Презентация к лабораторной работе №7

Цель работы

Освоить на практике применение режима однократного гаммирования.

Выполнение работы

Импорт библиотек. Функция для генерации случайного ключа

```
[1]: import random
     import string
```

```
[2]: def get_random_key(n):
         symbols = string.ascii_letters + string.digits
         return ''.join([random.choice(symbols) for i in range(n)])
```

Функция шифрования / дешифрования. Функция find_possible_keys.

```
[3]: def enc_dec(text, key):
         if len(text) != len(key):
             raise ValueError('Длины текста и ключа должны совпадать')
         return ''.join([chr(ord(text[i]) ^ ord(key[i % len(key)])) for i in range(len(text))])
```

```
[4]: def find_keys(text, part):
         all_keys = []
         for i in range(len(text) - len(part) + 1):
             new_key = ""
             for j in range(len(part)):
                 new_key += chr(ord(text[i + j]) ^ ord(part[j]))
             all_keys.append(new_key)
         return all_keys
```

Проверка корректности работы функций

```
[5]: text = 'С Новым Годом, друзья!'
     key = get_random_key(len(text))
     enc_text = enc_dec(text, key)
     print(f'Текст: {text}')
     print(f'Ключ: {key}')
     print(f'Шифротекст: {enc_text}')
     print(f'Расшифрованный текст: {enc_dec(enc_text, key)}')

     Текст: С Новым Годом, друзья!
     Ключ: E3IDtle0Mq9CDN1sEVJXv7
     Шифротекст: Ѥ▯еОцЧљ▯ўяЙӧЉЬ▯чSEӧДй▯
     Расшифрованный текст: С Новым Годом, друзья!
```

```
[6]: part='С Новым'
     potential_keys = find_keys(text, part)
     print(f'Список ключей: {potential_keys}')

     Список ключей: ['\x00\x00\x00\x00\x00\x00\x00', 'Ён#\x0cywM', '<O/u\x0eӂ/', '\x1fBV\x02BX\x02', '\x13ӂ!O!u\x08', 'јМн-\x0c\x7f\x02', '\x1d\x00\x0e\x00\x06u\x00', 'Ёг#\n\x0cwA', '2O)\x00\x0eѧM', '\x1fД#\x02Oӂ\x08', '\x15O!BB\x7f|', '\x1fМ6O\x06\x0b\x7f', '\x1d\x0cн\nr\x08\x0b', 'Й\x00)~q|p', 'ЁД]}\x05\x07s', '\x15Ѡ^\t~\x04H']
```

Вывод

В рамках выполнения данной лабораторной работы я освоила на практике применение режима однократного гаммирования.