
Front matter

lang: ru-RU

title: Лабораторная работа 7

subtitle: Основы информационной безопасности

author:

- Пинега Б.А.

institute:

- Российский университет дружбы народов, Москва, Россия

i18n babel

babel-lang: russian

babel-otherlangs: english

Formatting pdf

toc: false

toc-title: Содержание

slide_level: 2

aspectratio: 169

section-titles: true

theme: metropolis

header-includes:

- `\metroset{progressbar=frametitle,sectionpage=progressbar,numbering=fraction}`
- `'\makeatletter'`
- `'\beamer@ignorenonframefalse'`
- `'\makeatother'`

Докладчик

- * Пинега Белла Александровна

- * Студентка НБИБд-02-22

- * Российский университет дружбы народов

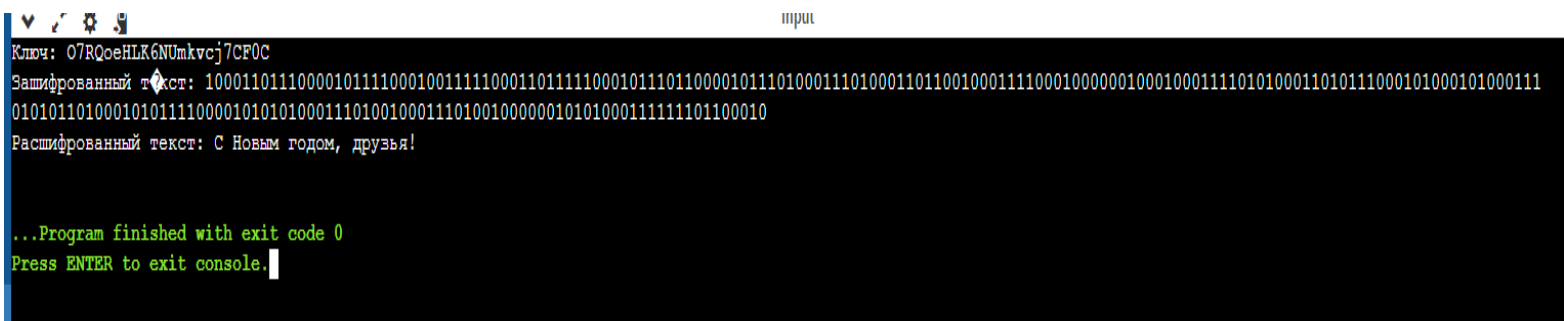
Цель

Освоить на практике применение режима однократного гаммирования

Код программы:

```
1 import random
2 import string
3
4 def generate_key(size):
5     characters = string.ascii_letters + string.digits
6     return ''.join(random.choice(characters) for _ in range(size))
7
8 def text_to_binary(text):
9     return ''.join(format(ord(char), '08b') for char in text)
10
11 def binary_text(binare_str):
12     binary_chunks = [binare_str[i:i+8] for i in range(0, len(binare_str), 8)]
13     return ''.join(chr(int(chunk, 2)) for chunk in binary_chunks)
14
15 def xor_encrypt(text, key):
16     encrypted = [ord(a) ^ ord(b) for a, b in zip(text, key)]
17     return ''.join(chr(encrypted_char) for encrypted_char in encrypted)
18
19 msg = "С Новым годом, друзья!"
20
21 key = generate_key(len(msg))
22
23 print("Ключ:", key)
24
25 msg2 = xor_encrypt(msg, key)
26
27 binary = text_to_binary(msg2)
28
29 print("Зашифрованный текст:", binary)
30
31 msg3 = xor_encrypt(binary, key)
32
33 print("Расшифрованный текст:", msg3)
```

Результат



```
Ключ: 07RQoeHLK6NUnkvcj7CF0C
Зашифрованный текст: 1000110111000010111100010011111000110111110001011101100001011101000111010001101100100011110001000000100010001111010100011010111000101000101000111
010101101000101011110000101010100011101001000111010010000001010100011111101100010
Расшифрованный текст: С Новым годом, друзья!

...Program finished with exit code 0
Press ENTER to exit console.
```

{#fig:002 width=70%}

Выводы

Я освоила на практике применение режима однократного гаммирования