Попович Ярослав

РОЗРОБКА СИСТЕМИ ШИФРУВАННЯ В ХМАРНИХ СХОВИЩАХ ДАНИХ

Актуальність

- Військова справа
- Захист персональних даних
- Відправлення файлів великого розміру
- Захищений обмін даними через гугл диск

Існуючі алгоритми

Шифр Віженера

Шифр Вернама

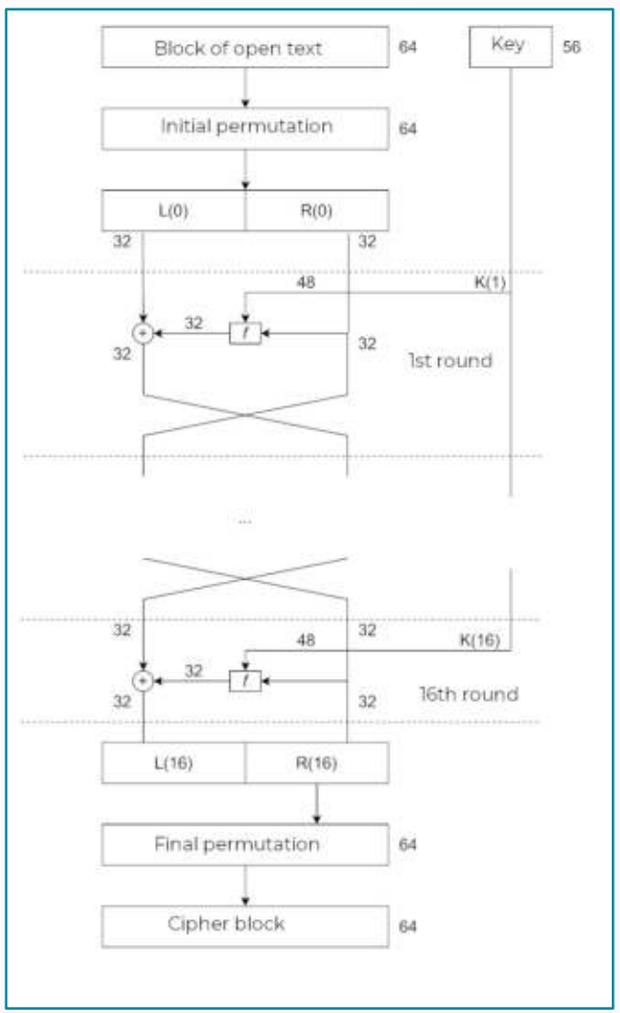
A - 000000 K - 001010 U - 010100 5 - 011110
B - 000001 L - 001011 V - 010101 6 - 011110
C - 000010 M - 001100 W - 010110 7 - 011111
D - 000011 N - 001101 X - 010111 8 - 100000
E - 000100 O - 001110 Y - 011000 9 - 100001
F - 000101 P - 001111 Z - 011001 0 - 100010
G - 000110 Q - 010000 1 - 011010 . - 100011
H - 000111 R - 010001 2 - 011011 , - 100100
I - 001000 S - 010010 3 - 011100 ? - 100101
J - 001001 T - 010011 4 - 011101 - 100110

open text: HI GUYS.

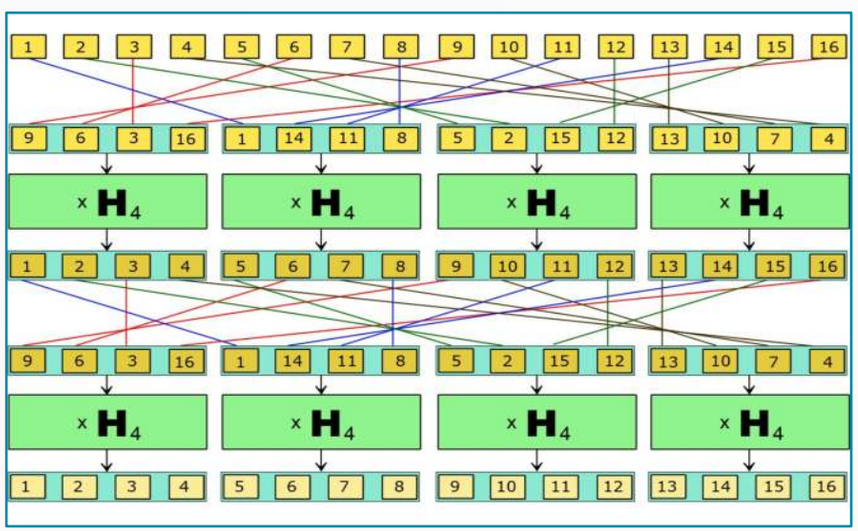
000111 - 001000 - 100110 - 000110 - 010100 - 011000 - 010010 - 100011
011000 - 011011 - 010011 - 000010 - 000101 - 011000 - 010011 - 001010

