Номер зачетки: 1800189

1. создать текстовый файл с вашим ФИО

```
taiiiga@raw:~$ cat > fullname
Khisamov Iskander Ravilevich
^Z
[1]+  Stopped                 cat > fullname
taiiiga@raw:~$ cat fullname
Khisamov Iskander Ravilevich
```

2. зашифровать и расшифровать созданный текстовый файл используя "пароль", различными алгоритмами симметричного шифрования (минимум 3 алгоритма: des-cfb, rc2-ecb, aes-256-cfb)

```
taiiiga@raw:~$ openssl enc -des-cfb -in fullname -out coded -iter 10000
enter des-cfb encryption password:
Verifying - enter des-cfb encryption password:
taiiiga@raw:~$ cat coded
D◆e@◆#__◆◆$◆0◆
      .◆U       8◆◆◆`Y◆◆ь◆◆taiiiga@raw:~$
taiiiga@raw:~$ openssl enc -des-cfb -d -in coded -out decoded -iter 10000
enter des-cfb decryption password:
taiiiga@raw:~$ cat decoded
Khisamov Iskander Ravilevich
```

```
taiiiga@raw:~$ openssl enc -rc2-ecb -in fullname -out coded -iter 10000
enter rc2-ecb encryption password:
Verifying - enter rc2-ecb encryption password:
taiiiga@raw:~$ cat coded
Salted__◆◆KLI3◆◆k} ◆>    ◆E◆+◆`=◆◆◆◆◆◆k◆◆◆◆◆Q◆ٱtaiiiga@raw:~$
taiiiga@raw:~$ openssl enc -rc2-ecb -d -in coded -out decoded -iter 10000
enter rc2-ecb decryption password:
taiiiga@raw:~$ cat decoded
Khisamov Iskander Ravilevich
```

```
taiiiga@raw:~$ openssl enc -aes-256-cfb -in fullname -out coded -iter 10000
enter aes-256-cfb encryption password:
Verifying - enter aes-256-cfb encryption password:
taiiiga@raw:~$ cat coded
Salted__'◆
          ◆◆R◆◆|◆4◆◆(◆◆◆◆◆◆◆Sk◆>◆◆"◆@◆>]taiiiga@raw:~$
taiiiga@raw:~$ openssl enc -aes-256-cfb -d -in coded -out decoded -iter 10000
enter aes-256-cfb decryption password:
taiiiga@raw:~$ cat decoded
Khisamov Iskander Ravilevich
```

3. попробовать расшифровать файл другим "паролем" и измененный зашифрованный файл

```
taiiiga@raw:~$ openssl enc -aes-256-cfb -d -in coded -out decoded -iter 10000
enter aes-256-cfb decryption password:
taiiiga@raw:~$ cat decoded
Khisamov Iskander Ravilevich
taiiiga@raw:~$ openssl enc -aes-256-cfb -d -in coded -out decoded -iter 10000
enter aes-256-cfb decryption password:
taiiiga@raw:~$ cat decoded

◆◆>◆◆y◆P
        d>9\◆◆◆67{◆Y◆◆[taiiiga@raw:~$
```

```
taiiiga@raw:~$ openssl enc -aes-256-cfb -in fullname -out coded -iter 10000
enter aes-256-cfb encryption password:
Verifying - enter aes-256-cfb encryption password:
taiiiga@raw:~$ cat coded
Salted__Vo◆+◆\◆◆◆◆(◆◆
                    EIt,zV◆    ◆F◆◆9◆◆گtaiiiga@raw:~$ echo 'text' >> coded
taiiiga@raw:~$ cat coded
Salted__Vo◆+◆\◆◆◆◆(◆◆
                    EIt,zV◆    ◆F◆◆9◆◆گtext
taiiiga@raw:~$ openssl enc -aes-256-cfb -d -in coded -out decoded -iter 10000
enter aes-256-cfb decryption password:
taiiiga@raw:~$ cat decoded
Khisamov Iskander Ravilevich
◆6◆◆wtaiiiga@raw:~$
```

