

Лабораторная работа 8

Элементы криптографии. Шифрование (кодирование) различных исходных текстов одним ключом

Ведьмина Александра Сергеевна

Содержание

1	Цель работы	1
2	Задание.....	1
3	Указания к работе	1
4	Выполнение лабораторной работы	2
5	Выводы.....	5

1 Цель работы

Освоить на практике применение режима однократного гаммирования на примере кодирования различных исходных текстов одним ключом.

2 Задание

Выполнить задания из файла в туисе.

3 Указания к работе

Две телеграммы Центра:

- 1) P1 = НаВашисходящийот1204
- 2) P2 = ВСеверныйфилиалБанка

Ключ Центра длиной 20 байт:

K = 05 0C 17 7F 0E 4E 37 D2 94 10 09 2E 22 57 FF C8 0B B2 70 54

Режим шифрования однократного гаммирования одним ключом двух видов открытого текста реализуется в соответствии со схемой. Шифротексты обеих телеграмм можно получить по формулам режима однократного гаммирования.

4 Выполнение лабораторной работы

Создаю пользователей guest и guest2.

[Создание пользователей](image/Screenshot from 2025-02-28 22-46-25.png{#fig:001 width=100%})

Добавляю пользователя guest2 в группу guest.

```
passwd: all authentication tokens updated successfully.  
[asvedjmina@localhost ~]$ sudo gpasswd -a guest2 guest  
Adding user guest2 to group guest  
[asvedjmina@localhost ~]$
```

Рис. 1: Добавление в группу

Вхожу в пользователей с разных консолей.

```
[asvedjmina@localhost ~]$ login  
[asvedjmina@localhost ~]$ su guest  
Password:  
[guest@localhost asvedjmina]$
```



```
guest2@localhost:~/ho  
File Edit View Search Terminal Help  
[asvedjmina@localhost ~]$ su guest2  
Password:  
[guest2@localhost asvedjmina]$
```

Рис. 2: Вход

Смотрю директории с помощью pwd.

```
guest is not in the sudoers file. This incident will be reported.
[guest@localhost ~]$ groups
guest
[guest@localhost ~]$
```



```
guest2@localhost:~
File Edit View Search Terminal Help
Password:
[guest2@localhost ~]$ pwd
/home/guest2
[guest2@localhost ~]$ groups
guest2 guest
[guest2@localhost ~]$
```

Рис. 3: Директория

Уточните имя вашего пользователя, его группу, кто входит в неё и к каким группам принадлежит он сам. Определите командами `groups guest` и `groups guest2`, в какие группы входят пользователи `guest` и `guest2`. Сравните вывод команды `groups` с выводом команд `id -Gn` и `id -G`.

```
guest
[guest@localhost ~]$ id -Gn
guest
[guest@localhost ~]$ id -G
1001
[guest@localhost ~]$
```



```
guest2@localhost:~
File Edit View Search Terminal Help
guest2 guest
[guest2@localhost ~]$ id -Gn
guest2 guest
[guest2@localhost ~]$ id -G
1002 1001
[guest2@localhost ~]$
```

Рис. 4: Id

```
1001
[guest@localhost ~]$ groups guest
guest : guest
[guest@localhost ~]$ groups guest2
guest2 : guest2 guest
[guest@localhost ~]$ █

guest2@localhost:~
File Edit View Search Terminal Help
1002 1001
[guest2@localhost ~]$ groups guest
guest : guest
[guest2@localhost ~]$ groups guest2
guest2 : guest2 guest
[guest2@localhost ~]$
```

Рис. 5: Groups

От имени пользователя guest2 выполняю регистрацию пользователя guest2 в группе guest.

```
guest2 : guest2 guest
[guest2@localhost ~]$ newgrp guest
[guest2@localhost ~]$ groups
guest guest2
[guest2@localhost ~]$ id
uid=1002(guest2) gid=1001(guest) groups=1001(guest),1002(guest2) context=
unconfined_u:unconfined_r:unconfined_t:s0-s0:c0.c1023
[guest2@localhost ~]$ █
```

Рис. 6: Регистрация guest2

От имени пользователя guest изменяю права директории /home/guest, разрешив все действия для пользователей группы.

```
guest2:~:1002:
[guest@localhost ~]$ chmod g+rwX /home/guest
[guest@localhost ~]$ █
```

Рис. 7: Изменение прав

Снимаю с директории /home/guest/dir1 все атрибуты командой.

```
[guest@localhost ~]$ chmod g+rx /home/guest
[guest@localhost ~]$ chmod 000 /home/guest/dir1
[guest@localhost ~]$ ls -l /home/guest
total 0
drwxr-xr-x. 2 guest guest  6 Mar  1 01:23 Desktop
d------. 2 guest guest  6 Mar  1 01:36 dir1
drwxr-xr-x. 2 guest guest  6 Mar  1 01:23 Documents
drwxr-xr-x. 2 guest guest  6 Mar  1 01:23 Downloads
drwxr-xr-x. 2 guest guest  6 Mar  1 01:23 Music
drwxr-xr-x. 2 guest guest 147 Mar  1 01:35 Pictures
drwxr-xr-x. 2 guest guest  6 Mar  1 01:23 Public
drwxr-xr-x. 2 guest guest  6 Mar  1 01:23 Templates
drwxr-xr-x. 2 guest guest  6 Mar  1 01:23 Videos
[guest@localhost ~]$
```

Рис. 8: Снятие прав

```
[guest@localhost ~]$ cd /home/guest/dir1
-bash: cd: /home/guest/dir1: Permission denied
[guest@localhost ~]$
```

Рис. 9: Проверка

5 Выводы

В ходе лабораторной работы я получила практические навыки работы в консоли с атрибутами файлов для групп пользователей.