

Підвищення стійкості електронних ключів систем контролю доступу на основі пропрієтарного протоколу з динамічним кодом

*Виконав ст. гр. УБ – 18м Щербатюк А.В.
Керівник к.т.н., доц. Карпінець В.В.*

Актуальність роботи:

- Зумовлена постійним зростанням попиту на встановлення систем контролю доступу, а отже необхідністю постійного їх вдосконалення та впровадження розробок.

Новизна роботи:

- Наукова новизна – підвищення стійкості електронних ключів систем контролю доступу на основі пропрієтарного протоколу з динамічним кодом.

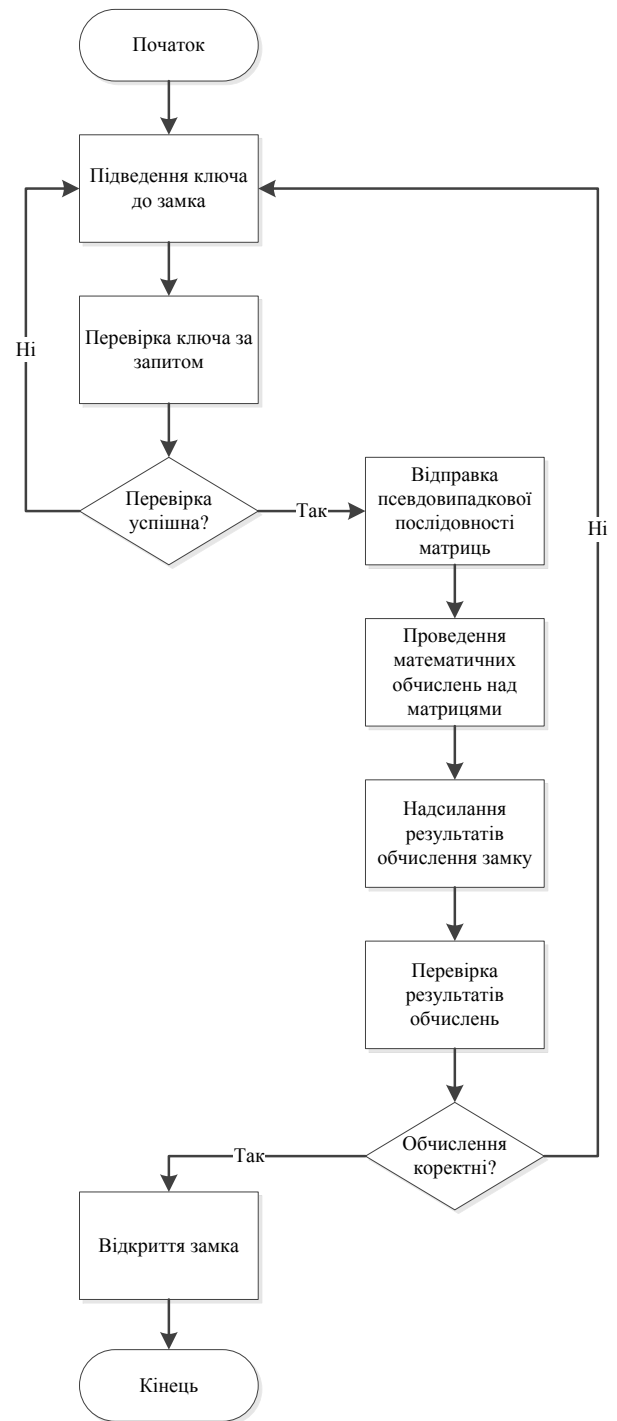
СКУД та ідентифікація користувача



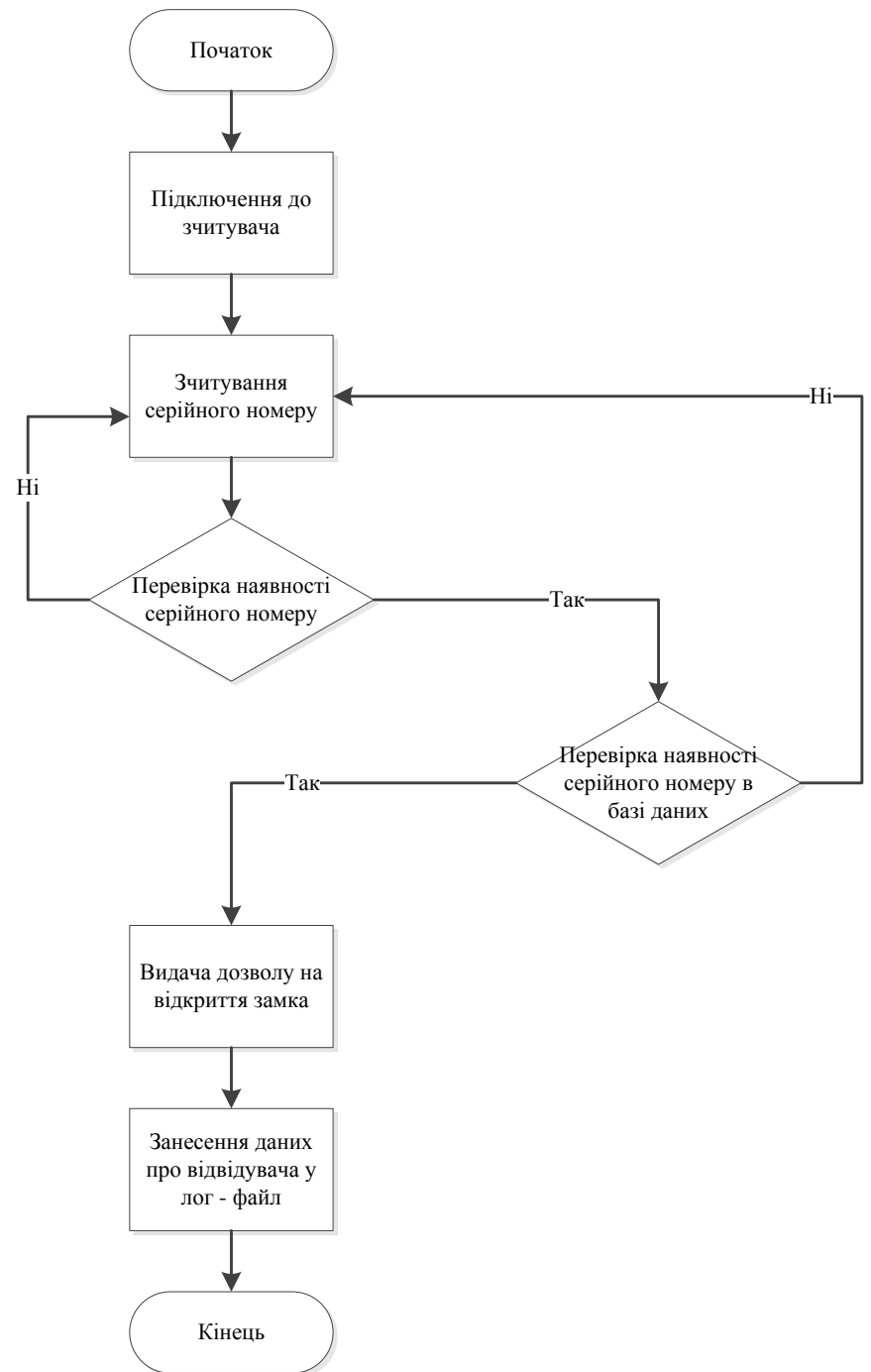
Приклад системи контролю доступу



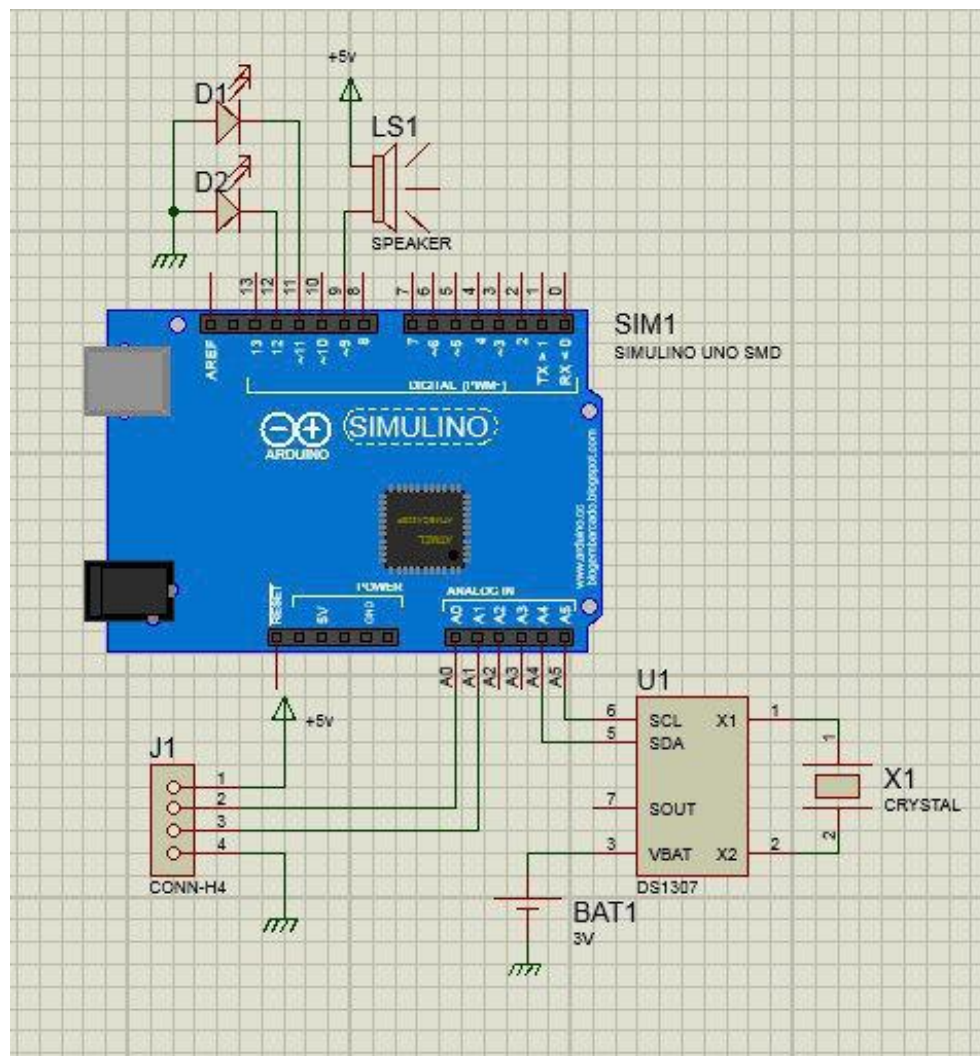
Блок – схема алгоритму роботи



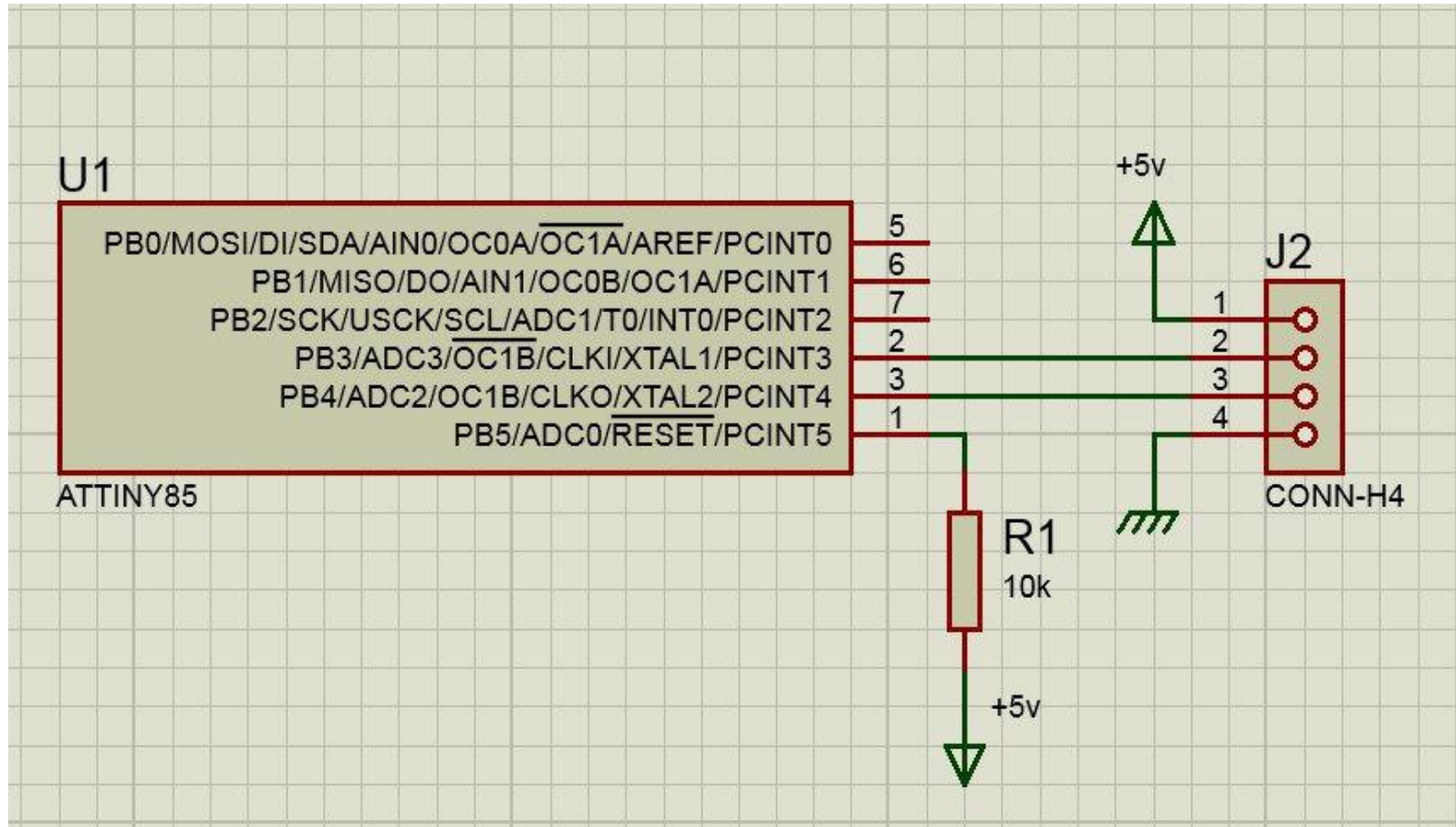
Блок – схема алгоритму роботи серверної частини



Принципова електрична схема замка




Принципова електрична схема ключа



Інтерфейс додатку

Сервер авторизації користувачів




COM15

Словіщення: **Порушень немає**


Номер поточного ключа:

Видалення



Вася Пупкін 12345123
Василь Петрович Геращенко 34576762345
Іванов Петро Вікторович 123455672342341


Додати особу



Серійний номер ключа:

П.І.Б.:

Історія відвідувань



22.01 3534524357644 Іванов Петро

Тестування

- ▶ Представлення даних сніфферу для обміну даними між ключем та замком



```
Sniff v1.4
Request:
13 28 e1 e2
a5 82 bc dd
d9 d4 ec f5
1c 3c 3e 87
Response
ee 38 62 13
da 2d 29 49
0a 72 f7 70
65 7a d8 53
```

- ▶ Приклад дампу – відповіді ключа на сеанс автентифікації



```
Sniff v1.4
Request:
19 db 47 8e
6b 40 e7 87
9f e3 87 a4
9b 45 05 56
Response
79 62 8e 02
2a f3 e5 c8
20 4c 7f 45
f7 ce bd 5b
```

