

Презентация №7

Элементы криптографии. Однократное гаммирование

Аскеров А.Э.

9 мая 2024

Российский университет дружбы народов, Москва, Россия

Вступление

Освоить на практике применение режима однократного гаммирования.

Выполнение лабораторной работы

Выполнение лабораторной работы

Приложение, позволяющее шифровать и дешифровать данные в режиме однократного гаммирования:

```
1 def encryptDecrypt(inpString):
2     xorKey = 'P';
3     length = len(inpString)
4     for i in range(length):
5         inpString = (inpString[:i] + chr(ord(inpString[i]) ^ ord(xorKey)) + inpString[i + 1:])
6         print(inpString[i], end = "")
7     return inpString
8
9
10 if __name__ == '__main__':
11     sampleString = "С Новым Годом, друзья!"
12
13     print("Encrypted String: ", end = "")
14     sampleString = encryptDecrypt(sampleString)
15     print("\n")
16
17     print("Decrypted String: ", end = "")
18     encryptDecrypt(sampleString)
19
```

PROBLEMS OUTPUT DEBUG CONSOLE TERMINAL PORTS

in32-x64\bundled\libs\debugpy\adapter\...\debugpy\launcher '52912' '--' 'c:\Users\Admin\Downloads\Univer7\lab 7.py'
Encrypted String: фрзџБлКрyџџџ|рџџџџџџ
Decrypted String: С Новым Годом, друзья!

Рис. 1: Программа

Заключение

Применение режима однократного гаммирования освоено на практике.

Список литературы

1. XOR cypher