

Дослідження та створення методів шифрування повідомлень користувача веб-сервісу для інтернет листування

Виконав: студент групи КІТ-М1196 Марценюк Б.В.
Керівник: проф. Філоненко А.М.

Метою дипломної роботи є: дослідження методів шифрування повідомлень веб-сервісу інтернет листування та впровадження вдосконаленого методу шифрування до створюваного веб-сервісу.

Задачі розробки:

- провести дослідження існуючих методів шифрування, виділити основні переваги та недоліки кожного;
- провести аналіз існуючих методів хешування;
- описати основні способи злому хешей;
- провести аналіз використовуваних технологій та методів розробки;
- розробити сласну модель веб-сервісу інтернет листування;
- запровадити до нього вдосконалений метод шифрування;
- провести економічне обґрунтування доцільності створюваного програмного продукту

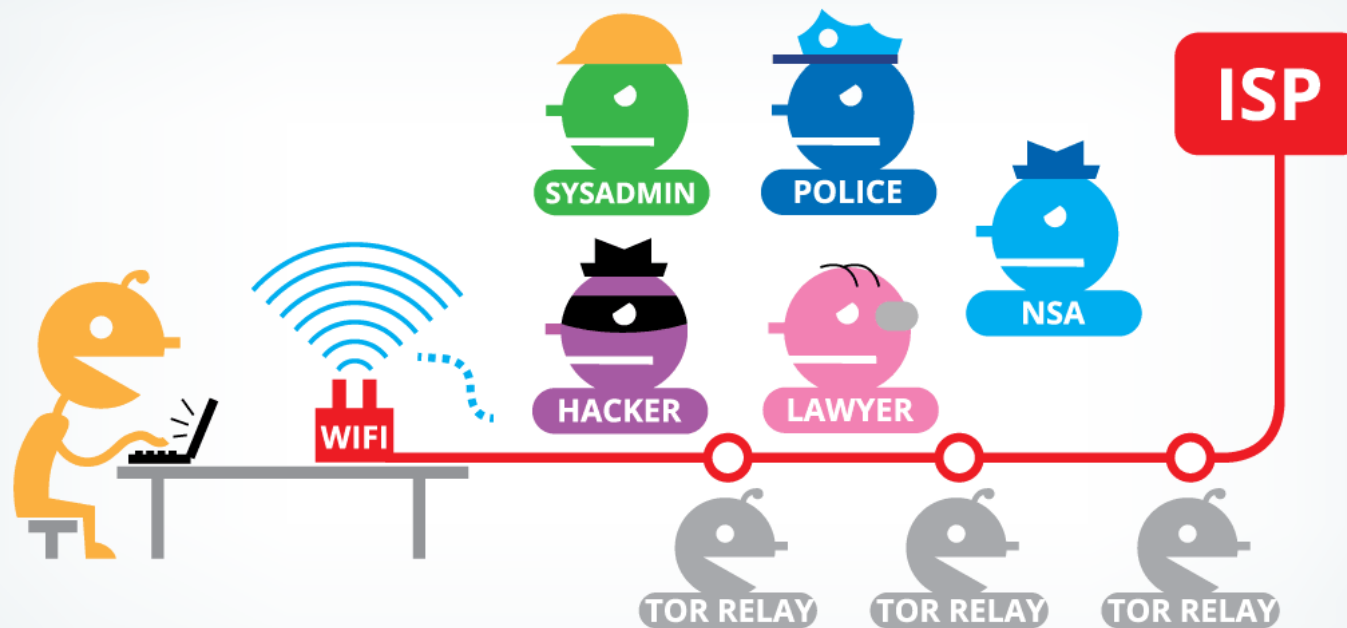
Симетричне шифрування



Асиметричне шифрування



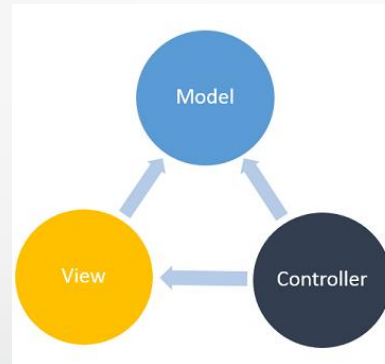
Наскрізне шифрування



Способи злому хешей

- словникові атаки;
- брутфорс;
- таблиці пошуку,
- обернені таблиці пошуку;
- райдужні таблиці пошуку.