4. сгенерируйте симметричный ключ с помощью openssl rand (закодируйте в base64), длина ключа = 189, проделайте 1-2 задания с этим ключом

```
taiiiga@raw:~$ openssl rand -base64 189 > key
taiiiga@raw:~$ cat key
93JMtuQ7QAwJ4/x4wMZoVEXsQITxJoAqpjAAHCrUN8EmiMlQceQpNWM6Dig94pTT
cL5mNJQ21u6sJit3HQBuQIT1Za+6UxxCcOu1lAX1HTHFus/wDTyONA+NVLCXzOEr
EIs/a6BDOxzzZEAHN9CT0VH8YdUv9ILLuu+mS7KnTMbhJq4O2TIz53a4J42Djssh
9FjSDvj9nDl67Zc+bA/EGzv6e42GvRw2sLNBEZ7vvOI95qiLVkLGGA0kAwXZ
taiiiga@raw:~$ openssl enc -des-cfb -in fullname -out coded -pass file:./key -iter 10000
taiiiga@raw:~$ cat coded
Salted__W@BFli◆"<◆q◆<)m◆◆]◆Uj◆◆◆◆_Yw◆taiiiga@raw:~$
taiiiga@raw:~$ openssl enc -des-cfb -d -in coded -out decoded -pass file:./key -iter 10000
taiiiga@raw:~$ cat decoded
Khisamov Iskander Ravilevich
```

```
taiiiga@raw:~$ openssl rand -base64 189 > key
taiiiga@raw:~$ cat key
/3bKAKMSADts1PaLa1r/8N159G8VaJZHBOoqXstXAggpsgaz6beIa95l9+NEOfqe
lRu1QmLveO9fviW8wwwuJ2QtRq+IRHnMprkV8lgLGnkDCyxZwkNmNj81xB2cAT8H
uMXQApFpUf0Ggt/xFAJ+ixOa2StTI2521t8cJ57O1o3VLLE1FrzJtPEchIZs64sW
+HQMmqZ30pS1/GVxw1IbzzCpunPlzg83s9B6nZEqDCGv4LVpW2eWVkmEF/lE
taiiiga@raw:~$ openssl enc -rc2-ecb -in fullname -out coded -pass file:./key -iter 10000
taiiiga@raw:~$ cat coded
Salted__◆◆hE} ◆◆GE◆{◆k◆◆LL◆◆nxC◆◆◆◆rT◆◆C<\◆◆@X◆taiiiga@raw:~$
taiiiga@raw:~$ openssl enc -rc2-ecb -d -in coded -out decoded -pass file:./key -iter 10000
taiiiga@raw:~$ cat decoded
Khisamov Iskander Ravilevich
```

```
taiiiga@raw:~$ openssl rand -base64 189 > key
taiiiga@raw:~$ cat key
mDPVlWTYHWQPnOrZIlrhlUO8ZYreexo+/jBABbA6+xRMLIUHW66ZJ844glmdOZY/
iPUKp17vGyzwHAjE1yGe/0hTMbF3oCfPsXv2hBfFYlkQWBuPPSZNWvvzN08ciSpk
6kHbdJ67Vs05ZIxozVpJB4yrCVT6z6qKN9y/FqPjXgwXJxy5NEtt8xpIaLH2qGk7
xa22bd0YwptoP7CpnZnyTXzKcRaMPkwWihkVIdAb4ybAkBHQRSusGAzoShVm
taiiiga@raw:~$ openssl enc -aes-256-cfb -in fullname -out coded -pass file:./key -iter 10000
taiiiga@raw:~$ cat coded
Salted__pIŐo%◆l◆◆◆:◆v◆V◆]yEsfK◆◆◆+◆s◆◆◆taiiiga@raw:~$
taiiiga@raw:~$ openssl enc -aes-256-cfb -d -in coded -out decoded -pass file:./key -iter 10000
taiiiga@raw:~$ cat decoded
Khisamov Iskander Ravilevich
```

5. Таким же способом сгенерируйте матрицу симметричных ключей для 12 абонентов криптосети

