

# ***RANDOM PASSWORD GENERATE FOR USER***

this project and presentation for partial fulfillment of  
**Problem Solving Using Python Programming**

**SESSION 2022-2023**

BY:

GROUP 10, TEAM-23

MEDHA ANAND CHOMAL:	2210991914
MD UMAIR RASHIDI:	2210991913
RAJAT JUNEJA:	2210931013

**SUPERVISOR**

**Dr. SANJOY KUMAR DEBNATH**

**INSTITUTE OF ENGINEERING AND TECHNOLOGY**  
**CHITKARA UNIVERSITY**

1. INTRODUCTION
2. PROBLEM STATEMENT
3. AIM AND OBJECTIVE
4. METHODOLOGY
5. RESULT AND ANALYSIS
6. LIMITATION OF THE PROJECT
7. CONCLUSION
8. REFERENCE
9. APPENDIX




# **INTRODUCTION**

A strong password is a key to protect your personal assets online. **Password Generator** is used in a way through which highly secure passwords are generated that is really hard to crack or hack.




PROBLEM

# PROBLEM STATEMENT



In a recent report, it's shown that over 80% of breaches related to hacking are a result of stolen or weak passwords. Creating strong and secure passwords is an important step to protect our personal information. Let's start developing this amazing project that helps in generating random passwords and also learn some concepts of python. So here is the Python password Generator project.

