ST. VINCENT PALLOTTI COLLEGE OF ENGINEERING & TECHNOLOGY, NAGPUR
(An autonomous institution affiliated to Rashtrasant Tukadoji Maharaj Nagpur University)

SECURE PRIVACY TOOLKIT

Group Number 4CSMP1-20

1.Tanish Dewase Roll no. -67
2.Jay Doble Roll no.-63
3.Paridhi Kshirsagar Roll no.-68
4.Neha Mahule Roll no.-66

Guided By
Mr Abhishek Pathak

COMPUTER SCIENCE & ENGINEERING (CYBER SECURITY)
B. Tech. Micro-Project 2024-25

Contents :

Introduction

In our interconnected digital world, privacy has become a critical concern. With sophisticated cyber threats and mass surveillance on the rise, individuals and organizations need robust tools to protect their sensitive communications and data. A Secure Privacy Toolkit provides an integrated suite of encryption solutions to safeguard digital privacy across multiple attack vectors.

What is a Secure Privacy Toolkit?

A Secure Privacy Toolkit is a collection of cryptographic tools and protocols designed to protect various aspects of digital communication and data storage. It combines multiple layers of encryption, anonymization techniques, and security best practices to create comprehensive protection against:

- Eavesdropping on communications
- Unauthorized data access
- Metadata collection
- Identity tracking
- Man-in-the-middle attacks

ABSTRACT :

In an era of increasing digital surveillance and cyber threats, protecting personal and sensitive data has become crucial. This project focuses on developing a **"Secure Privacy Toolkit"** – a comprehensive solution designed to safeguard digital communications and files through robust encryption and privacy-enhancing technologies.

The toolkit integrates multiple security layers, including **end-to-end encrypted messaging (AES-256), secure file storage, anonymous browsing (Tor/VPN integration), and metadata protection**. Built using **Python with PyCryptodome and cryptographic libraries**, it combines strong encryption standards with a user-friendly interface to make advanced privacy tools accessible to non-technical users.

Key features include:

- Military-grade file encryption/decryption
- Secure communication channels
- Identity protection through anonymization
- Cross-platform compatibility

Objective:

1. **Data Protection:**
   To implement robust encryption mechanisms (AES-256) for securing sensitive files and communications from unauthorized access.
2. **Privacy Enhancement:**
   To integrate anonymization technologies (Tor/VPN) for protecting user identity and browsing activities.
3. **User Accessibility:**
   To develop an intuitive GUI interface that makes advanced security tools accessible to non-technical users.
4. **Comprehensive Security:**
   To create an all-in-one solution combining file encryption, secure messaging, and metadata protection.

5. **Performance Optimization:**
   To maintain efficient system performance while implementing resource-intensive cryptographic operations.

Methodology :

1. **Requirement Analysis**
   Identified the need for private searching, cookie control, and anti-tracking awareness.
2. **Design**
   Created a multi-tab GUI using tkinter to organize features:
   - Private Search
   - Disable Cookies Guide
   - Stop Google Tracking
   - Privacy Tools List
3. **Development**
   - Integrated search function with no tracking or cookies.
   - Added step-by-step privacy instructions with clickable links.
   - Listed privacy-respecting tools (e.g., DuckDuckGo, Brave, ProtonMail).

4. **Testing**
   Verified all links, tab navigation, and privacy features. Ensured clean session behavior.
5. **Deployment**
   Lightweight Python app, ready to run locally with no data collection.

Design and Development Approach

1. **User Interface Design**
   - Built a clean, tab-based GUI using **Tkinter** for ease of navigation.
   - Tabs include: **Private Search**, **Disable Cookies**, **Google Tracking Settings**, and **Privacy Tools**.
2. **Modular Code Structure**
   - Created separate modules for GUI (secure_privacy_gui.py) and search functionality (search_engine.py) to maintain clean separation of concerns.
3. **Function Integration**
   - Used requests for private search results (DuckDuckGo API or scraper).
   - webbrowser module was used to open trusted privacy resource links directly.
4. **User-Centric Features**
   - Each tab provides actionable steps, tools, and clickable hyperlinks.
   - All features are offline-friendly and ensure **no data collection or tracking**.

5. **Lightweight and Secure**
   - No external GUI frameworks or servers required.
   - App ensures minimal resource use and enhanced privacy.

Expected Outcome

The project aims to deliver a standalone, user-friendly application that enables users to perform private web searches, disable tracking features, and access non-tracking tools—ultimately promoting digital privacy and reducing online data exposure.

Time Plan :

Week 1-2: Research and selection of encryption algorithms (AES, RSA).

Week 3-6: Set up development environment and design user interface.
Week 7-8: Implement encryption and decryption functions.
Week 9-10: Integrate UI with the encryption tool.
Week 11-12: Testing and debugging.
Week 13: Final documentation and preparation for presentation.

References :

- **Books, articles, and tutorials on Data Privacy.**
- **Python documentation and library reference.**
- **GitHub**
- www.ncbi.nlm.nih.gov
- https://ieeexplore.ieee.org
- https://www.python.org

Conclusion:

The **Secure Privacy Toolkit** empowers users to take control of their online privacy by enabling private search, disabling tracking mechanisms, and promoting the use of privacy-focused tools. This project highlights the importance of digital privacy and provides a simple yet effective solution for safer internet usage.

Thank You !