

Лабораторная работа №7

Унтевская Валерия НПИбд-02-19

Цель работы

Освоить на практике применение режима однократного гаммирования.

Выполнение лабораторной работы

1. Написала код на языке python, позволяющий шифровать и дешифровать данные в режиме однократного гаммирования.(рис. 1).

```

In [1]: 1 def xor_cipher(filename, outfilename, string):
        2     with open(outfilename, "w") as filewrite:
        3         with open(filename) as file:
        4             if not file:
        5                 print("no file")
        6                 exit(1)
        7
        8         main_offset = 0 # Главное смещение (относительно строки)
        9         str_offset = 0 # Относительное смещение
       10         for line in file: # Чтение файла построчно
       11             res_str = ""
       12             for i in range(len(line)): # Посимвольно
       13                 if main_offset!=0 and main_offset < len(line):
       14                     str_offset += 1
       15                     res_str += chr(ord(line[i])^ord(string[main_offset]))
       16                     main_offset += 1
       17
       18             filewrite.write(res_str) # Запись в файл
       19
       20 def main():
       21     string = input("Введите строку:\n")
       22     xor_cipher("test.txt", "output.txt", string)
       23     xor_cipher("output.txt", "output#2.txt", string)
       24     print("DONE!")
       25     input("Нажмите Enter для завершения программы")
    
```

```

In [2]: 1 if __name__ == "__main__":
        2     main()
    
```

Введите строку:
 KeyString
 DONE!
 Нажмите Enter для завершения программы

Выводы

Освоила на практике применение режима однократного гаммирования.