

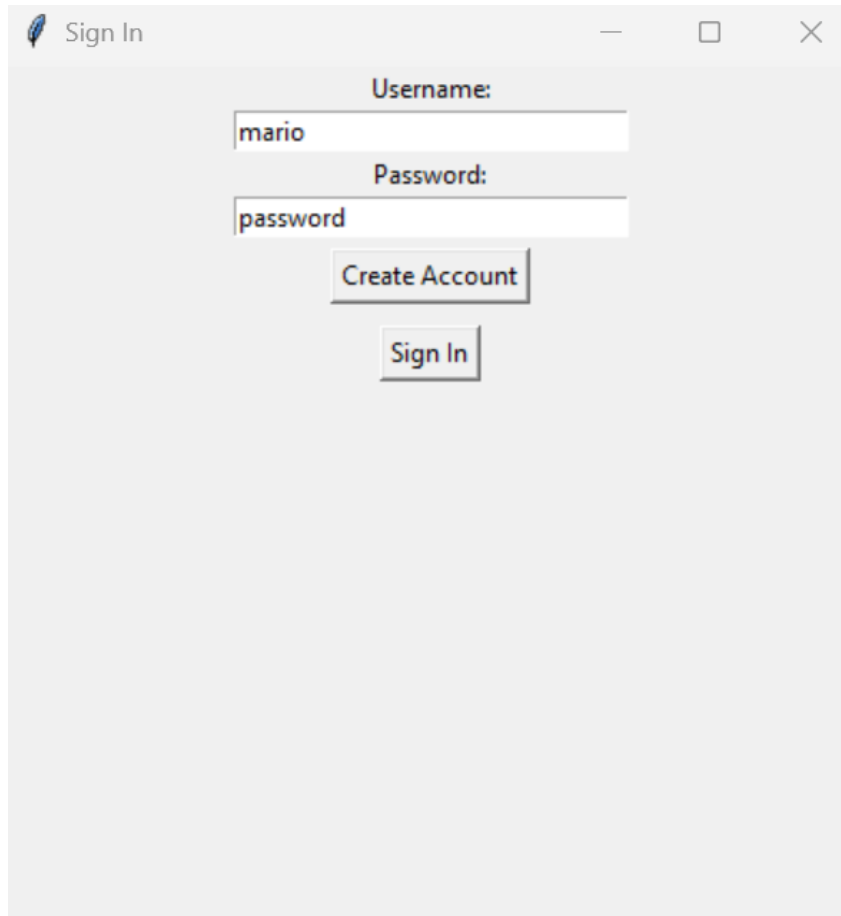
Weekly Update - Password Manager

Mario Getaw, Joshua Moore, Jarrett Wilson

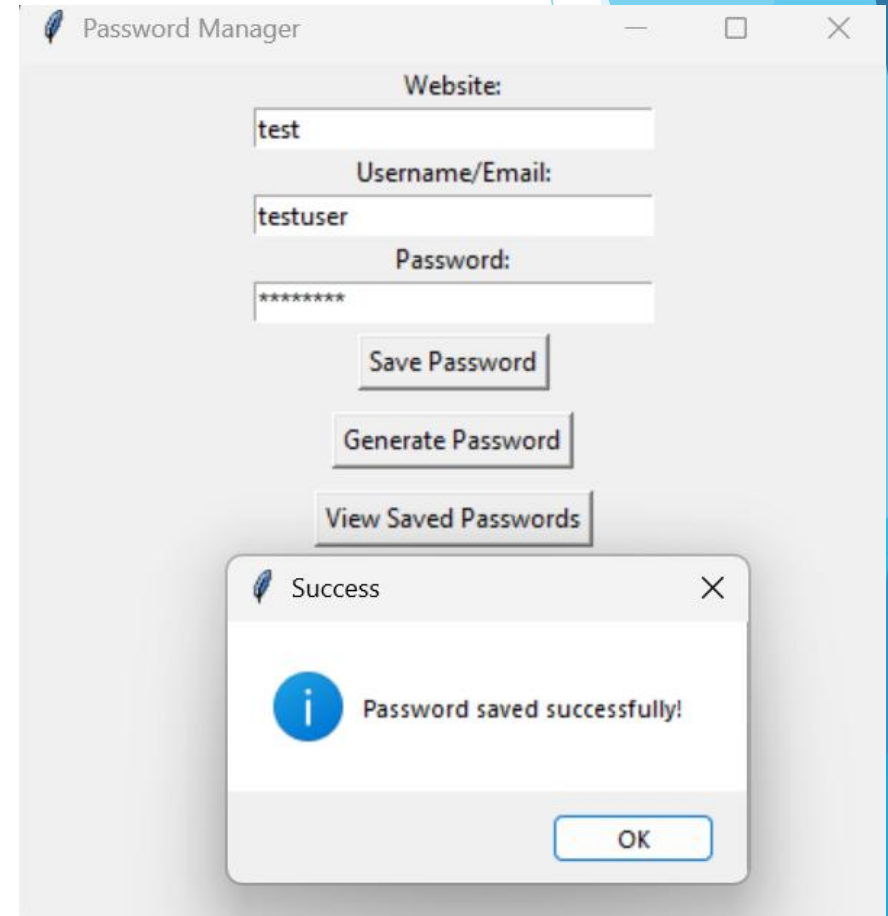
Encryption Code

```
9  # Function to load or create a key for encryption
10 def load_key():
11     if os.path.exists("password_manager.key"):
12         with open("password_manager.key", "rb") as key_file:
13             return key_file.read()
14     else:
15         key = generate_key()
16         with open("password_manager.key", "wb") as key_file:
17             key_file.write(key)
18     return key
19
20 # Encrypt password before saving
21 def encrypt_password(password, key):
22     f = Fernet(key)
23     encrypted_password = f.encrypt(password.encode())
24     return encrypted_password.decode() # This fixes the binary bytes to JSON issue
25
26 # Decrypt password when retrieving
27 def decrypt_password(encrypted_password, key):
28     f = Fernet(key)
29     decrypted_password = f.decrypt(encrypted_password.encode())
30     return decrypted_password.decode() #####
31
```

Results



A screenshot of a 'Sign In' window. It features a feather icon in the top-left corner and standard window controls (minimize, maximize, close) in the top-right. The form contains two text input fields: 'Username:' with the value 'mario' and 'Password:' with the value 'password'. Below these fields are two buttons: 'Create Account' and 'Sign In'.