011111 - 010011 - 110101 - 000100 - 010001 - 000000 - 000001 - 101001

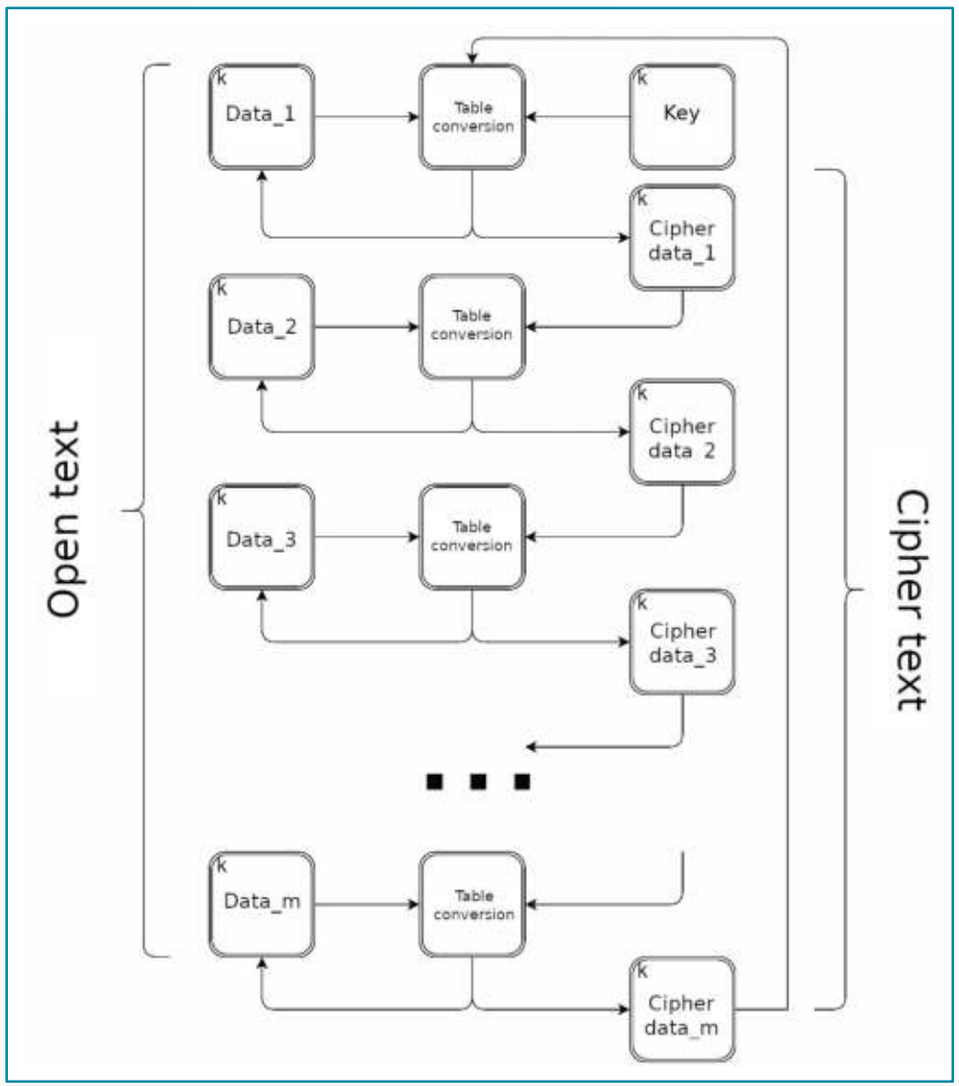
Шифр DES



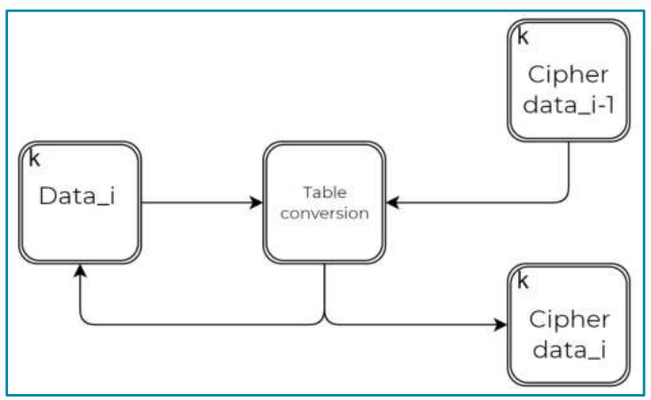
Шифр SAFER



Розроблений алгоритм



Block of data contained with k symbols



Encrypting Data_i using Vigenere's cipher with Cipher data_i-1 as initialization vector where answer writes in Data_i and Cipher data_i

Кількість раундів

Час роботи програми залежить від кількості раундів:

- Чим більша їх кількість, тим довше працює програма
- Чим вона менша, тим швидше працює програма

Порівняння шифрів

Шифри	Час роботи	Переваги та недоліки
Шифр Віженера	$O(n)$	Може бути дешифрованим
