

Лабораторная работа №8

Сыров Владислав

RUDN University, 2022 Moscow, Russia

Цель выполнения лабораторной работы

Освоить на практике применение режима однократного гаммирования на примере кодирования различных исходных текстов одним ключом.

Результат работы шифрователя

```
▶ k, t1, et1, t2, et2 = encryption(s1, s2)
```

```
↳ Открытый текст 1: С Новым Годом, друзья!
```

```
Открытый текст 1 в 16-ой системе: ['d1', '20', 'cd', 'ee', 'e2', 'fb', 'ec', '20', 'c3', 'ee', 'e4', 'ee', 'ec', '2c', '20', 'e4', 'f0', 'f3', 'e7', 'fc', 'ff', '21']
```

```
Открытый текст 2: Лабораторная работа №8
```

```
Открытый текст 2 в 16-ой системе: ['cb', 'e0', 'e1', 'ee', 'f0', 'e0', 'f2', 'ee', 'f0', 'ed', 'e0', 'ff', '20', 'f0', 'e0', 'e1', 'ee', 'f2', 'e0', '20', 'b9', '38']
```

```
Ключ в 16-ой системе: ['28', '9c', '6e', '6b', '1', '1', 'd6', '33', '42', '9d', '39', '94', '60', '29', 'a3', 'dc', 'a8', 'e6', 'c1', '2d', 'fc', '4d']
```

```
Шифротекст 1 в 16-ой системе: ['f9', 'bc', 'a3', '85', 'e3', 'fa', '3a', '13', '81', '73', 'dd', '7a', '8c', '05', '83', '38', '58', '15', '26', 'd1', '03', '6c']
```

```
Шифротекст 1: щjJ...гъ:0f'sЭzЫ0f8X0&C0l
```

```
Шифротекст 2 в 16-ой системе: ['e3', '7c', '8f', '85', 'f1', 'e1', '24', 'dd', 'b2', '70', 'd9', '6b', '40', 'd9', '43', '3d', '46', '14', '21', '0d', '45', '75']
```

```
Eu
```

Результат работы дешифрователя

```
▶ s3 = decryption(et1, et2, s1)
```

```
↳ Шифротекст 1: шjJ...гъ:0fsЭzт0f8X0&C0l
```

```
Шифротекст 1 в 16-ой системе: ['f9', 'bc', 'a3', '85', 'e3', 'fa', '3a', '13', '81', '73', 'dd', '7a', '8c', '05', '83', '38', '58', '15', '26', 'd1', '03', '6c']
```

```
Eu
```

```
Шифротекст 2 в 16-ой системе: ['e3', '7c', '8f', '85', 'f1', 'e1', '24', 'dd', 'b2', '70', 'd9', '6b', '40', 'd9', '43', '3d', '46', '14', '21', '0d', '45', '75']
```

```
Открытый текст 1: С Новым Годом, друзья!
```

```
Открытый текст 1 в 16-ой системе: ['d1', '20', 'cd', 'ee', 'e2', 'fb', 'ec', '20', 'c3', 'ee', 'e4', 'ee', 'ec', '2c', '20', 'e4', 'f0', 'f3', 'e7', 'fc', 'ff', '21']
```

```
Нахожу второй открытый текст...
```

```
Открытый текст 2 в 16-ой системе: ['cb', 'e0', 'e1', 'ee', 'f0', 'e0', 'f2', 'ee', 'f0', 'ed', 'e0', 'ff', '20', 'f0', 'e0', 'e1', 'ee', 'f2', 'e0', '20', 'b9', '38']
```

```
Открытый текст 2: Лабораторная работа №8
```

Вывод

В ходе данной лабораторной работы я освоила применение режима однократного гаммирования на примере кодирования различных исходных текстов одним ключом.

Спасибо за внимание