Петров Д.М. КІТ-М120б

Лабораторна робота 7

Створення ліцензійного ключа

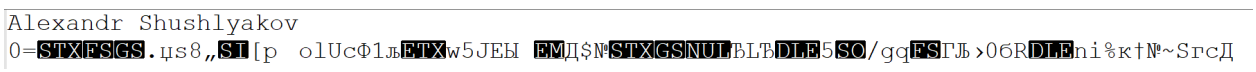
Мета: Дослідити і порівняти існуючі механізми створення і перевірки валідності ліцензійних ключів.

Хід роботи:

Механізм генерації ліцензійоного ключа №1

Створюємо пару ключів (приватний та публічний) через додаток GenKey та пишемо у файл:

Створюємо ліцензійний ключ, що має інформацію о кінцевому корисувачі через додаток MakeKey. У кінці цього ЛК лежить ЕЦП - геш сума, для калькуляції якої використовувся приватний ключ:



Перевіряємо валідність підпису та виводимо дані о користувачі на екран через додаток ReadKey:

Механізм генерації ліцензійоного ключа №2

Запускаємо локальний сервер який буде приймати ключі (додаток Server). У базі (файл) три ключі:

```
KEY1
KEY2
KEY4
```

Запускаємо клієнт з додатку Client та відправляємо на сервер існуючий ключ. Отримаємо відповідь, що ключ прийнято:

```
Enter key:
> KEY1
Key is accepted!
```

Сервер отримав ключ:

```
Received key: KEY1
```

Вводимо з клієнту неіснуючий ключ та отримуємо помилку:

```
Enter key:
> k;ojihlgukyfdjhgxfcvhbjlknm
Exception in thread "main" java.lang.SecurityException: Wrong key provided
        at keys.Client.main(Client.java:23)
```

Висновок: на цій лабораторній роботі ми вивчили пару механізмів створення ліцензійних ключів. Перший захищений через ЕЦП та парні ключі, а другий залежить від видаленого серверу. Обидва є добрими методами захисту від недосвідчених хакерів.