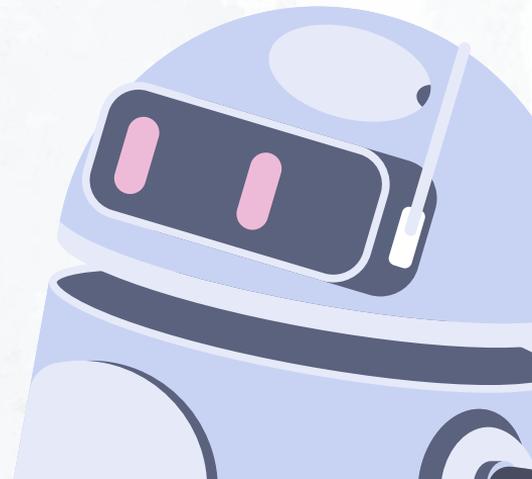


Организация информационной безопасности корпоративной сети



Выполнил: Шорец Д.И.
Руководитель: Лукьяненко А.Г.

Омск 2023



Цели и задачи

Цель: Создание мессенджера для корпоративной сети компании “Круг”

Задачи:

- 1) Анализ рынка программных средств передачи информации;
- 2) Выбор протокола передачи информации;
- 3) Описание функций мессенджера;
- 4) Создание клиент – серверного приложения.



Анализ рынка программных средств передачи информации



Briar



Telegram



Threema



Wickr



WhatsApp

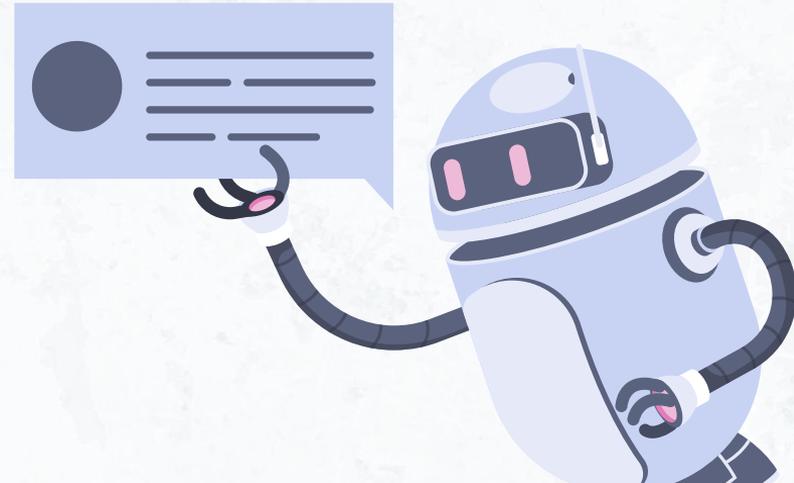


Viber

Выбор протокола передачи информации

Причины по которым был выбран AES:

- 1)Безопасность: AES обеспечивает высокий уровень безопасности и считается криптографически стойким;
- 2)Производительность: AES является эффективным и быстрым алгоритмом шифрования;
- 3)Ключевая длина: AES позволяет использовать ключи различной длины, включая 128, 192 и 256 бит.



Описание принципа работы протокола

Основные шаги при работе протокола:

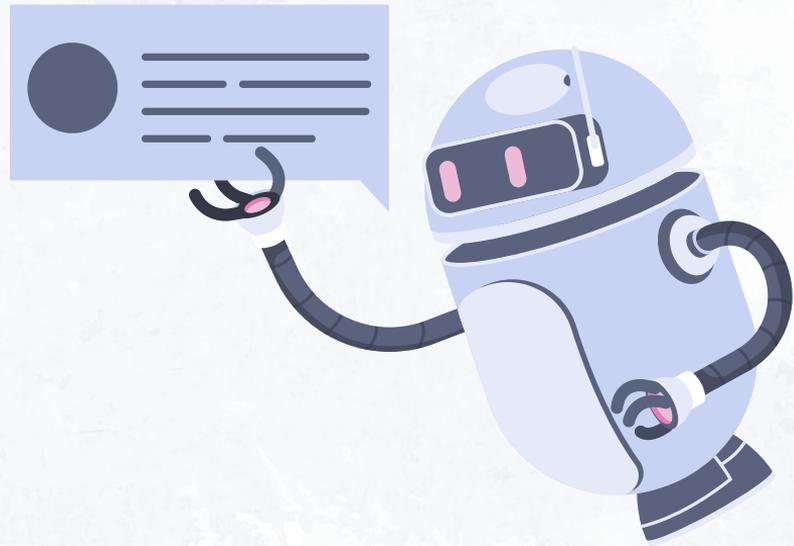
- 1) Инициализация: В начале протокола AES выбирается ключ шифрования;
- 2) Расширение ключа: из выбранного ключа шифрования создается расширенный ключ;
- 3) Шифрование: Данные разбиваются на блоки фиксированного размера.