A screenshot of a 'Password Manager' window. It has a feather icon and window controls in the title bar. The form includes four text input fields: 'Website:' with 'test', 'Username/Email:' with 'testuser', 'Password:' with '*****', and a 'Save Password' button. Below these are two more buttons: 'Generate Password' and 'View Saved Passwords'. A 'Success' dialog box is open in the foreground, displaying a blue information icon, the text 'Password saved successfully!', and an 'OK' button.

Results Continued

```
{ } passwords_mario.json > ...  
1  {  
2    "test": {  
3      "username": "testuser",  
4      "password": "gAAAAABn5L0iYPTAKJAnbCk8h2GoEv-OAN1vc36ktWqdJgOJCIQknHVcc1zb1VQ2yW0xSMTLT-gAVSY1Iza6i84VzMWfbZPLew=="  
5    }  
6  }
```

Schedule

- Week 3 (1/30) - Research secure password management practices and encryption methods
- Week 4 (2/6) - Compile research findings and outline code
- Week 5 (2/13) - Create the GUI for the application
- Week 6 (2/20) - Create a login for users to view their saved passwords
- Week 7 (2/27) - Write code to ensure all passwords meet the specifications above
- Week 8 (3/6) • F.I.RE Week
- Week 9 (3/13) • Spring break
- Week 10 (3/20) - Create a method for storing user data
- Week 11 (3/27) - Implement data encryption
- Week 12 (4/3) - Add password strength analysis
- Week 13 (4/11) - Test project
- Week 14 (4/18) - Create a project presentation
- Week 15 (4/25) Present project

Next Steps To Wrap off This Weeks Goal

- ▶ Securely allow the user to view their plaintext password
- ▶ Encrypt the actual password for the account
- ▶ Make JSON file secure and not named password
- ▶ Move to next weeks scheduled goal - password strength analysis