## Лабораторная работа 7

Генералов Даниил, 1032212280

2024 г.

Российский университет дружбы народов, Москва, Россия

## Задание



Освоить на практике применение режима однократного гаммирования.

## Выполнение

```
>>> text = 'C Hobbm Fodom, dpy3bs!'
>>> encoded = text.encode('cp1251')
>>> encoded
b'\xd1 \xcd\xee\xe2\xfb\xec \xc3\xee\xe4\xee\xec, \xe4\xf0\xf3\xe7\xfc\xff!'
>>> encoded.hex(' ')
'd1 20 cd ee e2 fb ec 20 c3 ee e4 ee ec 2c 20 e4 f0 f3 e7 fc ff 21'
>>> ■
```

**Рис. 1:** python

```
plaintext_text = plaintext.decode('cp1251')
        print('Plaintext как CP1251:')
        print(plaintext_text)
        print('Plaintext He CP1251')
    print('Key:')
    key = bytes.fromhex(input('> '))
    if len(plaintext) != len(key):
        print('Plaintext и key должны быть одной и той же длины')
    print('Ciphertext:')
19 ciphertext = bytes([a ^ b for a, b in zip(plaintext, key)])
    print(ciphertext.hex(' '))
        ciphertext text = ciphertext.decode('cp1251')
        print('Ciphertext как CP1251:')
        print(ciphertext_text)
        print('Ciphertext He CP1251')
```

Рис. 2: python

```
• danya@archlinux ..udy_2024-2025_infosec/labs/lab7/report (git)-[master] % python crypt.py Plaintext:

> DD FE FF 8F E5 A6 C1 F2 B9 30 CB D5 02 94 1A 38 E5 5B 51 75 Plaintext как CP1251:
ЭюяЏе¦БтМОЛХ"8e[Qu

Key:

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

Ciphertext:
d8 f2 e8 f0 eb e8 f6 20 2d 20 c2 fb 20 c3 e5 f0 ee e9 21 21
Сірhетtext как CP1251:
Штирлиц - Вы Герой!!

• danya@archlinux ..udy_2024-2025_infosec/labs/lab7/report (git)-[master] %
```

Рис. 3: python

```
danya@archlinux ..udy_2024-2025_infosec/labs/lab7/report (git)-[master] % python crypt.py Plaintext:

> DD FE FF 8F E5 A6 C1 F2 B9 30 CB D5 02 94 1A 38 E5 5B 51 75 Plaintext κακ CP1251:

3ωσμe¦δτωθ/Κ"8e[Qu

Key:

> d1 cd ee e2 fb ec 20 c3 ee e4 ee ec 2c e4 f0 f3 e7 fc ff 21

Ciphertext:

0c 33 11 6d le 4a e1 31 57 d4 25 39 2e 70 ea cb 02 a7 ae 54

Ciphertext κακ CP1251:

3mJ61W97%.pk/IS©T

danya@archlinux ..udy_2024-2025_infosec/labs/lab7/report (git)-[master] %
```

Рис. 4: python

```
odanya@archlinux ..udy_2024-2025_infosec/labs/lab7/report (git)-[master] % python crypt.py
Plaintext:

> DD FE FF 8F E5 A6 C1 F2 B9 30 CB D5 02 94 1A 38 E5 5B 51 75
Plaintext kak CP1251:

⇒ moRUe¦5™mOJX*8e[Qu

Key:

> 0c 33 11 6d 1e 4a e1 31 57 d4 25 39 2e 70 ea cb 02 a7 ae 54

Ciphertext:
d1 cd ee e2 fb ec 20 c3 ee e4 ee ec 2c e4 f0 f3 e7 fc ff 21

Ciphertext kak CP1251:
CHOBBM ГОДОМ,Друзья!

> danya@archlinux ..udy_2024-2025_infosec/labs/lab7/report (git)-[master] %
```

Рис. 5: python





В этой лабораторной работе мы рассмотрели алгоритм однократного гаммирования и показали, каким образом можно шифровать и дешифровать сообщения с помощью него.