

## Лабораторная работа №7

---

Якушевич Артём Юрьевич - студент группы НКНбд-01-18

15.10.2021

Элементы криптографии.

Однократное гаммирование

---

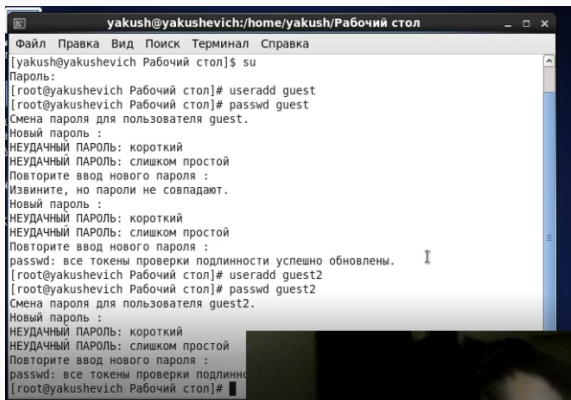
- Криптография - наука о методах шифрования. Знание однократного гаммирования и его особенностей является необходимым для дальнейшего знакомства с криптографией.

- Освоить на практике применение режима однократного гаммирования

- Написать программу, которая должна определить вид шифротекста при известном ключе и известном открытом тексте
- Также эта программа должна определить ключ, с помощью которого шифротекст может быть преобразован в некоторый фрагмент текста, представляющий собой один из возможных вариантов прочтения открытого текста

# Результаты выполнения лабораторной работы

- Написал программу, которая определяет вид шифротекста при известном ключе и известном открытом тексте (рис - @fig:001, рис - @fig:002)



```
yakush@yakushevich:/home/yakush/Рабочий стол
Файл Правка Вид Поиск Терминал Справка
[yakush@yakushevich Рабочий стол]$ su
Пароль:
[root@yakushevich Рабочий стол]# useradd guest
[root@yakushevich Рабочий стол]# passwd guest
Смена пароля для пользователя guest.
Новый пароль :
НЕУДАЧНЫЙ ПАРОЛЬ: короткий
НЕУДАЧНЫЙ ПАРОЛЬ: слишком простой
Повторите ввод нового пароля :
Извините, но пароли не совпадают.
Новый пароль :
НЕУДАЧНЫЙ ПАРОЛЬ: короткий
НЕУДАЧНЫЙ ПАРОЛЬ: слишком простой
Повторите ввод нового пароля :
passwd: все токены проверки подлинности успешно обновлены.
[root@yakushevich Рабочий стол]# useradd guest2
[root@yakushevich Рабочий стол]# passwd guest2
Смена пароля для пользователя guest2.
Новый пароль :
НЕУДАЧНЫЙ ПАРОЛЬ: короткий
НЕУДАЧНЫЙ ПАРОЛЬ: слишком простой
Повторите ввод нового пароля :
passwd: все токены проверки подлинности успешно обновлены.
[root@yakushevich Рабочий стол]#
```

Рис. 1: Функция, шифрующая данные

```
[root@yakushevich Рабочий стол]# passwd guest2
[root@yakushevich Рабочий стол]# passwd guest2
Смена пароля для пользователя guest2.
Новый пароль :
НЕУДАЧНЫЙ ПАРОЛЬ: короткий
НЕУДАЧНЫЙ ПАРОЛЬ: слишком простой
Повторите ввод нового пароля :
passwd: все токены проверки подлинности
[root@yakushevich Рабочий стол]#
```

Рис. 2: Результат работы функции, шифрующей данные

- Написанная мною программа определяет ключ, с помощью которого шифротекст может быть преобразован в некоторый фрагмент текста, представляющий собой один из возможных вариантов прочтения открытого текста (рис - @fig:003, рис - @fig:004)

```
passwd: все токены проверки подлинности успешно обновлены.  
[root@yakushevich Рабочий стол]# gpasswd -a guest2 guest  
Adding user guest2 to group guest  
[root@yakushevich Рабочий стол]#
```

Рис. 3: Функция, дешифрующая данные



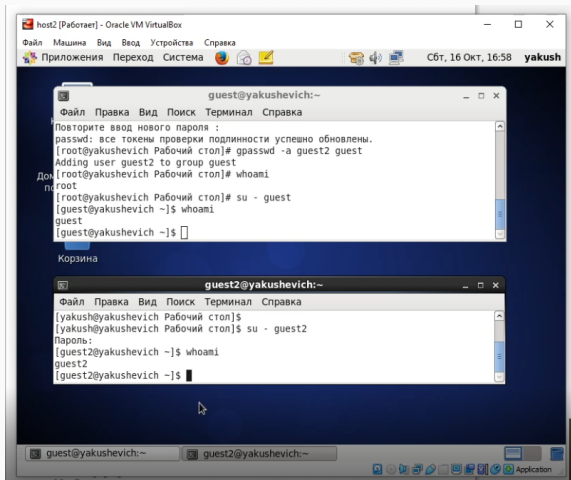


Рис. 4: Результат работы функции, дешифрующей данные

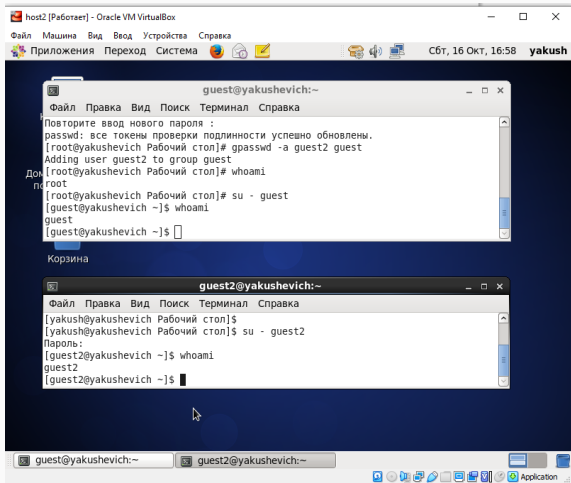


Рис. 5: Сравнение ключей

Таким образом, я освоил на практике применение режима однократного гаммирования.