- имя файла ключа должно содержать номер серии (номер криптосети, тоже 9)
- имя файла ключа должно содержать номера соответствующих абонентов

```
taiiiga@raw:/media/sf_Virtual/cryptonet/1$ openssl rand -base64 189 > 9.12
taiiiga@raw:/media/sf_Virtual/cryptonet/1$ openssl rand -base64 189 > 9.13
taiiiga@raw:/media/sf_Virtual/cryptonet/1$ openssl rand -base64 189 > 9.14
taiiiga@raw:/media/sf_Virtual/cryptonet/1$ openssl rand -base64 189 > 9.15
taiiiga@raw:/media/sf_Virtual/cryptonet/1$ openssl rand -base64 189 > 9.16
taiiiga@raw:/media/sf_Virtual/cryptonet/1$ openssl rand -base64 189 > 9.17
taiiiga@raw:/media/sf_Virtual/cryptonet/1$ openssl rand -base64 189 > 9.18
taiiiga@raw:/media/sf_Virtual/cryptonet/1$ openssl rand -base64 189 > 9.19
taiiiga@raw:/media/sf_Virtual/cryptonet/1$ openssl rand -base64 189 > 9.110
taiiiga@raw:/media/sf_Virtual/cryptonet/1$ openssl rand -base64 189 > 9.111
taiiiga@raw:/media/sf_Virtual/cryptonet/1$ openssl rand -base64 189 > 9.112
```

```
taiiiga@raw:/media/sf_Virtual/cryptonet/2$ openssl rand -base64 189 > 9.21
taiiiga@raw:/media/sf_Virtual/cryptonet/2$ openssl rand -base64 189 > 9.23
taiiiga@raw:/media/sf_Virtual/cryptonet/2$ openssl rand -base64 189 > 9.24
taiiiga@raw:/media/sf_Virtual/cryptonet/2$ openssl rand -base64 189 > 9.25
taiiiga@raw:/media/sf_Virtual/cryptonet/2$ openssl rand -base64 189 > 9.26
taiiiga@raw:/media/sf_Virtual/cryptonet/2$ openssl rand -base64 189 > 9.27
taiiiga@raw:/media/sf_Virtual/cryptonet/2$ openssl rand -base64 189 > 9.28
taiiiga@raw:/media/sf_Virtual/cryptonet/2$ openssl rand -base64 189 > 9.29
taiiiga@raw:/media/sf_Virtual/cryptonet/2$ openssl rand -base64 189 > 9.210
taiiiga@raw:/media/sf_Virtual/cryptonet/2$ openssl rand -base64 189 > 9.211
taiiiga@raw:/media/sf_Virtual/cryptonet/2$ openssl rand -base64 189 > 9.212
taiiiga@raw:/media/sf_Virtual/cryptonet/2$ cp ../1/9.12 9.21
```

```
taiiiga@raw:/media/sf_Virtual/cryptonet/3$ openssl rand -base64 189 > 9.34
taiiiga@raw:/media/sf_Virtual/cryptonet/3$ openssl rand -base64 189 > 9.35
taiiiga@raw:/media/sf_Virtual/cryptonet/3$ openssl rand -base64 189 > 9.36
taiiiga@raw:/media/sf_Virtual/cryptonet/3$ openssl rand -base64 189 > 9.37
taiiiga@raw:/media/sf_Virtual/cryptonet/3$ openssl rand -base64 189 > 9.38
taiiiga@raw:/media/sf_Virtual/cryptonet/3$ openssl rand -base64 189 > 9.39
taiiiga@raw:/media/sf_Virtual/cryptonet/3$ openssl rand -base64 189 > 9.310
taiiiga@raw:/media/sf_Virtual/cryptonet/3$ openssl rand -base64 189 > 9.311
taiiiga@raw:/media/sf_Virtual/cryptonet/3$ openssl rand -base64 189 > 9.312
taiiiga@raw:/media/sf_Virtual/cryptonet/3$ cp ../1/9.13 9.31
taiiiga@raw:/media/sf_Virtual/cryptonet/3$ cp ../2/9.23 9.32
```

```
taiiiga@raw:/media/sf_Virtual/cryptonet/4$ openssl rand -base64 189 > 9.45
taiiiga@raw:/media/sf_Virtual/cryptonet/4$ openssl rand -base64 189 > 9.46
taiiiga@raw:/media/sf_Virtual/cryptonet/4$ openssl rand -base64 189 > 9.47
taiiiga@raw:/media/sf_Virtual/cryptonet/4$ openssl rand -base64 189 > 9.48
taiiiga@raw:/media/sf_Virtual/cryptonet/4$ openssl rand -base64 189 > 9.49
taiiiga@raw:/media/sf_Virtual/cryptonet/4$ openssl rand -base64 189 > 9.410
taiiiga@raw:/media/sf_Virtual/cryptonet/4$ openssl rand -base64 189 > 9.411
taiiiga@raw:/media/sf_Virtual/cryptonet/4$ openssl rand -base64 189 > 9.412
taiiiga@raw:/media/sf_Virtual/cryptonet/4$ cp ../1/9.14 9.41
taiiiga@raw:/media/sf_Virtual/cryptonet/4$ cp ../2/9.24 9.42
taiiiga@raw:/media/sf_Virtual/cryptonet/4$ cp ../3/9.34 9.43
```

```
taiiiga@raw:/media/sf_Virtual/cryptonet/5$ openssl rand -base64 189 > 9.56
taiiiga@raw:/media/sf_Virtual/cryptonet/5$ openssl rand -base64 189 > 9.57
taiiiga@raw:/media/sf_Virtual/cryptonet/5$ openssl rand -base64 189 > 9.58
taiiiga@raw:/media/sf_Virtual/cryptonet/5$ openssl rand -base64 189 > 9.59
taiiiga@raw:/media/sf_Virtual/cryptonet/5$ openssl rand -base64 189 > 9.510
taiiiga@raw:/media/sf_Virtual/cryptonet/5$ openssl rand -base64 189 > 9.511
taiiiga@raw:/media/sf_Virtual/cryptonet/5$ openssl rand -base64 189 > 9.512
taiiiga@raw:/media/sf_Virtual/cryptonet/5$ cp ../1/9.15 9.51
taiiiga@raw:/media/sf_Virtual/cryptonet/5$ cp ../2/9.25 9.52
taiiiga@raw:/media/sf_Virtual/cryptonet/5$ cp ../3/9.35 9.53
taiiiga@raw:/media/sf_Virtual/cryptonet/5$ cp ../4/9.45 9.54
```

```
taiiiga@raw:/media/sf_Virtual/cryptonet/6$ openssl rand -base64 189 > 9.67
taiiiga@raw:/media/sf_Virtual/cryptonet/6$ openssl rand -base64 189 > 9.68
taiiiga@raw:/media/sf_Virtual/cryptonet/6$ openssl rand -base64 189 > 9.69
taiiiga@raw:/media/sf_Virtual/cryptonet/6$ openssl rand -base64 189 > 9.610
taiiiga@raw:/media/sf_Virtual/cryptonet/6$ openssl rand -base64 189 > 9.611
taiiiga@raw:/media/sf_Virtual/cryptonet/6$ openssl rand -base64 189 > 9.612
taiiiga@raw:/media/sf_Virtual/cryptonet/6$ cp ../1/9.16 9.61
taiiiga@raw:/media/sf_Virtual/cryptonet/6$ cp ../2/9.26 9.62
taiiiga@raw:/media/sf_Virtual/cryptonet/6$ cp ../3/9.36 9.63
taiiiga@raw:/media/sf_Virtual/cryptonet/6$ cp ../4/9.46 9.64
taiiiga@raw:/media/sf_Virtual/cryptonet/6$ cp ../5/9.56 9.65
```

```
taiiiga@raw:/media/sf_Virtual/cryptonet/7$ openssl rand -base64 189 > 9.78
taiiiga@raw:/media/sf_Virtual/cryptonet/7$ openssl rand -base64 189 > 9.79
taiiiga@raw:/media/sf_Virtual/cryptonet/7$ openssl rand -base64 189 > 9.710
taiiiga@raw:/media/sf_Virtual/cryptonet/7$ openssl rand -base64 189 > 9.711
taiiiga@raw:/media/sf_Virtual/cryptonet/7$ openssl rand -base64 189 > 9.712
taiiiga@raw:/media/sf_Virtual/cryptonet/7$ cp ../1/9.17 9.71
taiiiga@raw:/media/sf_Virtual/cryptonet/7$ cp ../2/9.27 9.72
taiiiga@raw:/media/sf_Virtual/cryptonet/7$ cp ../3/9.37 9.73
taiiiga@raw:/media/sf_Virtual/cryptonet/7$ cp ../4/9.47 9.74
taiiiga@raw:/media/sf_Virtual/cryptonet/7$ cp ../5/9.57 9.75
taiiiga@raw:/media/sf_Virtual/cryptonet/7$ cp ../6/9.67 9.76
```

```
taiiiga@raw:/media/sf_Virtual/cryptonet/8$ openssl rand -base64 189 > 9.89
taiiiga@raw:/media/sf_Virtual/cryptonet/8$ openssl rand -base64 189 > 9.810
taiiiga@raw:/media/sf_Virtual/cryptonet/8$ openssl rand -base64 189 > 9.811
taiiiga@raw:/media/sf_Virtual/cryptonet/8$ openssl rand -base64 189 > 9.812
taiiiga@raw:/media/sf_Virtual/cryptonet/8$ cp ../1/9.18 9.81
taiiiga@raw:/media/sf_Virtual/cryptonet/8$ cp ../2/9.28 9.82
taiiiga@raw:/media/sf_Virtual/cryptonet/8$ cp ../3/9.38 9.83
taiiiga@raw:/media/sf_Virtual/cryptonet/8$ cp ../4/9.48 9.84
taiiiga@raw:/media/sf_Virtual/cryptonet/8$ cp ../5/9.58 9.85
taiiiga@raw:/media/sf_Virtual/cryptonet/8$ cp ../6/9.68 9.86
taiiiga@raw:/media/sf_Virtual/cryptonet/8$ cp ../7/9.78 9.87
```