Шифр Вєрнама	$O(nk)$	Абсолютно криптостійкий
DES	$O(n^2)$	Гарно працює на малих рядках
SAFER	$O(n)$	Може бути дешифрованим
Розроблений шифр	$O(nc)$	Час роботи і криптостійкість залежить від кількості раундів

n – довжина рядка
k – час генерації випадкового числа
c – кількість раундів

Час роботи розробленого шифру

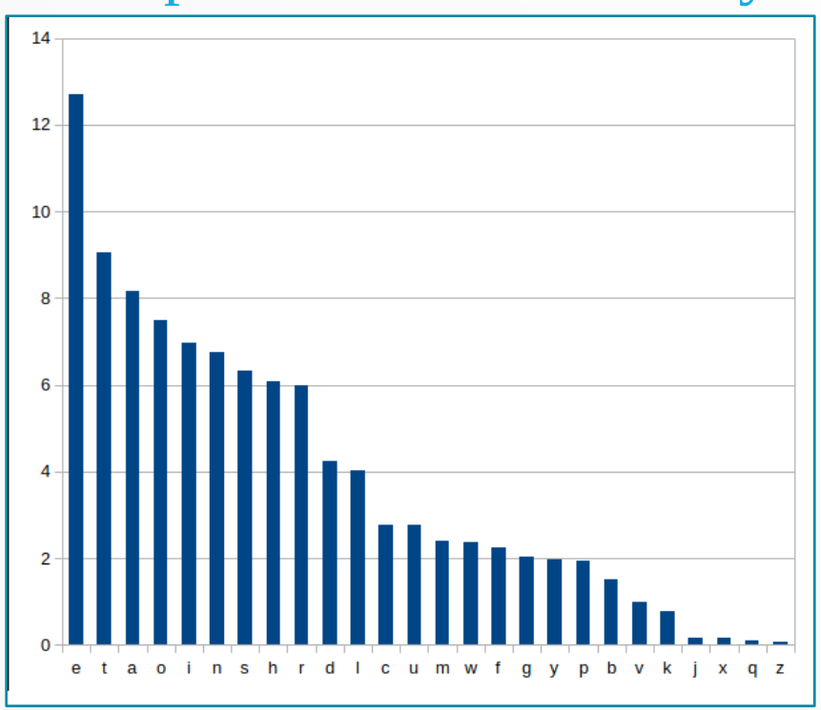
	1 раунд	10 раундів	100 раундів
1000 символів	0.0009973 sec.	0.00498 sec.	0.0428 sec.
10000 символів	0.0079779 sec.	0.04985 sec.	0.4363 sec.
100000 символів	0.0797855 sec.	0.48044 sec.	4.4514 sec.
1000000 символів	0.7979397 sec.	4.96143 sec.	48.784 sec.