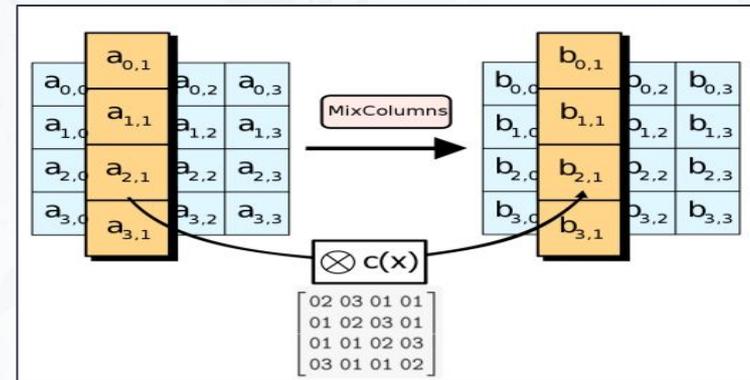
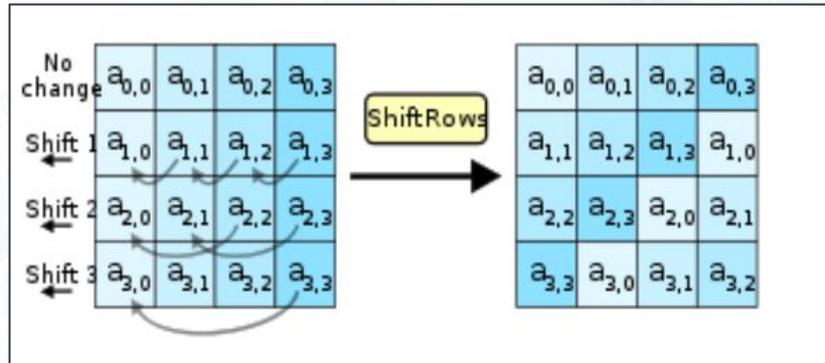
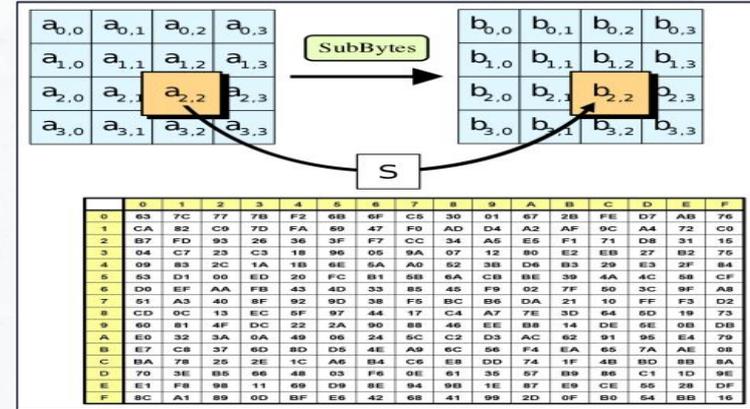
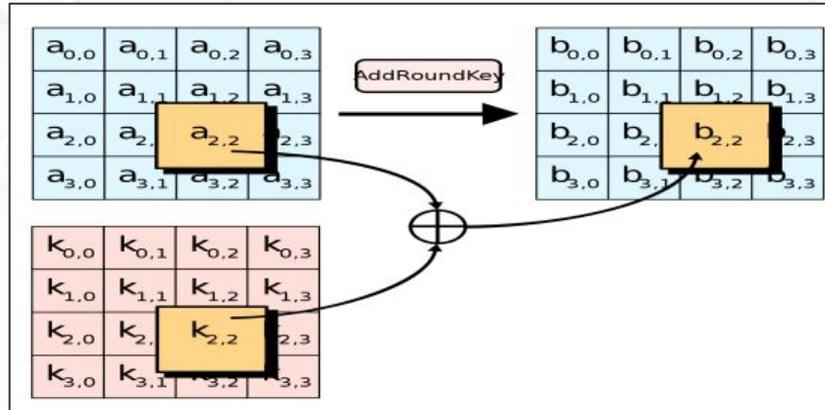
Описание принципа работы протокола

В процессе шифрования данные разбиваются на блоки, и каждый блок подвергается серии шифровательных раундов:

- 1)AddRoundKey;
- 2)SubBytes;
- 3)ShiftRows;
- 4)MixColumns.



