

Лабораторная работа №8

Основы информационной безопасности

Ищенко Ирина

Российский университет дружбы народов, Москва, Россия

- Ищенко Ирина Олеговна
- НПИбд-02-22

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

Выполнение лабораторной работы

```
def encrypt(text: str, key: list = None):  
    if not key:  
        key = generate_key(length=len(text))  
  
    text_16 = [ord(char) for char in text]  
    key = [ord(el) for el in key]  
  
    print(f"Ключ шифрования:", ' '.join(str(s) for s in key))  
    print(f"Исходный текст:", text)
```

```
encrypted_text = []  
for i in range(len(text)):  
    encrypted_text.append(text_16[i] ^ key[i])  
  
ciphertext = ''.join([chr(i) for i in encrypted_text])  
print(f'Шифротекст: {ciphertext}\n\n')  
  
return ciphertext
```

```
p1 = 'НаВашисходящийот1204'  
p2 = 'ВСеверныйфилиалБанка'  
key = generate_key(20)
```

```
c1 = encrypt(p1, key=key)  
c2 = encrypt(p2, key=key)
```

```
c1_c2 = encrypt(c1, key=c2)
```

```
encrypt(c1_c2, p1)  
encrypt(c1_c2, p2)
```

```
ioithenko@ioithenko:~  
[ioithenko@ioithenko ~]$ python main.py  
Ключ шифрования: 117 79 66 108 111 89 101 53 106 68 110 104 97 73 100 78 77 105 71 85  
Исходный текст: НаВашисходящий1204  
шифротекст: ИхКЧьОЧСЧК|wa  
  
Ключ шифрования: 117 79 66 108 111 89 101 53 106 68 110 104 97 73 100 78 77 105 71 85  
Исходный текст: ВСеверныйфилиалБанка  
шифротекст: А30уЙJQЕ1гаюиСеУж  
  
Ключ шифрования: 1127 1134 1143 1118 1114 1049 1112 1150 1107 1024 1110 1107 1113 1145 1119 1119 1149 1108 1149 1125  
Исходный текст: ИхКЧьОЧСЧК|wa  
шифротекст: ')x|рпг SEUE  
  
Ключ шифрования: 1053 1072 1042 1072 1096 1080 1089 1093 1086 1076 1103 1097 1080 1081 1086 1090 49 50 48 52  
Исходный текст: ')x|рпг SEUE  
шифротекст: ВСеверныйфилиалБанка  
  
Ключ шифрования: 1042 1057 1077 1074 1077 1088 1085 1099 1081 1092 1080 1083 1080 1072 1083 1041 1072 1085 1082 1072  
Исходный текст: ')x|рпг SEUE  
шифротекст: НаВашисходящий1204  
  
[ioithenko@ioithenko ~]$
```

Рис. 1: Вывод программы

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