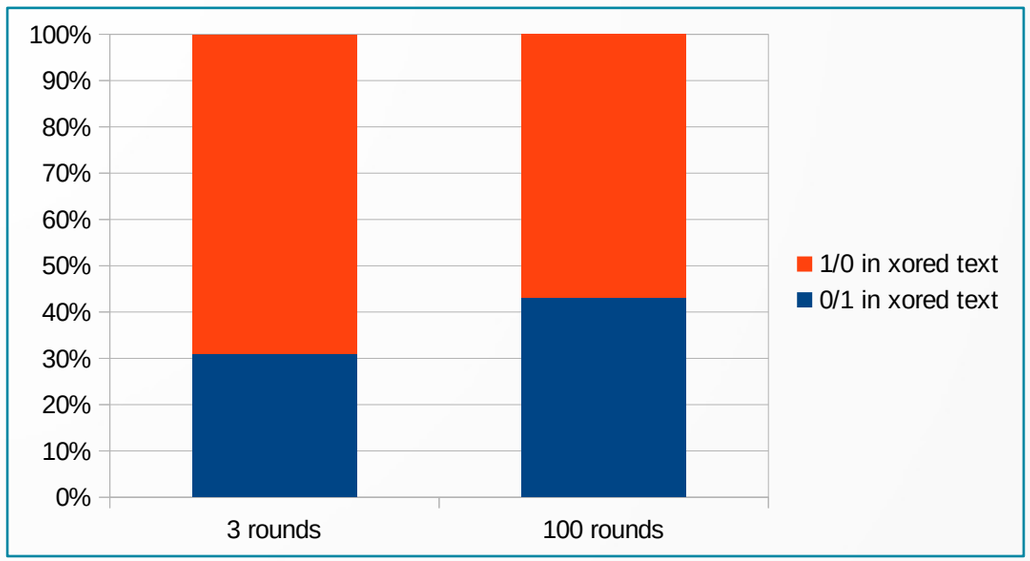
Криптоаналіз

Формула для розрохунку криптостійкості

$$P_{i_1} \otimes P_{i_2} \otimes P_{i_3} \otimes \ldots \otimes P_{i_a} \otimes C_{j_1} \otimes C_{j_2} \otimes C_{j_3} \otimes \ldots \otimes C_{j_b} = K_{k_1} \otimes K_{k_2} \otimes K_{k_3} \ldots \otimes K_{k_c}$$

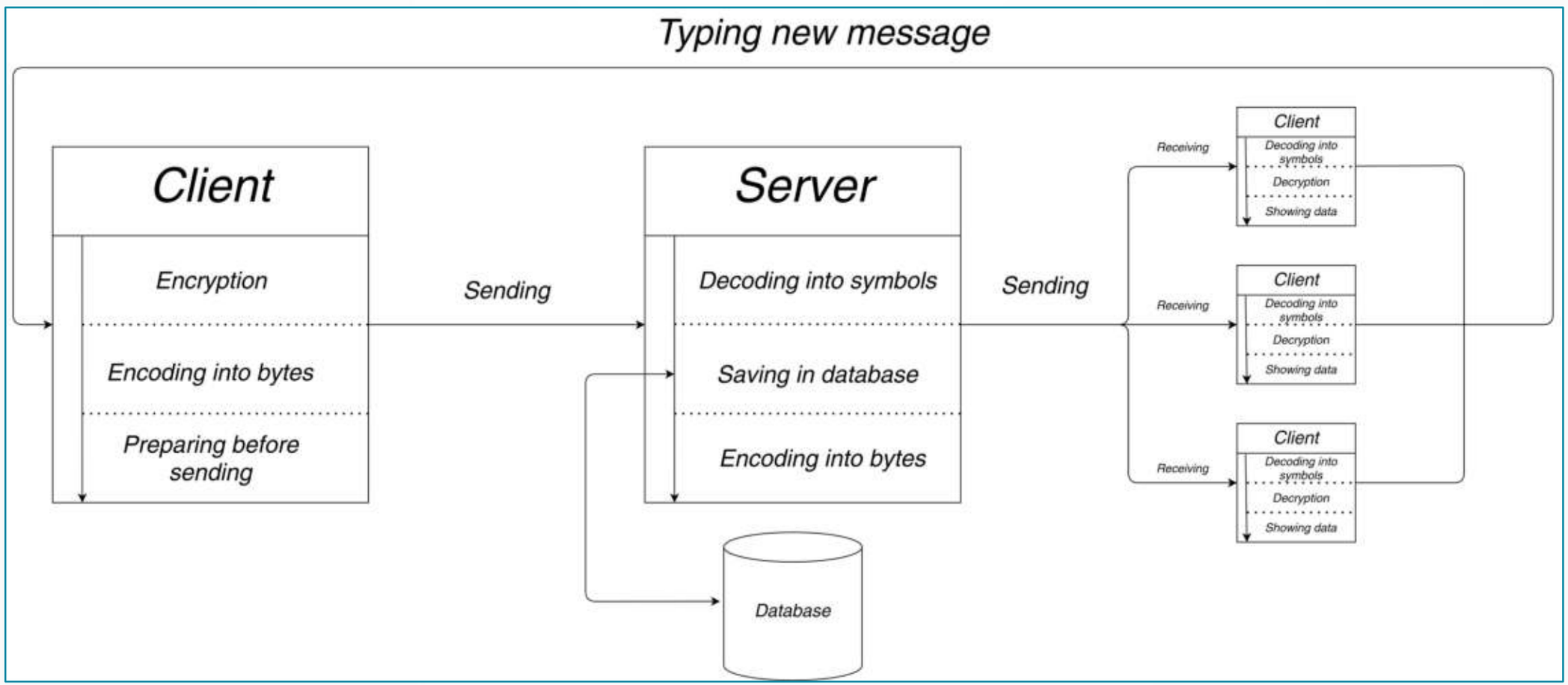
Ймовірність появи символу в тексті.





