СОДЕРЖАНИЕ

1. Постановка задачи

Тема работы: методы программной реализации симметричной криптографической защиты данных

Цели работы: рассмотреть понятие криптографической защиты информации; ознакомиться с классификацией методов криптографического преобразования информации; изучить методы симметричного шифрования.

Задание к лабораторной работе: создать программу, осуществляющую шифрование и дешифрование введённых текстовых данных согласно выбранному варианту. Для данной работы выбран вариант №39: шифр Вернама.

2. Шифр Вернама

Шифр Вернама, или одноразовый блокнот, был изобретён в 1917 году Гильбертом Вернамом в компании AT&T. Шифр Вернама является примером системы с абсолютной криптографической стойкостью, при этом он считается одной из простейших криптосистем [1].

Одноразовый блокнот является большой неповторяющейся последовательностью символов ключа, распределённых случайным образом.

Для каждого сообщения Вернам брал такую же по длине последовательность нулей и единиц – ключевую последовательность (гамму), каждый её бит складывал с соответствующим битом сообщения и отправлял адресату [2].

2.1. Зашифрование и расшифрование

При зашифровании и расшифровании используется ключевая последовательность, которая должна быть равномерно распределённой случайной последовательностью. Равномерно распределённая последовательность – это последовательность, каждый знак которой появляется равновероятно.

Пронумеруем буквы русского алфавита. В таблице 1 приведена эта нумерация.

Таблица 1 – Нумерация русского алфавита

А	Б	В	Г	Д	Е	Ё	Ж	З	И	Й	К	Л	М	Н	О	Я
00	01	02	03	04	05	06	07	08	09	10	11	12	13	14	15	
П	Р	С	Т	У	Ф	Х	Ц	Ч	Ш	Щ	Ъ	Ы	Ь	Э	Ю	32
16	17	18	19	20	21	22	23	24	25	26	27	28	29	30	31	

В таблице 2 представлен пример зашифрования. Первая строка таблицы – открытый текст, вторая – ключевая последовательность, третья – шифротекст.

Посчитаем код для первой буквы шифротекст. Код обозначим переменной К: (К(Р) + К(М)) mod 33 = (17 + 13) mod 33 = -3, где “33” – мощность выбранного алфавита.

Таблица 2 – Пример зашифрования

Р	У	С	С	К	И	Й	А	Л	Ф	А	В	И	Т
М	Ы	Г	Д	Ш	Н	Ё	М	М	Э	Й	М	А	Э
Э	О	Ф	Х	Г	Ц	П	М	Ш	С	Й	О	И	П

Для шифрования необходимо вычитать код буквы ключевой последовательности из кода буквы шифротекст: (К(М) - К(Э)) mod 33 = (13 - 30) mod 33 = 17. В таблице 3 представлен пример расшифрования шифротекста, полученного в таблице 2.

Таблица 3 – Пример расшифрования

М	Ы	Г	Д	Ш	Н	Ё	М	М	Э	Й	М	А	Э
Э	О	Ф	Х	Г	Ц	П	М	Ш	С	Й	О	И	П
Р	У	С	С	К	И	Й	А	Л	Ф	А	В	И	Т

2.2. Абсолютно стойкие и достаточно стойкие шифры

Абсолютно стойкий шифр – это такой шифр, который нельзя взломать ни теоретически, ни практически. Злоумышленник может применять метод грубой силы, но даже если перебрать все варианты ключевой последовательности, то он всё равно не поймет, удалось ли взломать сообщение.

Шифр Вернама является абсолютно стойким, потому что единственное, что мы про него знаем, – это длина шифротекста. Существует множество фраз одинаковой длины. Навскидку можно привести слова одинаковой длины: диск, яхта, торт, порт и многие другие.

2.3. Криптоанализ

Рассмотрим случай, когда возможно взломать шифр Вернама. Используем дважды одну и ту же гамму. Назовём гамму буквой Г и зашифруем два разных сообщения – А и Б – этой гаммой. Получим два шифротекста Ш1 и Ш2.

Если теперь сложить по модулю получившиеся шифротексты, то значение гаммы уничтожится: Г складывается сама с собой, и каждый его разряд будет равен 0: $0 \oplus 0 = 0$, $1 \oplus 1 = 0$. В таблице 4 представлен этот пример взлома шифра Вернама.

Таблица 4 – Пример взлома

А	0	1	1	1
Г	0	1	1	0
Б	1	1	0	1
Г	0	1	1	0
$А \oplus К \oplus Б \oplus К = А \oplus Б$	1	0	1	0

Когда мы получили выражение А ⊕ Б, можно применить атаку методом грубой силы. Мы будем подбирать А. Если угадаем правильно, настоящее А и наше подобранное А взаимоуничтожатся, и мы увидим открытое сообщение Б. Если получим осмысленное сообщение Б – шифр взломан.