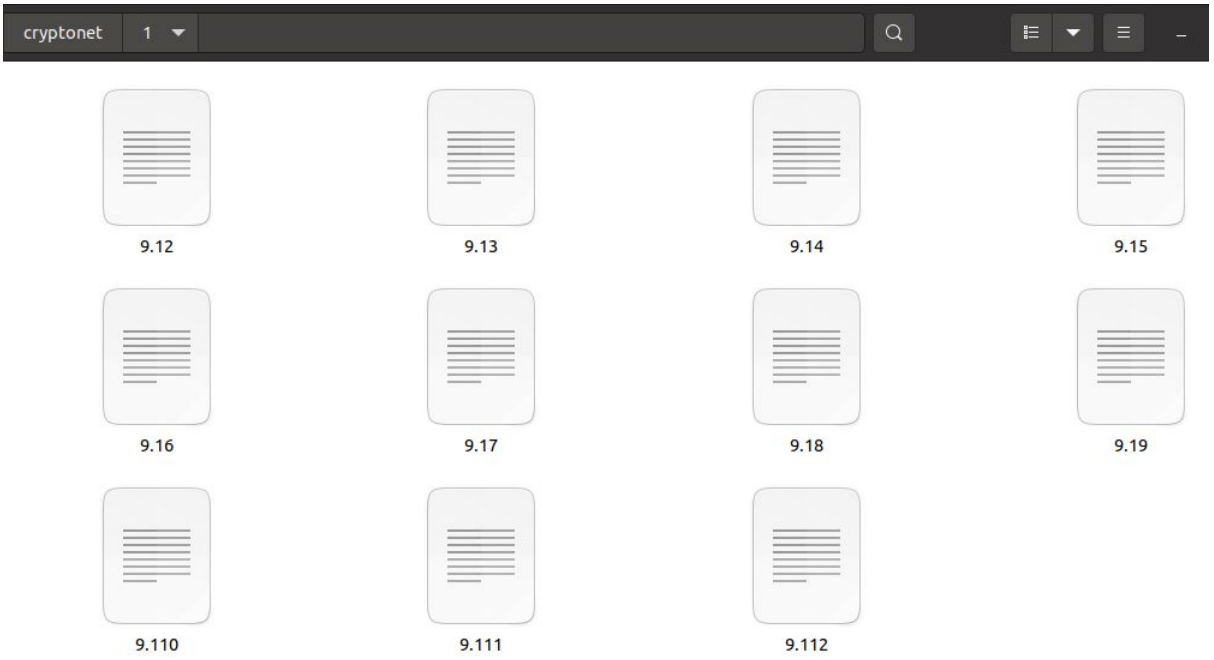
```
taiiiga@raw:/media/sf_Virtual/cryptonet/9$ openssl rand -base64 189 > 9.910
taiiiga@raw:/media/sf_Virtual/cryptonet/9$ openssl rand -base64 189 > 9.911
taiiiga@raw:/media/sf_Virtual/cryptonet/9$ openssl rand -base64 189 > 9.912
taiiiga@raw:/media/sf_Virtual/cryptonet/9$ cp ../1/9.19 9.91
taiiiga@raw:/media/sf_Virtual/cryptonet/9$ cp ../2/9.29 9.92
taiiiga@raw:/media/sf_Virtual/cryptonet/9$ cp ../3/9.39 9.93
taiiiga@raw:/media/sf_Virtual/cryptonet/9$ cp ../4/9.49 9.94
taiiiga@raw:/media/sf_Virtual/cryptonet/9$ cp ../5/9.59 9.95
taiiiga@raw:/media/sf_Virtual/cryptonet/9$ cp ../6/9.69 9.96
taiiiga@raw:/media/sf_Virtual/cryptonet/9$ cp ../7/9.79 9.97
taiiiga@raw:/media/sf_Virtual/cryptonet/9$ cp ../8/9.89 9.98
```

```
taiiiga@raw:/media/sf_Virtual/cryptonet/10$ openssl rand -base64 189 > 9.1011
taiiiga@raw:/media/sf_Virtual/cryptonet/10$ openssl rand -base64 189 > 9.1012
taiiiga@raw:/media/sf_Virtual/cryptonet/10$ cp ../1/9.110 9.101
taiiiga@raw:/media/sf_Virtual/cryptonet/10$ cp ../2/9.210 9.102
taiiiga@raw:/media/sf_Virtual/cryptonet/10$ cp ../3/9.310 9.103
taiiiga@raw:/media/sf_Virtual/cryptonet/10$ cp ../4/9.410 9.104
taiiiga@raw:/media/sf_Virtual/cryptonet/10$ cp ../5/9.510 9.105
taiiiga@raw:/media/sf_Virtual/cryptonet/10$ cp ../6/9.610 9.106
taiiiga@raw:/media/sf_Virtual/cryptonet/10$ cp ../7/9.710 9.107
taiiiga@raw:/media/sf_Virtual/cryptonet/10$ cp ../8/9.810 9.108
taiiiga@raw:/media/sf_Virtual/cryptonet/10$ cp ../9/9.910 9.109
```

```
taiiiga@raw:/media/sf_Virtual/cryptonet/11$ openssl rand -base64 189 > 9.1112
taiiiga@raw:/media/sf_Virtual/cryptonet/11$ cp ../1/9.111 9.111
taiiiga@raw:/media/sf_Virtual/cryptonet/11$ cp ../2/9.211 9.112
taiiiga@raw:/media/sf_Virtual/cryptonet/11$ cp ../3/9.311 9.113
taiiiga@raw:/media/sf_Virtual/cryptonet/11$ cp ../4/9.411 9.114
taiiiga@raw:/media/sf_Virtual/cryptonet/11$ cp ../5/9.511 9.115
taiiiga@raw:/media/sf_Virtual/cryptonet/11$ cp ../6/9.611 9.116
taiiiga@raw:/media/sf_Virtual/cryptonet/11$ cp ../7/9.711 9.117
taiiiga@raw:/media/sf_Virtual/cryptonet/11$ cp ../8/9.811 9.118
taiiiga@raw:/media/sf_Virtual/cryptonet/11$ cp ../9/9.911 9.119
taiiiga@raw:/media/sf_Virtual/cryptonet/11$ cp ../10/9.1011 9.1110
```

```
taiiiga@raw:/media/sf_Virtual/cryptonet/12$ cp ../1/9.112 9.121
taiiiga@raw:/media/sf_Virtual/cryptonet/12$ cp ../2/9.212 9.122
taiiiga@raw:/media/sf_Virtual/cryptonet/12$ cp ../3/9.312 9.123
taiiiga@raw:/media/sf_Virtual/cryptonet/12$ cp ../4/9.412 9.124
taiiiga@raw:/media/sf_Virtual/cryptonet/12$ cp ../5/9.512 9.125
taiiiga@raw:/media/sf_Virtual/cryptonet/12$ cp ../6/9.612 9.126
taiiiga@raw:/media/sf_Virtual/cryptonet/12$ cp ../7/9.712 9.127
taiiiga@raw:/media/sf_Virtual/cryptonet/12$ cp ../8/9.812 9.128
taiiiga@raw:/media/sf_Virtual/cryptonet/12$ cp ../9/9.912 9.129
taiiiga@raw:/media/sf_Virtual/cryptonet/12$ cp ../10/9.1012 9.1210
taiiiga@raw:/media/sf_Virtual/cryptonet/12$ cp ../11/9.1112 9.1211
```