При збільшенні кількості раундів, криптостійкість зростає, але робити більше 100-1000 раундів немає сенсу, бо криптостійкість буде змінюватись не суттєво.

Принцип роботи консольного чату



Приклад роботи консольного чату

Приєднання до потрібного серверу та встановлення свого імені

```
ip: 192.168.0.106
Type your nickname: Abraham
Enter group's secret key: ?open
Choose group name: MyGroup
Sending info...
Receiving info...
[GROUP MyGroup HAS BEEN CREATED]
Enter group's secret key: MyGroup
[TRYING TO ENTER GROUP: MyGroup]
=> [MyGroup]=>[Hector]=> has joined the chat.
=> [MyGroup]=>[Hector]=> Hello
=> Hi
=> Hector disconnected the server.
=> [EXITTING FROM THE CHAT...]
Enter group's secret key: GroupName2
[TRYING TO ENTER GROUP: GroupName2]
=> Ohh...
=> Hector disconnected the server.
=>
```

```
ip: 192.168.0.106
Type your nickname: Hector
Enter group's secret key: ?open
Choose group name: GroupName2
Sending info...
Receiving info...
[GROUP GroupName2 HAS BEEN CREATED]
Enter group's secret key: MyGroup
[TRYING TO ENTER GROUP: MyGroup]
=> Hello
=> [MyGroup]=>[Abraham]=> Hi
=> [EXITTING FROM THE CHAT...]
Enter group's secret key: GroupName2
[TRYING TO ENTER GROUP: GroupName2]
=> [GroupName2]=>[John]=> has joined the chat.
=> [GroupName2]=>[John]=> What's up?
=> Ok!
=> [GroupName2]=>[Abraham]=> has joined the chat.
=> [GroupName2]=>[Abraham]=> Ohh...
=> [EXITTING FROM THE CHAT...]
Enter group's secret key:
```

Створення групи

Open text	Passphrase	Rounds	Cipher text
Hello, my name is Sam. login - admin, password - admin	secret pass	100	VcPkh.f8A3O&#4GU-4#y.qg6H1+ZH4*&VoUv6lPHSV%*8-sqQt%e&URg