Описание принципа работы протокола



Описание функций и интерфейса мессенджера

Функции:

- 1) Отправка текстовых сообщений:
основная функция мессенджера
- 2) Групповые чаты: предоставляется
возможность создавать и участвовать в
групповых чатах
- 3) Шифрование в мессенджере создаются
комнаты для предотвращения
подслушивания и случайного
проникновения

Интерфейс:

 C:\Windows\py.exe

```
[+] Client Running
[+] Enter Destination IP   : 127.0.0.1
[+] Enter Destination Port : 5555
[+] AES Pre-Shared-Key For Connection :1111_
```

Тестирование безопасности передачи данных

Для тестирования безопасности было использовано ПО “WireShark”

The screenshot displays a network traffic capture in Wireshark. The top pane shows a list of packets, with packet 161 selected. The middle pane shows the details of the selected packet, including Ethernet II, Internet Protocol Version 4, and Transmission Control Protocol. The bottom pane shows the raw data of the packet in hexadecimal and ASCII format.

No.	Time	Source	Destination	Protocol	Length	Info
160	8.046456	127.0.0.1	127.0.0.1	TCP	44	49432 → 49152 [ACK] Seq=1211 Ack=3706 Win=10136 Len=0
161	8.315470	192.168.0.164	192.168.0.164	TCP	172	9999 → 50106 [PSH, ACK] Seq=1 Ack=1 Win=10232 Len=128
162	8.315503	192.168.0.164	192.168.0.164	TCP	44	50106 → 9999 [ACK] Seq=1 Ack=129 Win=10232 Len=0
163	10.054256	127.0.0.1	127.0.0.1	TCP	106	49432 → 49152 [PSH, ACK] Seq=1211 Ack=3706 Win=10136 Len=62
164	10.054283	127.0.0.1	127.0.0.1	TCP	44	49152 → 49432 [ACK] Seq=3706 Ack=1273 Win=9996 Len=0
165	10.054296	127.0.0.1	127.0.0.1	TCP	45	49432 → 49152 [PSH, ACK] Seq=1273 Ack=3706 Win=10136 Len=1
166	10.054304	127.0.0.1	127.0.0.1	TCP	44	49152 → 49432 [ACK] Seq=3706 Ack=1274 Win=9996 Len=0
167	10.054573	127.0.0.1	127.0.0.1	TCP	134	49152 → 49432 [PSH, ACK] Seq=3706 Ack=1274 Win=9996 Len=90
168	10.054591	127.0.0.1	127.0.0.1	TCP	44	49432 → 49152 [ACK] Seq=1274 Ack=3796 Win=10136 Len=0
169	10.054604	127.0.0.1	127.0.0.1	TCP	45	49152 → 49432 [PSH, ACK] Seq=3796 Ack=1274 Win=9996 Len=1
170	10.054613	127.0.0.1	127.0.0.1	TCP	44	49432 → 49152 [ACK] Seq=1274 Ack=3797 Win=10136 Len=0
171	10.054629	127.0.0.1	127.0.0.1	TCP	102	49432 → 49152 [PSH, ACK] Seq=1274 Ack=3797 Win=10136 Len=58
172	10.054640	127.0.0.1	127.0.0.1	TCP	44	49152 → 49432 [ACK] Seq=3797 Ack=1332 Win=9996 Len=0
173	10.054649	127.0.0.1	127.0.0.1	TCP	45	49432 → 49152 [PSH, ACK] Seq=1332 Ack=3797 Win=10136 Len=1
174	10.054656	127.0.0.1	127.0.0.1	TCP	44	49152 → 49432 [ACK] Seq=3797 Ack=1333 Win=9996 Len=0
175	10.054933	127.0.0.1	127.0.0.1	TCP	407	49152 → 49432 [PSH, ACK] Seq=3797 Ack=1333 Win=9996 Len=363

Frame 161: 172 bytes on wire (1376 bits), 172 bytes captured (1376 bits) on interface \Device\NPF_{Loopback}, id 0