6. создайте ключевой носитель для каждого абонента криптосети (в виде отдельного каталога)



7. продемонстрируйте защищенный обмен между этими абонентами

```
taiiiga@raw:/media/sf_Virtual/cryptonet/1$ cat > text
hello, world!
^Z
[1]+  Stopped                 cat > text
taiiiga@raw:/media/sf_Virtual/cryptonet/1$ openssl enc -des-ecb -in text -out codedtext -pass file:./9.12 -iter 1000
taiiiga@raw:/media/sf_Virtual/cryptonet/1$ cat codedtext
Salted__X◆
3D57n◆◆◆V◆G`◆◆◆Q◆◆taiiiga@raw:/media/sf_Virtual/cryptonet/1$
taiiiga@raw:/media/sf_Virtual/cryptonet/1$ mv codedtext ../2
taiiiga@raw:/media/sf_Virtual/cryptonet/1$ cd ..
taiiiga@raw:/media/sf_Virtual/cryptonet$ cd 2
taiiiga@raw:/media/sf_Virtual/cryptonet/2$ ls
9.21  9.210  9.211  9.212  9.23  9.24  9.25  9.26  9.27  9.28  9.29  codedtext
taiiiga@raw:/media/sf_Virtual/cryptonet/2$ openssl enc -des-ecb -d -in codedtext -out text -pass file:./9.21 -iter 1000
taiiiga@raw:/media/sf_Virtual/cryptonet/2$ cat text
hello, world!
```

8. в графическом редакторе создайте файл (1000x1000пк) в формате BMP с надписью "ИМЯ ФАМИЛИЯ", жирным и с максимальным размером шрифта

9. скопируйте файл на виртуальную машину

10. зашифруйте файл методами ECB и CBC 3-мя различными алгоритмами

```
taiiiga@raw:/media/sf_Virtual$ openssl enc -des-cbc -in fullname.bmp -out fullname-des-cbc.bmp -iter 1000
enter des-cbc encryption password:
Verifying - enter des-cbc encryption password:
taiiiga@raw:/media/sf_Virtual$ openssl enc -des-cbc -d -in fullname-des-cbc.bmp -out fullname-decoded-des-cbc.bmp -iter 1000
enter des-cbc decryption password:
taiiiga@raw:/media/sf_Virtual$ dd if=fullname.bmp of=fullname-des-cbc.bmp bs=1 count=54 conv=notrunc
54+0 records in
54+0 records out
54 bytes copied, 0,0754329 s, 0,7 kB/s
```

```
taiiiga@raw:/media/sf_Virtual$ openssl enc -rc2-cbc -in fullname.bmp -out fullname-rc2-cbc.bmp -iter 1000
enter rc2-cbc encryption password:
Verifying - enter rc2-cbc encryption password:
taiiiga@raw:/media/sf_Virtual$ openssl enc -rc2-cbc -d -in fullname-rc2-cbc.bmp -out fullname-decoded-rc2-cbc.bmp -iter 1000
enter rc2-cbc decryption password:
taiiiga@raw:/media/sf_Virtual$ dd if=fullname.bmp of=fullname-rc2-cbc.bmp bs=1 count=54 conv=notrunc
54+0 records in
54+0 records out
54 bytes copied, 0,0601589 s, 0,9 kB/s
```

```
taiiiga@raw:/media/sf_Virtual$ openssl enc -aes-256-cbc -in fullname.bmp -out fullname-aes-256-cbc.bmp -iter 1000
enter aes-256-cbc encryption password:
Verifying - enter aes-256-cbc encryption password:
taiiiga@raw:/media/sf_Virtual$ openssl enc -aes-256-cbc -d -in fullname-aes-256-cbc.bmp -out fullname-decoded-aes-256-cbc.bmp -iter 1000
enter aes-256-cbc decryption password:
taiiiga@raw:/media/sf_Virtual$ dd if=fullname.bmp of=fullname-aes-256-cbc.bmp bs=1 count=54 conv=notrunc
54+0 records in
54+0 records out
54 bytes copied, 0,0654042 s, 0,8 kB/s
```