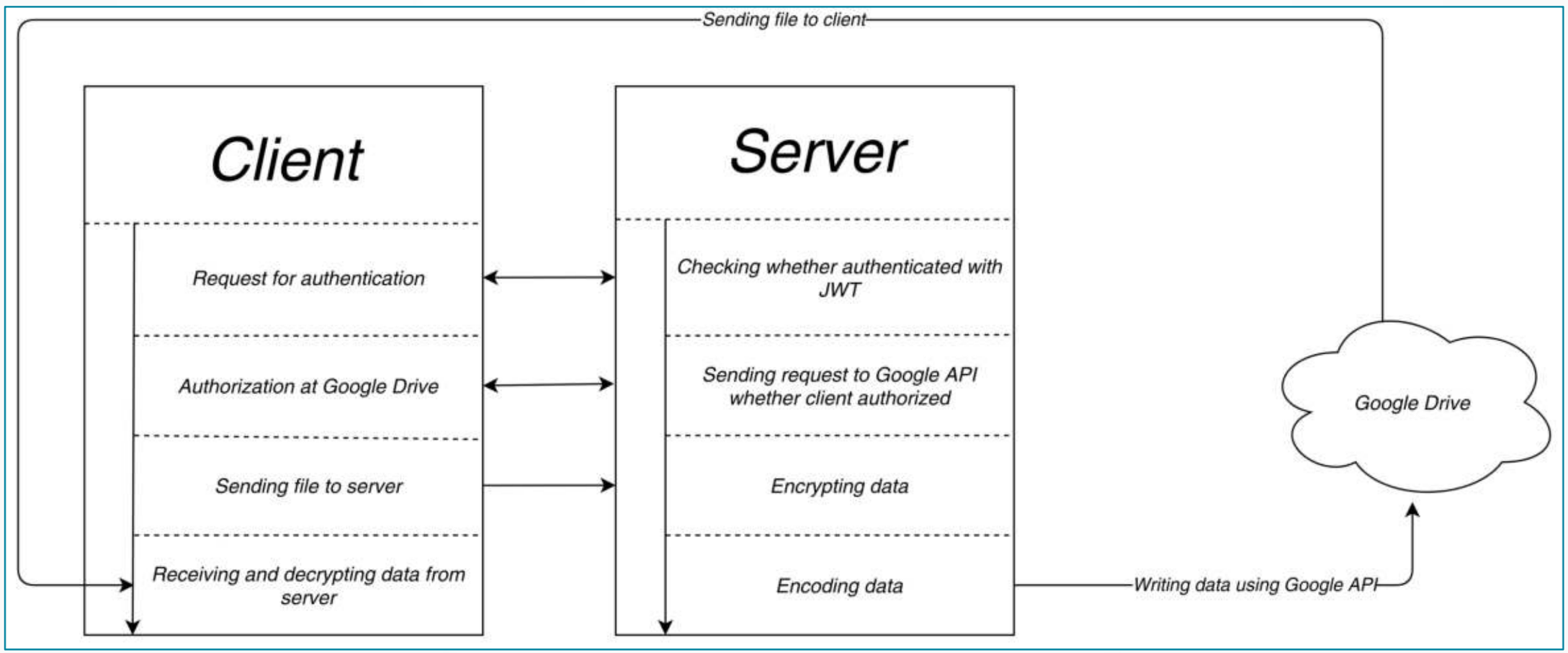
Вихід та вхід учасника з бесіди

```
ip: 192.168.0.106
Type your nickname: John
Enter group's secret key: GroupName2
[TRYING TO ENTER GROUP: GroupName2]
=> What's up?
=> [GroupName2]=>[Hector]=> Ok!
=> [GroupName2]=>[Abraham]=> has joined the chat.
=> [GroupName2]=>[Abraham]=> Ohh...
=> Hector disconnected the server.
=>
```

