Правительство Российской Федерации
ФЕДЕРАЛЬНОЕ ГОСУДАРСТВЕННОЕ АВТОНОМНОЕ
ОБРАЗОВАТЕЛЬНОЕ УЧРЕЖДЕНИЕ ВЫСШЕГО ОБРАЗОВАНИЯ
«НАЦИОНАЛЬНЫЙ ИССЛЕДОВАТЕЛЬСКИЙ УНИВЕРСИТЕТ
«ВЫСШАЯ ШКОЛА ЭКОНОМИКИ»
(НИУ ВШЭ)

Московский институт электроники и математики им. А.Н. Тихонова

ОТЧЕТ
О ПРАКТИЧЕСКОЙ РАБОТЕ № 3
по дисциплине «Математические основы защиты информации»

ШИФРЫ ГАММИРОВАНИЯ

Студент гр. БИБ 201
К.Ш.Ёркулов
«_» ____ 2022 г.

Руководитель
Заведующий кафедрой информационной безопасности кибер физических систем
канд. техн. наук, доцент
_____ О.О. Евсютин
«___» _____ 2022 г.

Москва 2022

СОДЕРЖАНИЕ

1 Задание на практическую работу

Целью данной работы является приобретение навыков программной реализации и криптоанализа применительно к шифрам гаммирования.
В рамках практической работы необходимо выполнить следующее:

- написать программную реализацию следующих шифра Виженера с тремя способами выработки гаммы на основе секретного ключа шифрования:
    1. Повторение короткого лозунга;
    2. Самоключ Виженера по открытому тексту;
    3. Самоключ Виженера по шифртексту;
- изучить методы криптоанализа шифров гаммирования с использованием дополнительных источников;
- провести криптоанализ данных шифров;

2 Краткая теоретическая часть

Гаммирование заключается в наложении на открытый текст некоторой последовательности (гаммы), генерируемой на основе ключа шифрования. Под наложением гаммы на открытый текст обычно подразумевается сложение символов открытого текста с символами гаммы по модулю соответствующего алфавита. Однако в классических шифрах наложение гаммы может означать вычисление значений символов шифртекста на основе значений соответствующих символов открытого текста и гаммы по некоторому правилу.

Классическим представителем шифров гаммирования является шифр Виженера.

Символы алфавита мощностью представляются элементами кольца классов вычетов .

Шифрование заключается в сложении символов открытого текста с символами гаммы по модулю .

Расшифрование заключается в сложении символов шифртекста с символами гаммы по модулю .

В шифре Виженера в качестве ключа шифрования обычно использовалась короткая фраза, называемая лозунгом (паролем), которая циклически повторялась, формируя гамму.

Существует другой подход к формированию псевдослучайной ключевой последовательности — самоключ Виженера. Здесь в качестве начального ключа мы выбираем только один символ, к нему добавляем все символы открытого текста, за

исключением последнего, и таким образом формируем гамму. Либо мы можем формировать гамму, добавляя к начальному символу поочередно символы шифртекста

3 Пример шифрования

Ручное шифрование

1. **Шифрование по короткому лозунгу**

Допустим у нас есть слово “LINUX”, и ключ KEY. Шифрование происходит следующим образом: ключ накладывается по длине ключевого слова (в нашем случае KEYKE), затем получим поочередно для каждого символ зашифрованного текста, беря столбец, определенного по открытому тексту.

Открытый текст: LINUX

Ключ: KEY (ключ при наложении: KEYKE)

Шифртекст: VMLEB

Процесс расшифровки происходит аналогичным способом, вводится шифртекст, затем ключ, и на выходу получим открытый текст.

Шифртекст: VMLEB

Ключ: KEY

Открытый текст: LINUX

2. **Шифрование по открытому ключу**

В данном случае ключ накладывается на открытый текст таким образом чтобы ключ + открытый текст были по размеру открытого текста (mod 26). Например открытый текст ATTACKATDAWN, и ключ LEMON

Открытый текст: ATTACKATDAWN

Ключ: LEMON (ключ при наложении: LEMONATTACKA)

Шифртекст: LXFOPVEFRNHR

Процесс расшифровки происходит аналогичным способом, вводится шифртекст, затем ключ, и на выходу получим открытый текст.

