HW2#
```

Running the `guess-passwd.py` to get the original message using the following command.

```
time python ./guess-passwd.py '<hash_here>'  --number --max 5
```

Total Execution Time: Adding `user` + `sys` to get Total time it took to guess the message.

Guesses Per Second: max/total time = 100000/total time.

Method	Execution Time	Guesses Per Second	Ratio with SHA256
SHA256	224.698s	445	1
Crypt	0.520s	192,307	432.150
MD5	11.246s	8892	19.982

```
root@25236d8c6337:~/HW2# time python ./guess-passwd.py 'uqT5B1gakEpDY'  --numb
er --max 5
/root/HW2/./guess-passwd.py:3: DeprecationWarning: 'crypt' is deprecated and s
lated for removal in Python 3.13
  import crypt
Trying numbers from 0 to 99999 ...
91080

real    0m0.521s
user    0m0.506s
sys     0m0.014s
root@25236d8c6337:~/HW2# time python ./guess-passwd.py '$1$RNCymQDW$Z.GYbORbQC
rSuDRrCLPH80'  --number --max 5
/root/HW2/./guess-passwd.py:3: DeprecationWarning: 'crypt' is deprecated and s
lated for removal in Python 3.13
  import crypt
Trying numbers from 0 to 99999 ...
91080

real    0m11.275s
user    0m11.233s
sys     0m0.013s
root@25236d8c6337:~/HW2# time python ./guess-passwd.py '$5$yuUPJgolmF.C/fC9$zq
VJnysrosCGqjtdA/X4/z7N3tuuo.MacbwL2z0aRi6'  --number --max 5
/root/HW2/./guess-passwd.py:3: DeprecationWarning: 'crypt' is deprecated and s
lated for removal in Python 3.13
  import crypt
Trying numbers from 0 to 99999 ...
91080

real    3m45.335s
user    3m44.589s
sys     0m0.109s
root@25236d8c6337:~/HW2#
```

---

f)

1. **Ten decimal digits**
   Time = Total possible passwords / passwords per second
   = 10^{10} / 100000 = 100,000 seconds
   = 1 day (approximately)
2. **Ten characters of decimal digits, uppercase and lowercase English letters.**
   Choices = 26 + 26 + 10 = 62
   Total passwords = 2^{62}
   Time = Total Passwords / 100,000 = 266 years (approx.)
3. **Four English words randomly chosen from a dictionary of 10,000 words. A word maybe chosen multiple times. For example, “ILoveComputerScience”, “UpPalaceRubSoap”, or “SesameSesameOpenDoor”.**
   Each word is randomly chosen from 10,000 words and we have four words in it
   So, Total Paswords = $10,000^4$ = 10^{16}
   Total Time = Total Passwords / 100,000
   = 3169 years (approx.)