Використані технології



База даних

User_from

id_user_from (PK)
name_user_from

User_to

id_user_to (PK)
id_user_from
name_to
msg_text
msg_time

User

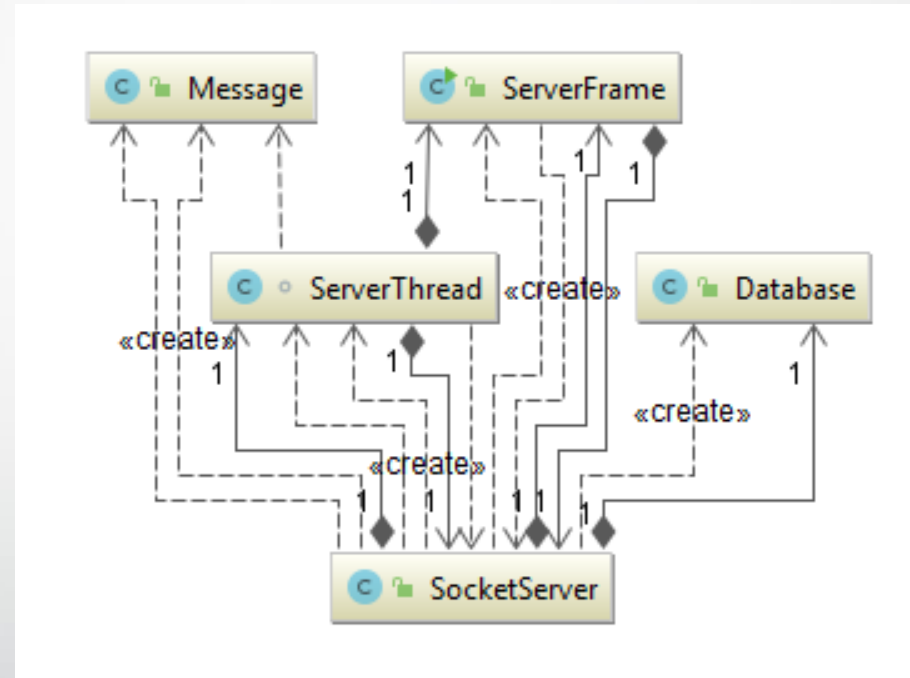
id_user (PK)
email
user_name
user_password

Msg

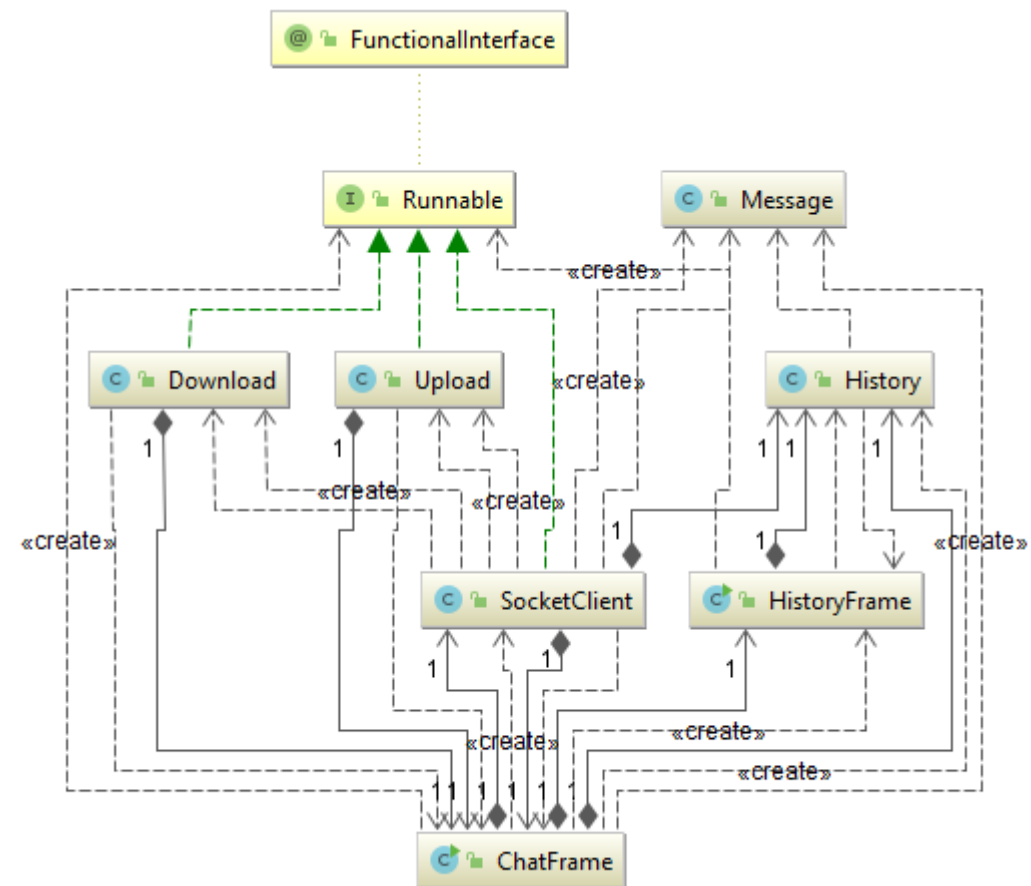
id_msg (PK)
from_user
to_user
msg_text
msg_time