2.4. Достоинства и недостатки

Достоинства:

– простой процесс шифрования;

– если длина гаммы равна длине текста, шифр является невзламываемым.

Недостатки:

– в использовании шифра нет смысла, если мы имеем защищённый канал передачи (незачем шифровать);

– при потере хотя бы одного бита, можем получить другое сообщение.

3. Реализация

На рисунке 1 представлен снимок экрана разработанной программы шифрования сообщения при помощи алгоритма Вернама.

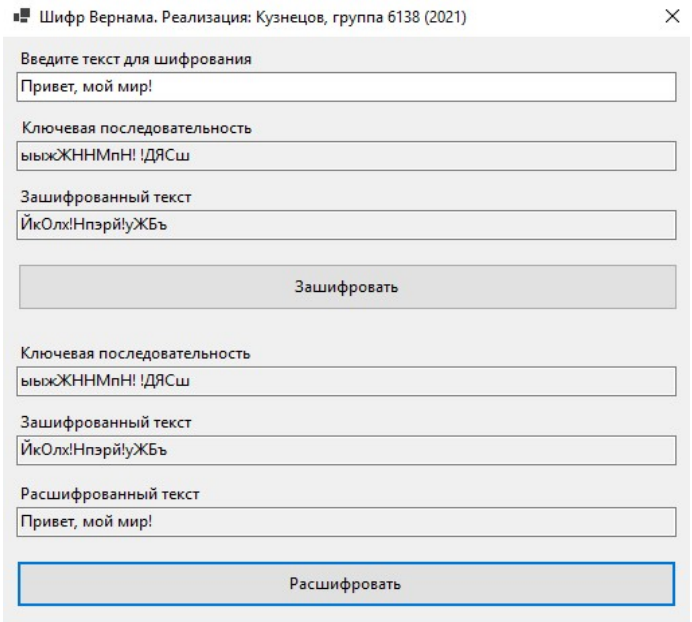

Рисунок 1 – Снимок экрана программы

В окно ввода нужно вести открытый текст, по нажатию на кнопку “Зашифровать” программа создаст случайную последовательность символов – ключевая последовательность и зашифрует открытый текст, используя эту последовательность. По нажатию на кнопку “Расшифровать” шифротекст расшифруется.

Исходный код программы доступен в публичном репозитории по следующей ссылке – https://github.com/apkuznetsov/infosec-math-2021. В приложении А представлен код на языке C#, разработанного алгоритма шифрования (класс VernamCipher).

ПРИЛОЖЕНИЕ А ИСХОДНЫЙ КОД АЛГОРИТМА

```
using System;
using System.Text;

namespace Vernam
{
    public static class VernamCipher
    {
        private static readonly string ALPHABET = " ,!" +
            "АБВГДЕЁЖЗИЙКЛМНОПРСТУФХЦЧШЩЪЫЬЭЮЯ" +
            "абвгдеёжзийклмнопрстуфхцчшщъыьэюя ";

        private static int Code(char symbol)
        {
            return ALPHABET.IndexOf(symbol);
        }

        public static string GenerateKeyseq(int textLen)
        {
            StringBuilder sb = new StringBuilder(textLen);

            Random random = new Random();
            int len = ALPHABET.Length;
            int idx;
            for (int i = 0; i < textLen; i++)
            {
                idx = random.Next(len);
                sb.Append(ALPHABET[idx]);
            }

            return sb.ToString();
        }

        public static string Encrypt(string text, string keyseq)
        {
            StringBuilder sb = new StringBuilder(text.Length);

            int mod = ALPHABET.Length;
            int idx;
            for (int i = 0; i < text.Length; i++)
            {
                idx = (Code(text[i]) + Code(keyseq[i])) % mod;
                sb.Append(ALPHABET[idx]);
            }

            return sb.ToString();
        }

        public static string Decrypt(string text, string keyseq)
        {
            StringBuilder sb = new StringBuilder(text.Length);

            int mod = ALPHABET.Length;
            int idx;
            for (int i = 0; i < text.Length; i++)
            {
                idx = (Code(text[i]) - Code(keyseq[i])) % mod;
                idx = idx < 0 ? mod + idx : idx % mod;
                sb.Append(ALPHABET[idx]);
            }

            return sb.ToString();
        }}}
```

СПИСОК ИСПОЛЬЗОВАННЫХ ИСТОЧНИКОВ

1 Фомичёв В. М. Дискретная математика и криптология: Курс лекций / под ред. Н. Д. Подуфалов — М.: Диалог-МИФИ, 2013. — С. 239—246. — 397 с. — ISBN 978-5-86404-185-7

2 Лекция 5. Шифр Вернама [Электронный ресурс]. URL: https://stepik.org/lesson/288961/step/1 (дата обращения: 05.04.2021).