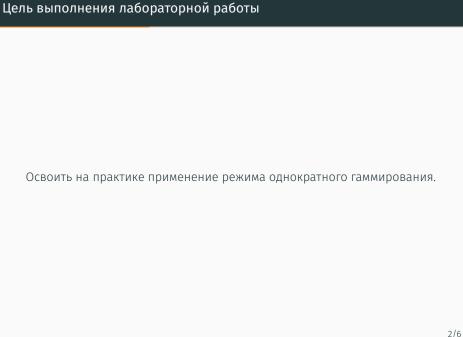
## Лабораторная работа № 7. Элементы криптографии. Однократное гаммирование

Ильин Никита Евгеньевич, НФИбд-01-19

работы

Цель выполнения лабораторной



## Результат выполнения лабораторной работы

```
import numpy as np
✓ 0.5s
  def encrypt(text):
      print("Открытый текст: ". text)
      text_arr = []
      for i in text:
          text arr.append(i.encode("cp1251").hex())
      print("Текст в шестнадцатиричном представлении: ", *text arr)
      kev dec = np.random.randint(0, 255, len(text))
      kev hex = [hex(i)[2:]] for i in kev decl
      print("Ключ в шестнапцатиричном представлении: ". *kev hex)
      text_crypt = []
      for i in range(len(text arr)):
          text crypt.append("{:02x}".format(int(text arr[i], 16) ^ int(key hex[i], 16)))
      print("Зашифрованный текст в шестнадцатиричном представлении: ", *text crypt)
      text_fin = bytearray.fromhex("".join(text_crypt)).decode("cp1251")
      print("Зашифрованный текст: ", text_fin)
      return kev hex. text fin
✓ 0.3s
```

## Результат выполнения лабораторной работы

```
def decrypt(text, text_fin):
   print("Открытый текст: ", text)
   print("Зашифрованный текст: ", text_fin)
   hex text = []
    for i in text:
        hex text.append(i.encode("cp1251").hex())
   print("Открытый текст в шестнадцатиричном представлении: ", *hex text)
   hex_text_fin = []
   for i in text_fin:
        hex_text_fin.append(i.encode("cp1251").hex())
   print("Зашифрованный текст в шестнадцатиричном представлении: ", *hex_text_fin)
   key = [hex(int(i, 16) \land int(j, 16))[2:] for (i, j) in zip(hex_text, hex_text_fin)]
   print("Полученный ключ в шестнадцатиричном представлении: ", *key)
    return key
0.3s
```

Figure 2: функция расшифровки

## Результат выполнения лабораторной работы

```
text = "С Новым Годом, друзья!"
   key_encr, text_crypt = encrypt(text)

√ 0.3s

Открытый текст: С Новым Годом, друзья!
Текст в шестнадцатиричном представлении: d1 20 cd ee e2 fb ec 20 c3 ee e4 ee ec 2c 20 e4 f0 f3 e7 fc ff 21
Ключ в шестнадцатиричном представлении: bf f1 b5 2f d8 a7 a5 69 2c d5 12 7a 79 42 79 44 45 99 5e 3e d8 3a
Зашифрованный текст в шестнапцатиричном представлении: 6e d1 78 c1 3a 5c 49 49 ef 3b f6 94 95 6e 59 a0 b5 6a b9 c2 27 1b
Зашифрованный текст: nCxБ:\IIn;ц"•nY µj%B'
   key = decrypt(text, text crypt)
Открытый текст: С Новым Годом, друзья!
Зашифрованный текст: nCxБ:\IIn;ц"•nY µj%B'
Открытый текст в шестналцатиричном представлении: d1 20 cd ee e2 fb ec 20 c3 ee e4 ee ec 2c 20 e4 f0 f3 e7 fc ff 21
Зашифрованный текст в шестнадцатиричном представлении: 6e d1 78 c1 3a 5c 49 49 ef 3b f6 94 95 6e 59 a0 b5 6a b9 c2 27 1b
Полученный ключ в шестнапцатиричном представлении: bf f1 b5 2f d8 a7 a5 69 2c d5 12 7a 79 42 79 44 45 99 5e 3e d8 3a
   print("Ключ верный") if key_encr == key else print("Ключ не подошел")
 ✓ 0.9s
Ключ верный
```

Figure 3: Работа программы

Выводы по лабораторной работе