Класи серверної частини

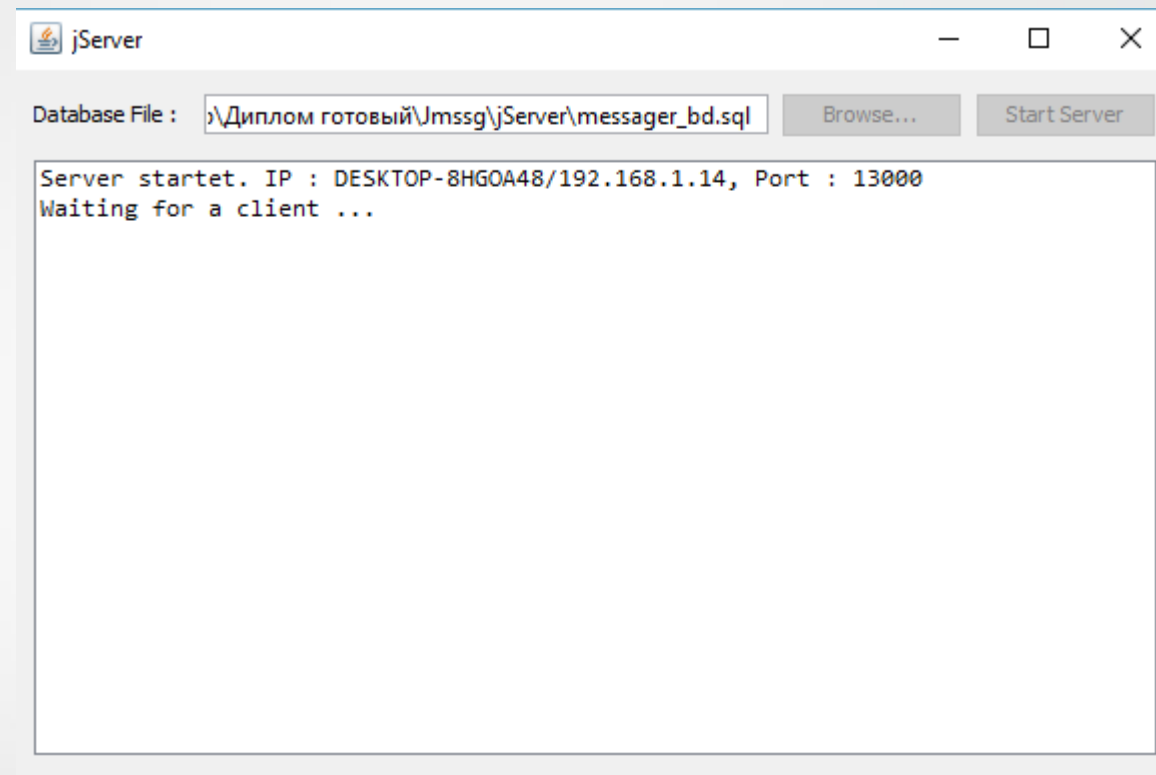
- Message
- ServerFrame
- ServerThread
- Database
- SocketServer



