LABORATORIUM CYBERBEZPIECZEŃSTWO

Data wykonania ćwiczenia:	25.11.2024
Rok studiów:	4
Semestr:	7
Grupa studencka:	2
Grupa laboratoryjna:	2B

Ćwiczenie nr.	4

Temat: Licencje oprogramowania komputerowego

Osoby wykonujące ćwiczenia:

1. Igor Gawłowicz

Katedra Informatyki i Automatyki

Sprawozdanie na temat zabezpieczeń CAPTCHA i Google reCAPTCHA

1. Wprowadzenie

Licencja oprogramowania to umowa określająca zasady korzystania z programu komputerowego. Jest zawierana pomiędzy właścicielem praw autorskich do oprogramowania a użytkownikiem. W praktyce użytkownicy najczęściej spotykają się z licencjami typu **EULA (End User License Agreement)**, które szczegółowo określają ograniczenia dotyczące użytkowania oprogramowania. Ograniczenia te mogą dotyczyć m.in. liczby urządzeń, na których można zainstalować program, czy rodzaju użytkowania (komercyjne/domowe).

Rodzaje licencji różnią się pod względem możliwości i ograniczeń. Wśród najczęściej spotykanych typów można wyróżnić:

- **Freeware**: Oprogramowanie darmowe, ale najczęściej zamknięte źródłowo.
- **Shareware**: Programy udostępniane bezpłatnie na określony czas lub z ograniczoną funkcjonalnością.
- **Adware**: Oprogramowanie finansowane przez reklamy.
- **Trialware**: Programy dostępne w pełnej funkcjonalności przez ograniczony czas.
- **Demoware**: Oprogramowanie o ograniczonej funkcjonalności lub dostępne w wersji próbnej.

Każda licencja definiuje także sposoby zabezpieczeń, często korzystając z algorytmów szyfrujących, takich jak szyfr Cezara czy szyfr Vigenère'a.

2. Cel i realizacja zadania

Zadanie polegało na zaprojektowaniu systemu licencyjnego dla oprogramowania w modelu **Demoware**. Kluczowe wymagania obejmowały:

1. Ograniczenie funkcjonalności programu – w tym przypadku możliwość otwierania plików o rozmiarze nieprzekraczającym 100 KB.
2. Implementację algorytmu szyfrowania i deszyfrowania klucza licencji przy użyciu szyfru Cezara.

3. Rozwiązanie

W celu realizacji zadania zaimplementowano aplikację internetową w oparciu o framework Flask. Kluczowe funkcjonalności obejmowały:

- **Mechanizm szyfrowania klucza licencji**: Wykorzystano szyfr Cezara do szyfrowania i deszyfrowania klucza licencyjnego. Klucz „UnlockKey123” umożliwiał zniesienie ograniczeń rozmiaru pliku.
- **Ograniczenie funkcjonalności**: Użytkownicy z podstawową wersją licencji mogli otwierać pliki o rozmiarze do 100 KB. Próba otwarcia większego pliku kończyła się komunikatem o błędzie.
- **Elastyczność rozmiaru plików**: Po wprowadzeniu poprawnego klucza licencji limit rozmiaru pliku był zwiększany do 10 MB.

Kod realizujący zadanie zawierał zabezpieczenia przed nieautoryzowanym dostępem oraz możliwość dynamicznej zmiany parametrów w zależności od podanego klucza.

4. Wykorzystane algorytmy szyfrujące

- **Szyfr Cezara**: Każda litera klucza była przesuwana o 3 pozycje w alfabecie. W przypadku deszyfrowania kierunek przesunięcia był odwrotny. Algorytm ten, mimo prostoty, pozwolił na skuteczne zarządzanie kluczem licencji.

5. Wnioski

Zrealizowane zadanie pozwoliło na praktyczne wykorzystanie wiedzy o licencjonowaniu oprogramowania oraz implementacji systemów zabezpieczeń. Wprowadzone ograniczenia funkcjonalności w wersji **Demoware** spełniały wymagania zadania, a zastosowanie szyfru Cezara umożliwiło sprawne zarządzanie kluczami licencyjnymi.

Rozwiązanie to może być rozbudowane w przyszłości, np. o bardziej zaawansowane algorytmy szyfrujące czy dodatkowe typy licencji, co pozwoli na zwiększenie bezpieczeństwa i elastyczności systemu.