Шифртекст: LXFOPVEFRNHR

Ключ: LEMON

Открытый текст: ATTACKATDAWN

4 Программная реализация

```
PS D:\Programs\VScode\MOZI\Practice_3> & C:/Users/kuva0/AppData/Local/Programs/Python/Python310/python.exe d:/Programs/VScode/MOZI/Practic
e_3/vigenere_openkey.py
Write the message: attacklinux
Write the key: key
Ciphertext : KXRAVDLKXFF
Decrypted Ciphertext: ATTACKLINUX
PS D:\Programs\VScode\MOZI\Practice_3>
```

Рисунок 1. Программная реализация шифра виженера по открытому ключу

```
PS D:\Programs\VScode\MOZI\Practice_3> & C:/Users/kuva0/AppData/Local/Programs/Python/Python310/python.exe d:/Programs/VScode/MOZI/Practic
e_3/vigenere_cipherkey.py
Write the message: attacklinux
Write the key: kali
Ciphertext : KTEIMDPQZXM
Decrypted Ciphertext: ATTACKLINUX
PS D:\Programs\VScode\MOZI\Practice_3>
```

Рисунок 2. Программная реализация шифра виженера по шифртексту.

```
PS D:\Programs\VScode\MOZI\Practice_3> & C:/Users/kuva0/AppData/Local/Programs/Python/Python310/python.exe d:/Programs/VScode/MOZI/Practic
e_3/vigenere_shortslogan.py
Write the message: attacklinux
Write the key: kali
Encrypted Text: KTEIMKWQXUI
Decrypted Text: ATTACKLINUX
PS D:\Programs\VScode\MOZI\Practice_3>
```

Рисунок 2. Программная реализация шифра виженера по короткому лозунгу.

5 Примеры криптоанализа

```
PS D:\Programs\VScode\MOZI\Practice_3> & C:/Users/kuva0/AppData/Local/Programs/Python/Python310/python.exe d:/Programs/VScode/MOZI/Practic
e_3/crypt_vig_open.py
Write the message: KXRAVDLKXFF
Write the key: key
Decrypted Text: ATTACKLINUX
PS D:\Programs\VScode\MOZI\Practice_3>
```

Рисунок 3. Криптоанализ шифра виженера по открытому ключу

```
PS D:\Programs\VScode\MOZI\Practice_3> & C:/Users/kuva0/AppData/Local/Programs/Python/Python310/python.exe d:/Programs/VScode/MOZI/Practic
e_3/crypt_vig_cipher.py
Write the message: KXRKZBVHOPE
Write the key: key
Decrypted Text: ATTACKLINUX
PS D:\Programs\VScode\MOZI\Practice_3>
```

Рисунок 4. Криптоанализ шифра виженера по шифртексту.

```
PS D:\Programs\VScode\MOZI\Practice_3> & C:/Users/kuva0/AppData/Local/Programs/Python/Python310/python.exe d:/Programs/VScode/MOZI/Practic
e_3/crypt_vig_short.py
Write the message: KXRKGIUEJS
Write the key: key
Decrypted Text: ATTACKKALI
PS D:\Programs\VScode\MOZI\Practice_3>
```

Рисунок 4. Криптоанализ шифра виженера по короткому лозунгу.

6 Выводы о проделанной работе

По ходу практической работы было выполнено изучение и закрепление навыков по шифрам гаммирования, изучили как работает шифр Виженера. Данный шифр легко поддается взлому, то есть перебором ключа можно взломать зашифрованное сообщение.

7 Список использованных источников

Шифр Виженера — Википедия (wikipedia.org)

Шифр Вижинера и его разгадка / Хабр (habr.com)

Шифр Виженера | это... Что такое Шифр Виженера? (academic.ru)

Шифр Виженера: уязвимая криптосистема, из которой в итоге выросли одноразовые шифр-блокноты | Блог Касперского (kaspersky.ru)