

Шифрование гаммированием конечной гаммой.

Кейела Патачона

20 ноября, 2021, Москва, Россия

Российский Университет Дружбы Народов

Цели и задачи

Цель лабораторной работы

Изучение алгоритма гаммированием конечной гаммой.

Выполнение лабораторной работы

Шифр гаммированием конечной гаммой

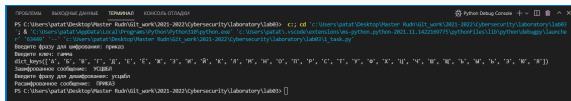
В методе гаммирования шифрование выполняется путем сложения символов исходного текста и ключа по модулю, равному числу букв в алфавите. Если в исходном алфавите, например, 33 символа, то сложение производится по модулю 33. Такой процесс сложения исходного текста и ключа называется в криптографии наложением гаммы.

Контрольный пример (код)

```
1 # Вводим алфавит и ключ
2 word_to_encode = input("Введите фразу для шифрования: ").upper()
3 key_word = input("Введите ключ: ").upper()
4 # Растягиваем ключ на длину слова
5 if len(key_word) < len(word_to_encode):
6     k = (len(word_to_encode) % len(key_word))
7     key_word = '' + key_word * (len(word_to_encode) // len(key_word)) + key_word[:k]
8 # Формируем алфавит и порядковый словарь
9 alphabet = 'АБВГДЕЖЗИЙКЛМНОПРСТУФХЦЧШЩЪЫЬЭЮЯ'
10 alp_dict = {letter: idx + 1 for idx, letter in enumerate(alphabet)}
11 # процесс кодировки
12 encoded_word = ''
13 for word_letter, key_letter in zip(word_to_encode, key_word):
14     encoded_word += list(alp_dict.keys())[alp_dict[word_letter] + alp_dict[key_letter] % len(alphabet))-1]
15 print("Зашифрованное сообщение: ", encoded_word)
16 # процесс декодировки
17 word_to_decode = input("Введите фразу для дешифрования: ").upper()
18 decoded_word = ''
19 for word_letter, key_letter in zip(word_to_decode, key_word):
20     decoded_word += list(alp_dict.keys())[alp_dict[word_letter] - alp_dict[key_letter] % len(alphabet))-1]
21 print("Расшифрованное сообщение: ", decoded_word)
22
```

Figure 1: Программный код

Контрольный пример (алгоритм)



The screenshot shows a Python Debug Console window with the following content:

```
ПРОБЛЕМЫ  ВХОДЯЩИЕ ДАННЫЕ  ТЕРМИНАЛ  КОНСОЛЬ ОТЛАДКИ Python Debug Console + - [] [?] [X]
PS C:\Users\patat\Desktop\Master_Ruh\git_work\2021-2022\Cybersecurity\laboratory\lab03> cd 'C:\Users\patat\Desktop\Master_Ruh\git_work\2021-2022\Cybersecurity\laboratory\lab03'
> & "C:\Users\patat\AppData\Local\Programs\Python\Python38\python.exe" "C:\Users\patat\vscode-extension\src\python_python_2021_11_14\22209773\python\lib\python\debugpy\launcher"
"7" "0x00000000" "C:\Users\patat\Desktop\Master_Ruh\git_work\2021-2022\Cybersecurity\laboratory\lab03\1_task.py"
Введите фразу для отладки: преекс
Введите команду: print
dict_keys(['A', 'B', 'C', 'D', 'E', 'F', 'G', 'H', 'I', 'J', 'K', 'L', 'M', 'N', 'O', 'P', 'Q', 'R', 'S', 'T', 'U', 'V', 'W', 'X', 'Y', 'Z', 'a', 'b', 'c', 'd', 'e', 'f', 'g', 'h', 'i', 'j', 'k', 'l', 'm', 'n', 'o', 'p', 'q', 'r', 's', 't', 'u', 'v', 'w', 'x', 'y', 'z'])
Запрошено сообщение: PCIDBA
Введите фразу для завершения: уааааа
Расширенное сообщение: PRKAS
PS C:\Users\patat\Desktop\Master_Ruh\git_work\2021-2022\Cybersecurity\laboratory\lab03> |
```

Figure 2: Работа кода

Выводы

Изучили работу алгоритма гаммированием конечной гаммой.