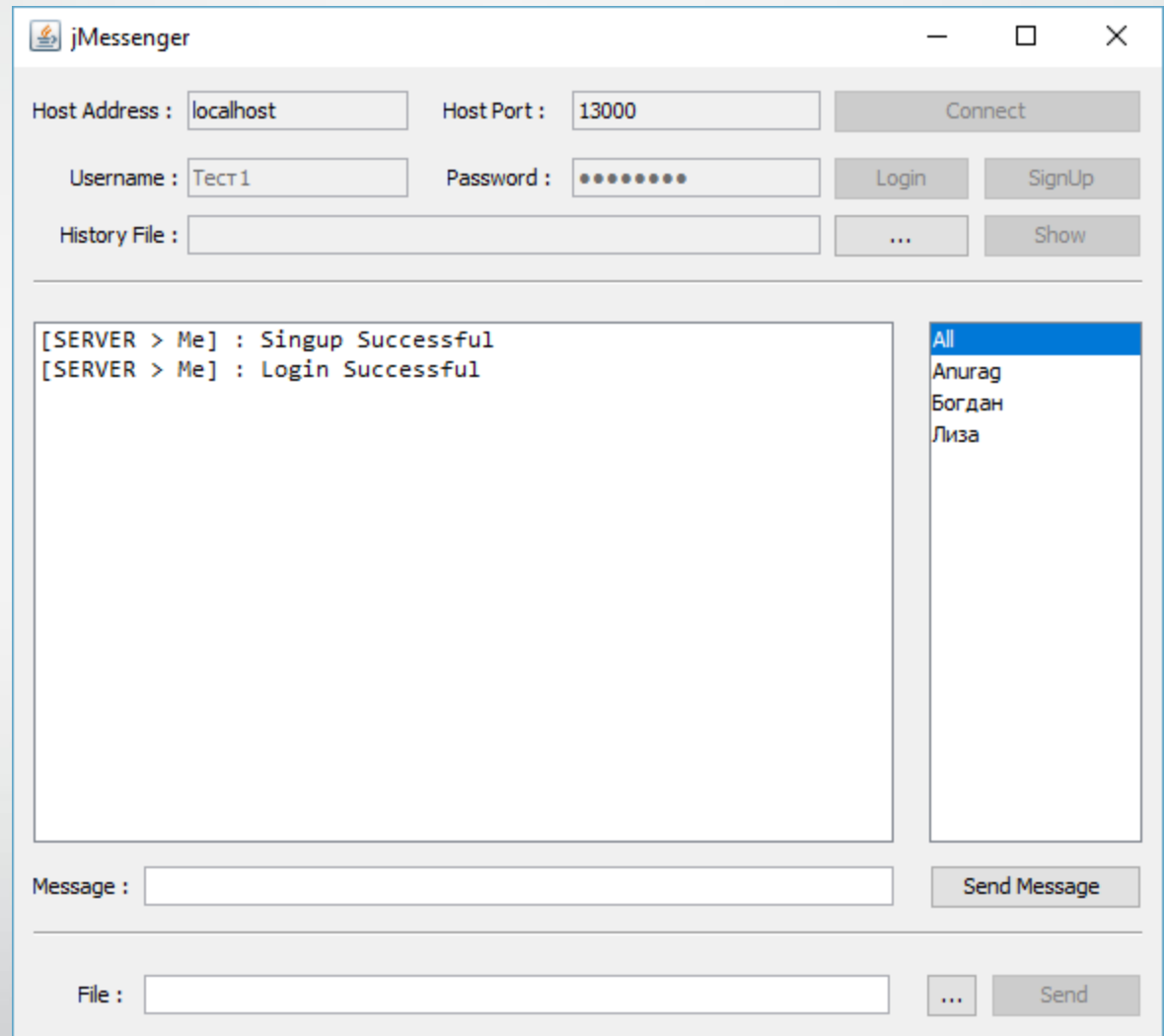
- ChatFrame
- SocketClient
- HistoryFrame
- History
- Message
- Upload
- Download



Запуск
серверу



Підключення
користувача
до серверу



The screenshot shows the jMessenger application window. The title bar reads "jMessenger". The interface includes several input fields and buttons:

- Host Address:** localhost
- Host Port:** 13000
- Connect** button
- Username:** Тест1
- Password:** masked with dots
- Login** button
- SignUp** button
- History File:** (empty)
- ...** button
- Show** button

The main chat area displays the following messages:

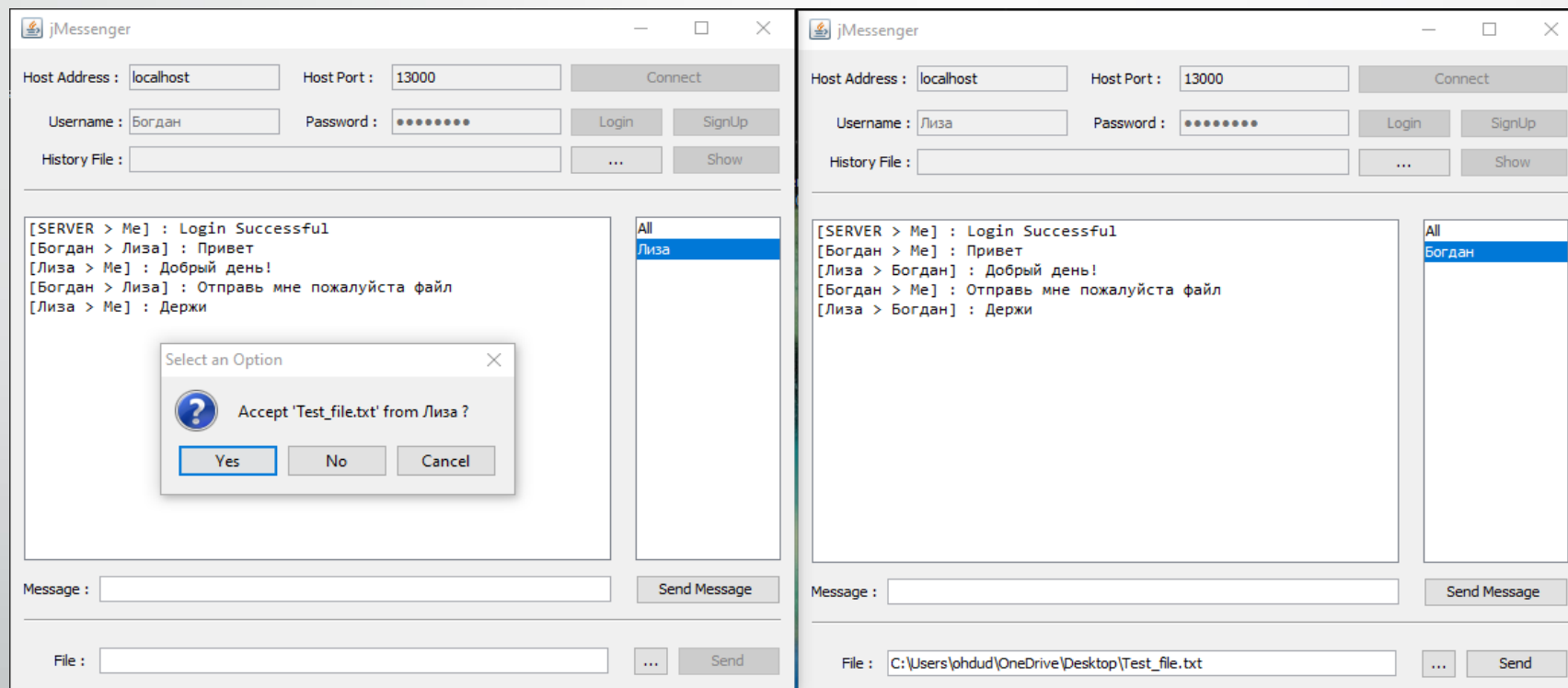
```
[SERVER > Me] : Singup Successful  
[SERVER > Me] : Login Successful
```

On the right side, there is a list of users:

- All
- Anurag
- Богдан
- Лиза

At the bottom, there is a **Message :** input field and a **Send Message** button. Below that is a **File :** input field, a **...** button, and a **Send** button.

Фрагмент діалогу



Висновки:

- Детально розглянуті існуючі методи шифрування повідомлень, порівняні існуючі методи з метою виявлення недоліків і переваг кожного з них;
- Проведено аналіз існуючих методів хешування паролів. Досліджені способи злому хешей. Проведено аналіз технологій та методів розробки.
- У проектному розділі були виконані розробку бази даних, з описом усіх таблиць і їх призначення, розроблено інтерфейс, створений власний алгоритм шифрування, спроектовано серверну і клієнтську частину веб-сервісу.



Дякую за увагу