# AIM AND OBJECTIVE

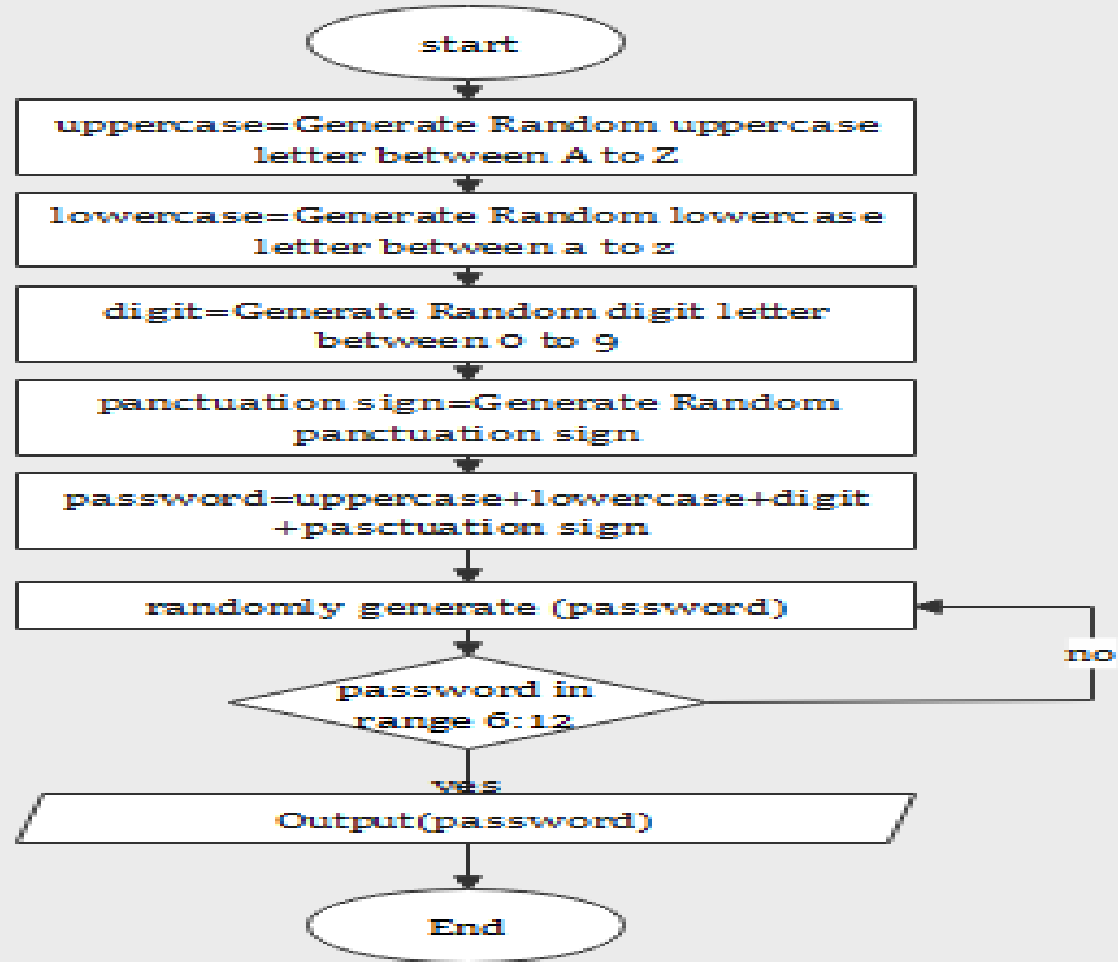


This is a very simple project in which we just have to enter the length of the password and select the password strength from the given options. After entering these two things a password will be generated randomly according to our requirement at the bottom of the screen. The objective of this project is to generate passwords in Python. It requires three modules: Tkinter , random and string. Knowledge of functions in python is recommended in this project. Our objective is to create a program which can secure information.

# **METHODOLOGY**

The use of **Password Generator** is extremely easy. It requires simple step when you have to select the criteria for the password. After selecting the field, all you need is to select the generate password option. That will help you in getting a password that is absolutely secured and safe to use.

# FLOWCHART

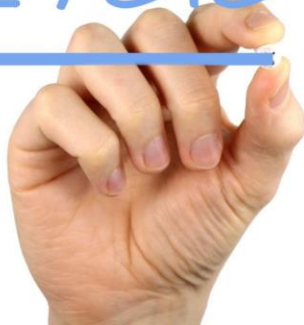




# RESULT AND ANALYSIS

We have completed the password Generator python project successfully. Few functions are also created to develop this python project. It will create a strong password which will secure the important files and documents, also used in many websites.

# ANALYSIS





# **LIMITATIONS OF THE PROJECT**

- Forgetting master password could be disastrous.
- Forgetting to sign out could allow someone access to all accounts.
- It may not protect your data from specific threats.
- Passwords you have created using the free online service might be stolen.
- It may fail to support all kinds of devices and browsers.
- Data is not secure in case of an attack from hackers.

# CONCLUSION

➤ The password generated using alpha-numerical random password mechanism that was illustrated above is practical and can be used with great results. When the password is selected manually, most of the time, the users select the password that are related to himself or herself and related to any of the event. This gives the space for the intruders to deploy various attacks in breaking the passwords. The random generated passwords avoid this particular situation. One of the drawbacks could be the difficulty in memorizing the randomly generated password. But when comparing the security achieved through the randomly generated password, it is much preferable than the manually chosen password. The encryption and decryption standard provided here also strengthens the security measures. Since, the encryption and decryption standards are simple, it is cost effective. The above done work also creates awareness and interest to start exploring this field more



Conclusion

# **REFERENCE**

[1] Robert Biddle, Mohammad Mannan, Paul C van Oorschot, and Tara Whalen. User study, analysis, and usable security of passwords based on digital objects. *IEEE Transactions on Information Forensics and Security*, 6(3):970–979, 2011.

[2] Dinei Florêncio, Cormac Herley, and Paul C van Oorschot. Password portfolios and the finite-effort user: Sustainably managing large numbers of accounts. In *Proceedings of the 23rd USENIX Security Symposium*, San Diego, CA, USA, August 20–22, 2014, pages 575–590. USENIX Association.

[3] J Alex Halderman, Brent Waters, and Edward W Felten. A convenient method for securely managing passwords. In Allan Ellis and Tatsuya Hagino, editors, *Proceedings of the 14th international conference on World Wide Web*, WWW 2005, Chiba, Japan, May 10–14, 2005, pages 471–479. ACM, 2005.



# APPENDIX

```
import random
import string

print('Hello, Welcome to Password generator!')

length = int(input('\nEnter the length of password: '))

lower = string.ascii_lowercase
upper = string.ascii_uppercase
num = string.digits
symbols = string.punctuation

a= lower + upper + num + symbols

temp = random.sample(a,length)
password = "".join(temp)
all = string.ascii_letters + string.digits + string.punctuation

password = "".join(random.sample(a,length))
print("Your Random Password is:",password)
if length<8:
    print("The password is not strong")
elif length==8:
    print("The password is mid")
else:
    print("Strong password")|
```



Thank  
You