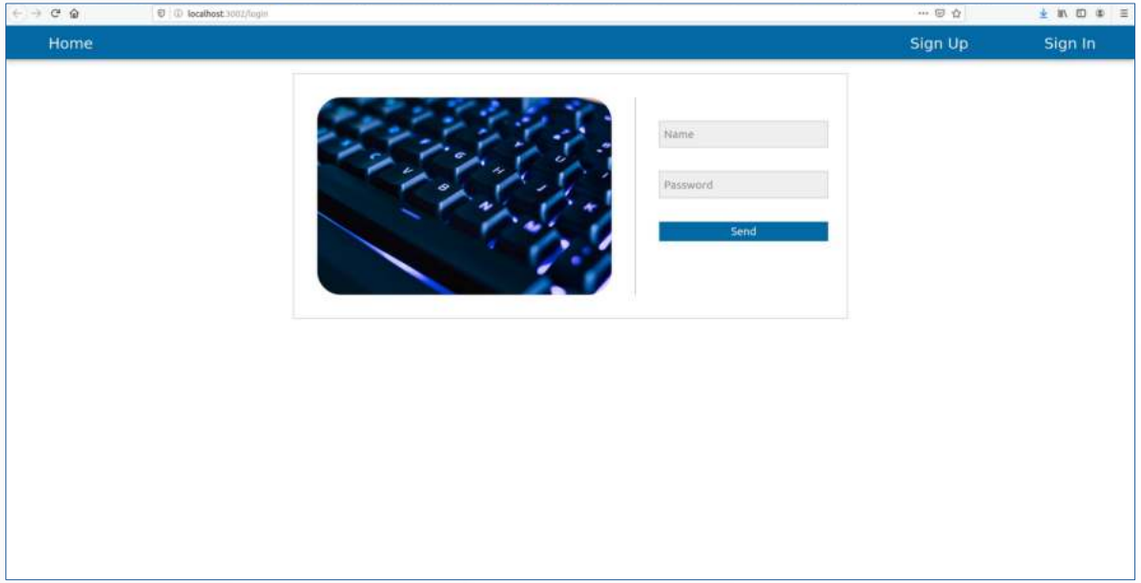
Приєднання до групи

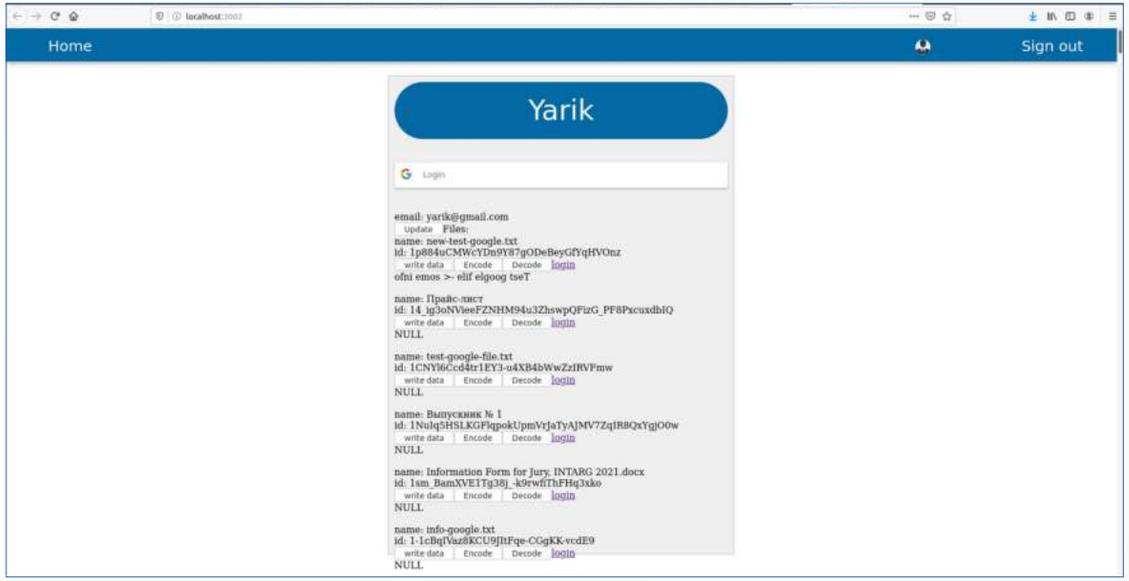
Github

Принцип роботи сайту-програми



Github


localhost:3002/login
Home
Sign Up
Sign In
Name
Password
Send


localhost:3002
Home
Sign out
Yarik
Login
email: yarik@gmail.com
Update Files:
name: new-test-google.txt
id: 1p884uCMWcYDn9Y87gODeBeyGfYqHVOnz
write data Encode Decode login
ofni emos >- elif elgoog tseT
name: Прайс-лист
id: 14_ig3oNVieeFZNHM94u3ZhswpQFizG_PF8PxcuxdbIQ
write data Encode Decode login
NULL
name: test-google-file.txt
id: 1CNYl6Ccd4tr1EY3-u4XB4bWwZzIRVFmw
write data Encode Decode login
NULL
name: Выпускник № 1
id: 1Nulq5HSLKGFlqpokUpmVrJaTyAJMV7ZqIR8QxYgjO0w
write data Encode Decode login
NULL
name: Information Form for Jury, INTARG 2021.docx
id: 1sm_BamXVE1Tg38j_-k9rwfiThFHq3xko
write data Encode Decode login
NULL
name: info-google.txt
id: 1-1cBqlVaz8KCU9JItFqe-CGgKK-vcdE9
write data Encode Decode login
NULL

Висновки

Для зберігання файлів великого розміру на хмарних сховищах даних краще всього себе продемонстрував саме розроблений шифр, через можливість керування часом роботи алгоритму і його криптостійкістю. Даний алгоритм має більш надійну криптостійкість порівняно з шифром Віженера, не потребує генерації великої кількості випадкових чисел, як шифр Вєрнама, та працює набагато швидше за шифр DES.

ДЯКУЮ ЗА УВАГУ