- Null/Loopback
- Internet Protocol Version 4, Src: 192.168.0.164, Dst: 192.168.0.164
- Transmission Control Protocol, Src Port: 9999, Dst Port: 50106, Seq: 1, Ack: 1, Len: 128
- Data (128 bytes)

Data: 3ab159a336da7ae5fe85d69410fd8922309b053e0de55ea5e91496ce350a03af00293575...
[Length: 128]

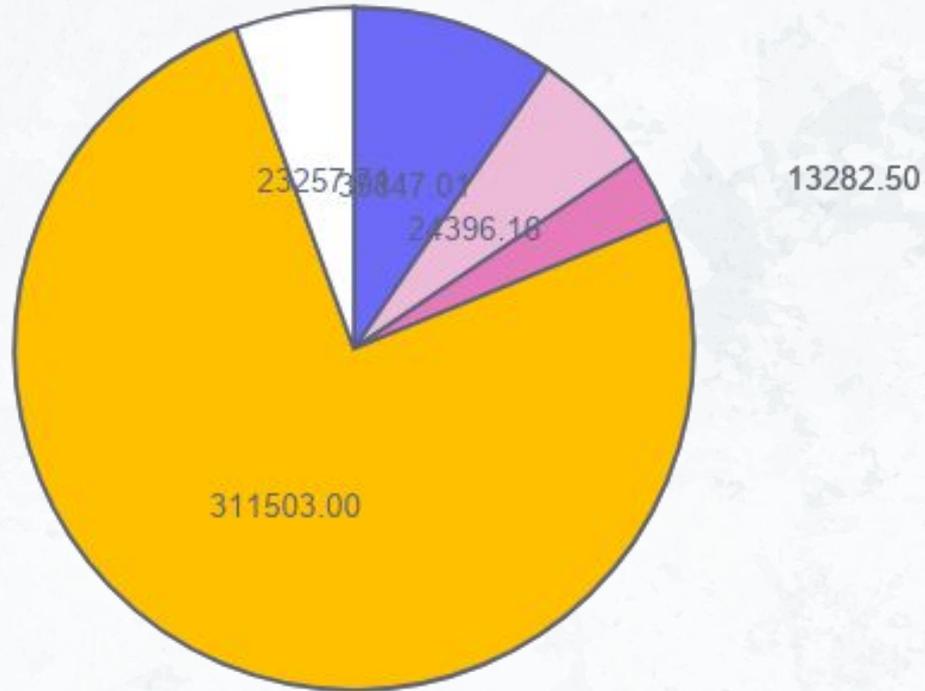
```
0000 02 00 00 00 45 00 00 a8 e3 90 40 00 80 06 00 00  ....E....@.....
0010 c0 a8 00 a4 c0 a8 00 a4 27 0f c3 ba 2b 1f b9 68  .........'+.h
0020 f5 11 a0 ca 50 18 27 f8 02 7f 00 00 3a b1 59 a3  ....P.....Y.
0030 36 da 7a e5 fe 85 d6 94 10 fd 89 22 30 9b 05 3e  6-z....."0->
0040 04 e5 5e a5 e9 14 96 ce 35 0a 03 af 00 29 35 75  ..~.....5...)5u
0050 e1 e8 08 d2 03 76 f2 96 b3 ba 66 3c e9 1c b8 6f  ....v.....f<...c
0060 63 0d da 77 68 49 d2 8d 89 2f 56 e0 8f 6f 12 63  c..whI.../V.o.c
0070 66 9a 27 3a 07 61 44 f1 16 3b 32 a2 b5 42 49 71  f.'aD..;2..BIc
0080 fb 10 22 48 92 6c 23 52 92 9c 7c b4 cd b4 e3 aa  .."H.I#R..|...
0090 60 8a 6e ae 6a e7 9c 0e a0 3b 56 d6 35 c3 5b 1a  ~n-j....;V.5.[
00a0 b7 9e 9d ed 19 eb 53 44 05 16 e5 25  .......S0....
```

Экономическая часть

Наименование статьи затрат	Буквенное обозначение	Сумма, руб.
1. Затраты на проектирование и документацию	ВПД	39 847,01
2. Затраты на разработку	ВРП	24 396,19
3. Затраты на тестирование безопасности	ВТБ	13 282,5
4. Материальные затраты	Зоб	311 503
5. Затраты на страховые взносы	СВ	23 257,71
Всего затрат на создание СКСБ		412 286,41

Диаграмма затрат

Сумма



■ ВПД ■ ВРП ■ ВТБ ■ Зоб ■ СВ