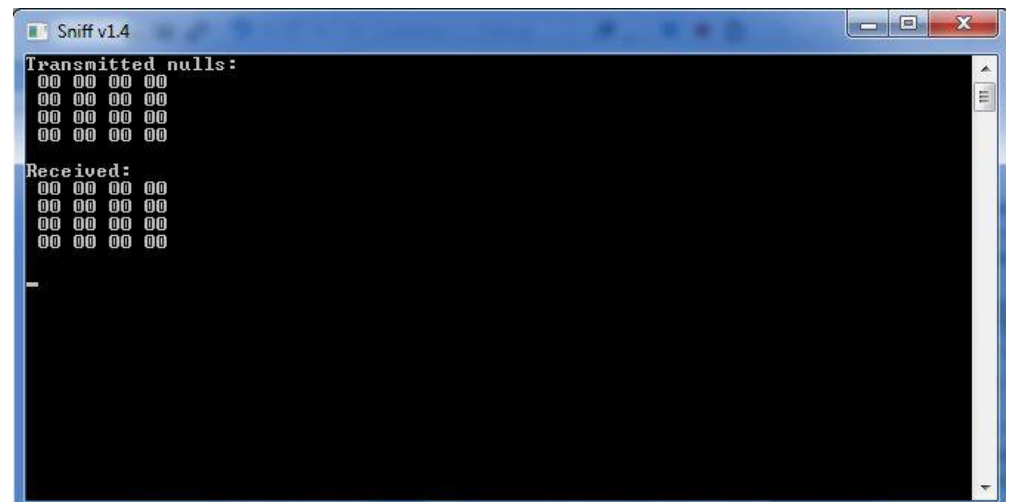
Тестування

- ▶ Відправка ключеві копії запиту замка
- ▶ Відправка ключеві власної матриці (заповненої нулями)



```
Sniff v1.4
Transmitted dump #1:
6f 7a 3a 93
72 4c 9c ba
55 10 ff 5b
c6 44 3f 6b

Received:
8e 96 30 c6
9b 93 49 58
a2 98 2c 92
15 b4 da 23
```

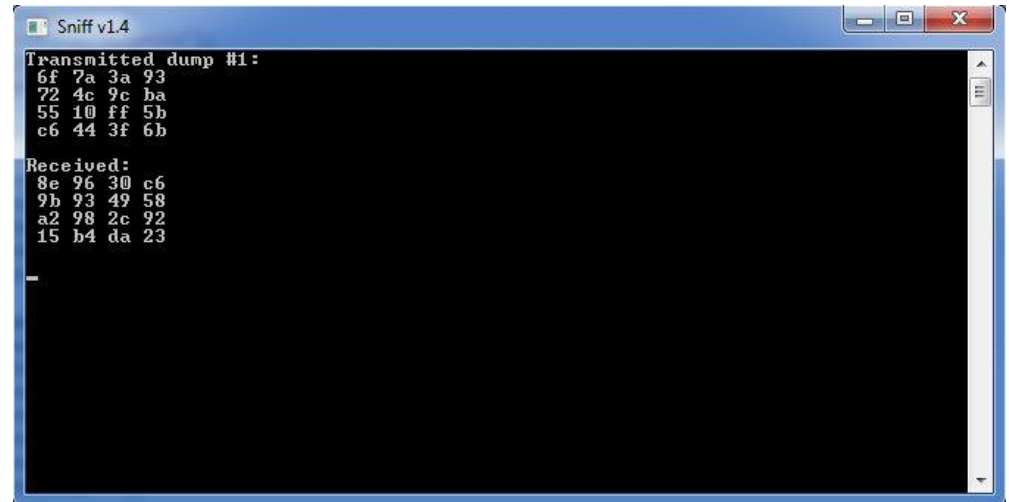


```
Sniff v1.4
Transmitted nulls:
00 00 00 00
00 00 00 00
00 00 00 00
00 00 00 00

Received:
00 00 00 00
00 00 00 00
00 00 00 00
00 00 00 00
```

Тестування

- ▶ Відправка ключеві власної матриці з певними значеннями



```
Sniff v1.4
Transmitted dump #1:
6f 7a 3a 93
72 4c 9c ba
55 10 ff 5b
c6 44 3f 6b

Received:
8e 96 30 c6
9b 93 49 58
a2 98 2c 92
15 b4 da 23
```

- ▶ Отже, перебір матриць обмежується не лише їх значною кількістю, але і часовими рамками. Аналізуючи подані дані, можна зрозуміти, що це неможливим, а головне – недоцільним.
- ▶ Отримані в ході тестування результати, можна вважати, що розроблена система контролю доступу є досить стійкою та ефективною.

Переваги роботи

Отже, розроблений та реалізований пропрієтарний протокол для системи контролю доступу з використанням контактного ключа має такі переваги:

- динамічний код
- динамічну кількість матриць;
- протокол дає "шанс на помилку" без зниження рівня захищеності, додавання кількості матриць, без повторної автентифікації, без сигналізації, відповідно, про те що ключ не пройшов;
- такий алгоритм не має прямих аналогів;
- матриці ніколи не повторюються (в межах розрядності МД5).

Таким чином, можна вважати, що поставлені задачі в результаті виконання роботи було реалізовано.

ДЯКУЮ ЗА УВАГУ!