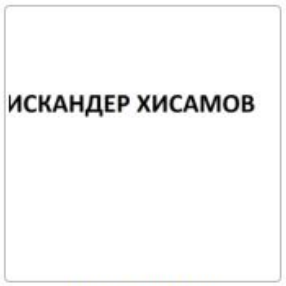
```
taiiiga@raw:/media/sf_Virtual$ openssl enc -aes-256-ecb -in fullname.bmp -out fullname-aes-256-ecb.bmp -iter 1000
enter aes-256-ecb encryption password:
Verifying - enter aes-256-ecb encryption password:
taiiiga@raw:/media/sf_Virtual$ openssl enc -aes-256-ecb -d -in fullname-aes-256-ecb.bmp -out fullname-decoded-aes-256-ecb.bmp -iter 1000
enter aes-256-ecb decryption password:
taiiiga@raw:/media/sf_Virtual$ dd if=fullname.bmp of=fullname-aes-256-ecb.bmp bs=1 count=54 conv=notrunc
54+0 records in
54+0 records out
54 bytes copied, 0,0842257 s, 0,6 kB/s
```

```
taiiiga@raw:/media/sf_Virtual$ openssl enc -rc2-ecb -in fullname.bmp -out fullname-rc2-ecb.bmp -iter 1000
enter rc2-ecb encryption password:
Verifying - enter rc2-ecb encryption password:
taiiiga@raw:/media/sf_Virtual$ openssl enc -rc2-ecb -d -in fullname-rc2-ecb.bmp -out fullname-decoded-rc2-ecb.bmp -iter 1000
enter rc2-ecb decryption password:
taiiiga@raw:/media/sf_Virtual$ dd if=fullname.bmp of=fullname-rc2-ecb.bmp bs=1 count=54 conv=notrunc
54+0 records in
54+0 records out
54 bytes copied, 0,0643396 s, 0,8 kB/s
```

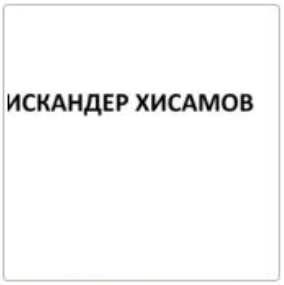
```
taiiiga@raw:/media/sf_Virtual$ openssl enc -des-ecb -in fullname.bmp -out fullname-des-ecb.bmp -iter 1000
enter des-ecb encryption password:
Verifying - enter des-ecb encryption password:
taiiiga@raw:/media/sf_Virtual$ openssl enc -des-ecb -d -in fullname-des-ecb.bmp -out fullname-decoded-des-ecb.bmp -iter 1000
enter des-ecb decryption password:
taiiiga@raw:/media/sf_Virtual$ dd if=fullname.bmp of=fullname-des-ecb.bmp bs=1 count=54 conv=notrunc
54+0 records in
54+0 records out
54 bytes copied, 0,0791612 s, 0,7 kB/s
```

11. зашифруйте файл методами ECB и CBC, одним алгоритмом, но различными 2-мя ключами

```
taiiiga@raw:/media/sf_Virtual$ cat > key
123456789
^Z
[1]+  Stopped                 cat > key
taiiiga@raw:/media/sf_Virtual$ openssl enc -rc2-ecb -in fullname.bmp -out fullname-rc2-ecb.bmp file:./key -iter 1000
Extra arguments given.
enc: Use -help for summary.
taiiiga@raw:/media/sf_Virtual$ openssl enc -rc2-ecb -in fullname.bmp -out fullname-rc2-ecb.bmp -pass  file:./key -iter 1000
taiiiga@raw:/media/sf_Virtual$ cat key
123456789
taiiiga@raw:/media/sf_Virtual$ openssl enc -rc2-ecb -in fullname.bmp -out fullname-rc2-ecb.bmp -pass  file:./key -iter 1000
taiiiga@raw:/media/sf_Virtual$ openssl enc -rc2-ecb -d -in fullname-rc2-ecb.bmp -out fullname-decoded-rc2-ecb.bmp -pass  file:./key -iter 100
0
taiiiga@raw:/media/sf_Virtual$ dd if=fullname.bmp of=fullname-rc2-ecb.bmp bs=1 count=54 conv=notrunc
54+0 records in
54+0 records out
54 bytes copied, 0,0695633 s, 0,8 kB/s
taiiiga@raw:/media/sf_Virtual$
```



