Докладчик

- Ду Нашсименту Висенте феликс Жозе
- студент группы НКНбд-01-20
- Факультет физико-математических и естественных наук
- Российский университет дружбы народов
- https://github.com/kpatocfelix

Цель работы

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

Выполнение лабораторной работы

```
[18] import random
     import string
```

```
def hextext(text):
  t="".join(hex(ord(i))[2:]for i in text)
  return t
```

```
[20] def gen_klyo(size):
       g=''.join(random.choice(string.ascii_letters + string.digits)for _ in range(size))
       return g
```

```
[21] def encrypted(ms1,ms2):
       ms1=[ord(i) for i in ms1]
       ms2=[ord(i) for i in ms2]
       create=''.join(chr(a^b)for a,b in zip(ms1,ms2))
       return create
```

```
[22] P1= " НаВашисходящийот1204"
     P2= " ВСеверныйфилиалБанка"
```

```
[23] key = gen_klyo(len(P1))
     print(key)
     hex_klyuch=hextext(key)
     print("Ключ в шестнадцатиричном виде: {}".format(hex_klyuch))

     AHwgLQ4cVVXAyHW7Zua7F
     Ключ в шестнадцатиричном виде: 414877674c513463565658417948573 75a75613746
```

```
[24] C1= encrypted(P1,key)
     C2= encrypted(P2,key)
     print("Шифрованный текст: {}".format(C1))
     print("Шифрованный текст: {}".format(C2))

     decrypt=encrypted(C1,C2)
     print("Расфрованный текст: {}".format(encrypted(decrypt,P2)))
     print("Расфрованный текст: {}".format(encrypted(decrypt,P1)))

     Шифрованный текст: asчѵѼЙЌТГѭѬЎaѰѮљИDS?r
     Шифрованный текст: aњiђѾѥVўНѮМѹтѰѫЌыхќЍѷ
     Расфрованный текст:  НаВашисходящийот1204
     Расфрованный текст:  ВСеверныйфилиалБанка
```

Выводы

Этот код выполняет простую форму шифрования XOR. Это базовая демонстрация XOR-шифрования и не должен использоваться для безопасных коммуникационных целей. Кроме того, код предполагает, что входное сообщение и ключ находятся в той же кодировке символов. Если это не так, результаты могут не соответствовать ожиданиям.