

Лабораторная работа №8

Основы информационной безопасности

Мишина А. А.

23 мая 2024

- Мишина Анастасия Алексеевна
- НПИбд-02-22

Выполнение лабораторной работы

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

```
7 import string
8
9
10 def generate_key(length: int):
11     """
12     Генерация случайного ключа длины length
13     """
14     return random.sample(string.ascii_letters + string.digits, length)
15
16
17 def encrypt(text: str, key: list = None):
18     """
19     Выводит шифротекст для заданного текста.
20     Если ключа нет, то генерируется случайный ключ
21     """
22     if not key:
23         key = generate_key(length=len(text))
24
25     text_l6 = [ord(char) for char in text]
26     key = [ord(el) for el in key]
27
28     print(f"Ключ шифрования:", ' '.join(str(s) for s in key))
29     print(f"Исходный текст:", text)
30
31     encrypted_text = []
32     for i in range(len(text)):
33         encrypted_text.append(text_l6[i] ^ key[i])
34
35     ciphertext = ''.join([chr(i) for i in encrypted_text])
36     print(f"Шифротекст: {ciphertext}\n\n")
37
38     return ciphertext
39
40
41 p1 = 'НаВашинской1204'
42 p2 = 'ВСеверныйФилиалБанка'
43 key = generate_key(20)
44
45 c1 = encrypt(p1, key=key)
46 c2 = encrypt(p2, key=key)
47
48 c1_c2 = encrypt(c1, key=c2)
49
50 encrypt(c1_c2, p1)
51 encrypt(c1_c2, p2)
```

Рис. 1: Исходный код программы

Запуск main2.py

```
[aamishina@aamishina Documents]$ python main2.py
Ключ шифрования: 57 106 69 83 75 48 51 76 122 66 85 103 89 78 97 101 107 70 108 109
Исходный текст: НаВашисходящийот1204
Шифротекст: Ф%тЪГЖ0лфVК00wу4Zt\Y

Ключ шифрования: 57 106 69 83 75 48 51 76 122 66 85 103 89 78 97 101 107 70 108 109
Исходный текст: ВСеверныйфилиалБанка
Шифротекст: Ы%У00VYIуIл%00Vh0iй

Ключ шифрования: 1067 1099 1136 1121 1150 1136 1038 1031 1091 1030 1133 1116 1121 1150 1114 1140 1115 1147 1110 1117
Исходный текст: Ф%тЪГЖ0лфVК00wу4Zt\Y
Шифротекст: '}x|pwr SEUь€

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|pwr SEUь€
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|pwr SEUь€
Шифротекст: НаВашисходящийот1204

[aamishina@aamishina Documents]$ █
```

Рис. 2: Работа программы

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