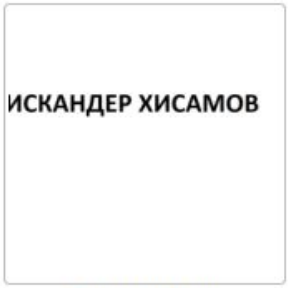
fullname.bmp



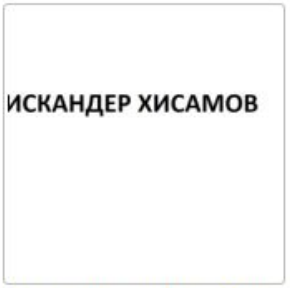
fullname-decoded-rc2-ecb.bmp

fullname-rc2-ecb.bmp

```
taiiiga@raw:/media/sf_Virtual$ cat key
98765
taiiiga@raw:/media/sf_Virtual$ openssl enc -rc2-ecb -in fullname.bmp -out fullname-rc2-ecb.bmp -pass file:./key -iter 1000
taiiiga@raw:/media/sf_Virtual$ openssl enc -rc2-ecb -d -in fullname-rc2-ecb.bmp -out fullname-decoded-rc2-ecb.bmp -pass  file:./key -iter 100
0
taiiiga@raw:/media/sf_Virtual$ dd if=fullname.bmp of=fullname-rc2-ecb.bmp bs=1 count=54 conv=notrunc
54+0 records in
54+0 records out
54 bytes copied, 0,0817524 s, 0,7 kB/s
```



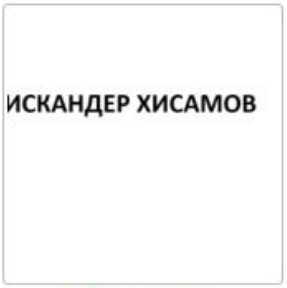
fullname.bmp



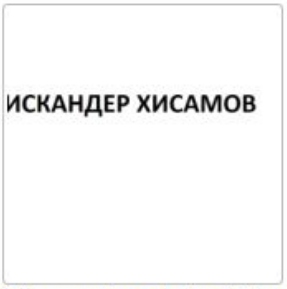
fullname-decoded-rc2-ecb.bmp

fullname-rc2-ecb.bmp

```
taiiiga@raw:/media/sf_Virtual$ cat key
98765
taiiiga@raw:/media/sf_Virtual$ openssl enc -rc2-cbc -in fullname.bmp -out fullname-rc2-cbc.bmp -pass file:./key -iter 1000
taiiiga@raw:/media/sf_Virtual$ openssl enc -rc2-cbc -d -in fullname-rc2-cbc.bmp -out fullname-decoded-rc2-cbc.bmp -pass  file:./key -iter 100
0
taiiiga@raw:/media/sf_Virtual$ dd if=fullname.bmp of=fullname-rc2-cbc.bmp bs=1 count=54 conv=notrunc
54+0 records in
54+0 records out
54 bytes copied, 0,0662351 s, 0,8 kB/s
```



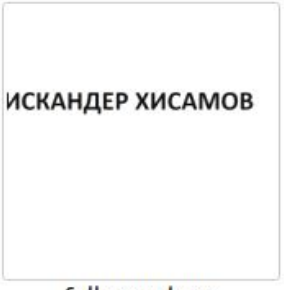
fullname.bmp



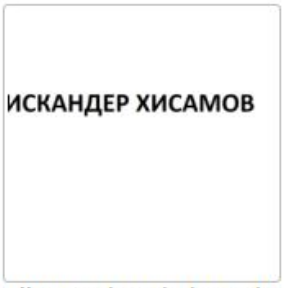
fullname-decoded-rc2-cbc.bmp

fullname-rc2-cbc.bmp

```
taiiiga@raw:/media/sf_Virtual$ cat key
123456789
taiiiga@raw:/media/sf_Virtual$ openssl enc -rc2-cbc -in fullname.bmp -out fullname-rc2-cbc.bmp -pass file:./key -iter 1000
taiiiga@raw:/media/sf_Virtual$ openssl enc -rc2-cbc -d -in fullname-rc2-cbc.bmp -out fullname-decoded-rc2-cbc.bmp -pass  file:./key -iter 100
0
taiiiga@raw:/media/sf_Virtual$ dd if=fullname.bmp of=fullname-rc2-cbc.bmp bs=1 count=54 conv=notrunc
54+0 records in
54+0 records out
54 bytes copied, 0,0758597 s, 0,7 kB/s
```



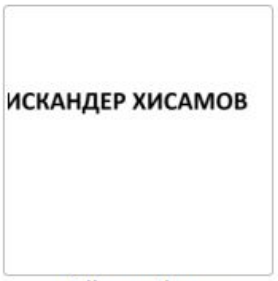
fullname.bmp



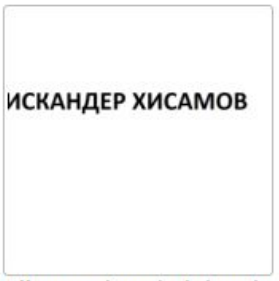
fullname-decoded-rc2-cbc.bmp

fullname-rc2-cbc.bmp

12. просмотрите и сравните изображения, до просмотра необходимо заменить заголовки в зашифрованных файлах: dd if=image.bmp of=image-ecb.bmp bs=1 count=54 conv=notrunc



