User Manual – Random Password Generator

📄 ข้อมูลทั่วไปของโปรแกรม

โปรแกรม **Random Password Generator.py** เป็นเครื่องมือสำหรับสร้างรหัสผ่านแบบสุ่ม โดยผู้ใช้สามารถกำหนดความยาวของรหัสผ่านและเลือกประเภทตัวอักษรที่ต้องการ เช่น ตัวพิมพ์ใหญ่ ตัวพิมพ์เล็ก ตัวเลข และสัญลักษณ์พิเศษ เพื่อให้ได้รหัสผ่านที่ปลอดภัยตรงตามความต้องการ

🧩 คุณสมบัติของโปรแกรม (Features)

- กำหนดความยาวรหัสผ่านได้ (ขั้นต่ำ 4 ตัวอักษร)
- เลือกประเภทของตัวอักษรที่ต้องการใช้งาน
  - ตัวอักษรพิมพ์ใหญ่ (A–Z)
  - ตัวอักษรพิมพ์เล็ก (a–z)
  - ตัวเลข (0–9)
  - สัญลักษณ์พิเศษ (!@#$% เป็นต้น)
- สุ่มรหัสผ่านพร้อมรับประกันว่ามีตัวอักษรตามประเภทที่เลือก
- ใช้งานผ่าน Command Line / Terminal

💻 วิธีการใช้งานโปรแกรม

รันโปรแกรม

ให้เปิด Terminal หรือ Command Prompt แล้วพิมพ์:

python Random_Password_Generator.py

หน้าจอจะแสดงข้อความ:

--- Random Password Generator ---

กำหนดความยาวของรหัสผ่าน

โปรแกรมจะถามว่า:

Enter password length (min 4):

ให้ป้อนตัวเลข **ตั้งแต่ 4 ตัวขึ้นไป**
หากป้อนต่ำกว่า 4 หรือไม่ใช่ตัวเลข โปรแกรมจะแจ้งเตือนและให้ป้อนใหม่

เลือกประเภทตัวอักษร

โปรแกรมจะถามทีละข้อ โดยให้ตอบ **y = ใช่**, **n = ไม่ใช่**

ตัวอย่าง:

Include Uppercase letters? (y/n):

Include Lowercase letters? (y/n):

Include Numbers? (y/n):

Include Symbols? (y/n):

ผู้ใช้สามารถเลือกได้หลายแบบ เช่น

- y y y y → มีทุกประเภท
- y n y n → เฉพาะตัวใหญ่ + ตัวเลข
- n n n n → ❌ ไม่ได้ (โปรแกรมจะเตือนให้เลือกอย่างน้อย 1 ประเภท)

โปรแกรมจะสร้างรหัสผ่าน

หลังจากกำหนดทุกอย่างแล้ว โปรแกรมจะแสดงผล:

Generated Password: A8s#fK

รหัสผ่านจะสุ่มใหม่ทุกครั้งที่รัน

⚙️ หลักการทำงาน (สรุปโค้ดสำหรับผู้สนใจ)

1. รับความยาวรหัสผ่านจากผู้ใช้
2. ถามว่าต้องการใช้ตัวอักษรประเภทใดบ้าง
3. สร้างชุดอักขระ (Character Pool) ตามที่ผู้ใช้เลือก
4. รับประกันว่าทุกประเภทที่เลือกมีอยู่ในรหัสผ่าน
5. เติมตัวอักษรที่เหลือให้ครบความยาว
6. สลับตำแหน่ง (shuffle) แล้วแสดงผล

❗ ข้อควรทราบ

- หากไม่เลือกประเภทตัวอักษรเลย โปรแกรมจะไม่สร้างรหัสผ่านและแสดงข้อความเตือน
- การสร้างรหัสผ่านในโปรแกรมนี้เหมาะกับการใช้งานทั่วไป ไม่เหมาะสำหรับความมั่นคงระดับองค์กรที่ต้องใช้ Cryptographically Secure RNG