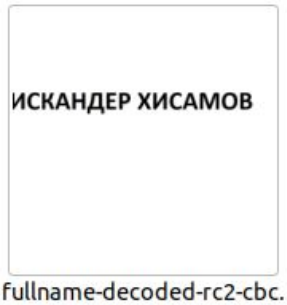
fullname.bmp



fullname-decoded-des-cbc.bmp

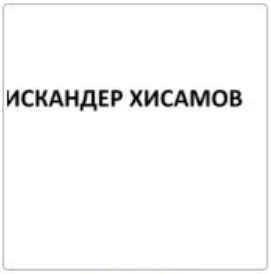

fullname-des-cbc.bmp

fullname.bmp



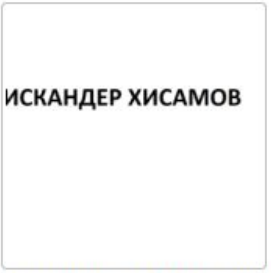
fullname-decoded-rc2-cbc.bmp


fullname-rc2-cbc.bmp



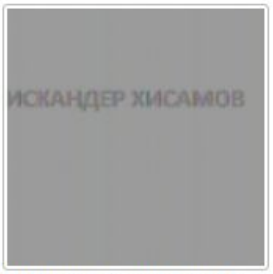
fullname.bmp


fullname-aes-256-cbc.bmp

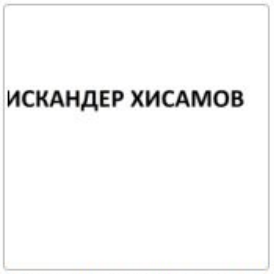


fullname-decoded-aes-256-cbc.bmp

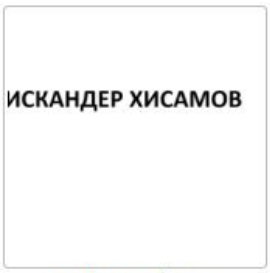
fullname.bmp



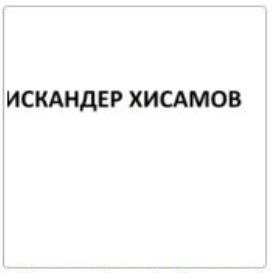
fullname-aes-256-ecb.bmp



fullname-decoded-aes-256-ecb.bmp

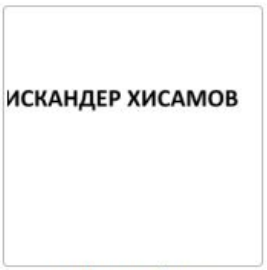


fullname.bmp

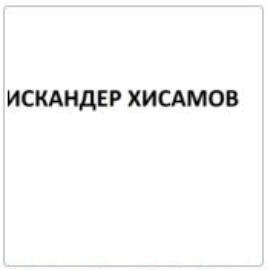


fullname-decoded-rc2-ecb.bmp

fullname-rc2-ecb.bmp



fullname.bmp



fullname-decoded-des-ecb.bmp


fullname-des-ecb.bmp

13. возьмите свою фотографию в разрешении (1000x1000), проделайте тоже самое для одного алгоритма шифрования

```
taiiiga@raw:/media/sf_Virtual$ cat key
123456789
taiiiga@raw:/media/sf_Virtual$ openssl enc -rc2-cbc -in me.bmp -out me-coded1.bmp -pass file:./key -iter 1000
taiiiga@raw:/media/sf_Virtual$ openssl enc -rc2-cbc -d -in me-coded1.bmp -out me-decoded1.bmp -pass file:./key -iter 1000
taiiiga@raw:/media/sf_Virtual$ dd if=me.bmp of=me-coded1.bmp bs=1 count=54 conv=notrunc
54+0 records in
54+0 records out
54 bytes copied, 0,0855513 s, 0,6 kB/s
```


me.bmp


me-coded1.bmp


me-decoded1.bmp

```
taiiiga@raw:/media/sf_Virtual$ cat key
98765
taiiiga@raw:/media/sf_Virtual$ openssl enc -rc2-cbc -in me.bmp -out me-coded2.bmp -pass file:./key -iter 1000
taiiiga@raw:/media/sf_Virtual$ openssl enc -rc2-cbc -d -in me-coded2.bmp -out me-decoded2.bmp -pass file:./key -iter 1000
taiiiga@raw:/media/sf_Virtual$ dd if=me.bmp of=me-coded2.bmp bs=1 count=54 conv=notrunc
54+0 records in
54+0 records out
54 bytes copied, 0,0591719 s, 0,9 kB/s
```

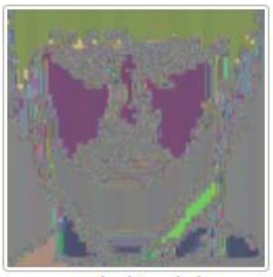

me.bmp


me-coded2.bmp


me-decoded2.bmp

```
taiiiga@raw:/media/sf_Virtual$ cat key
98765
taiiiga@raw:/media/sf_Virtual$ openssl enc -rc2-ecb -in me.bmp -out me-coded1-ecb.bmp -pass file:./key -iter 1000
taiiiga@raw:/media/sf_Virtual$ openssl enc -rc2-ecb -d -in me-coded1-ecb.bmp -out me-decoded1-ecb.bmp -pass file:./key -iter 1000
^[[Ataiiiga@raw:/media/sf_Virtudd if=me.bmp of=me-coded1-ecb.bmp bs=1 count=54 conv=notrunc
54+0 records in
54+0 records out
54 bytes copied, 0,0780235 s, 0,7 kB/s
```

me.bmp



me-coded1-ecb.bmp

me-decoded1-ecb.bmp

```
taiiiga@raw:/media/sf_Virtual$ cat key
54321
taiiiga@raw:/media/sf_Virtual$ openssl enc -rc2-ecb -in me.bmp -out me-coded2-ecb.bmp -pass file:./key -iter 1000
taiiiga@raw:/media/sf_Virtual$ openssl enc -rc2-ecb -d -in me-coded2-ecb.bmp -out me-decoded2-ecb.bmp -pass file:./key -iter 1000
taiiiga@raw:/media/sf_Virtual$ dd if=me.bmp of=me-coded2-ecb.bmp bs=1 count=54 conv=notrunc
54+0 records in
54+0 records out
54 bytes copied, 0,0790468 s, 0,7 kB/s
```

me.bmp

me-coded2-ecb.bmp

me-decoded2-ecb.bmp