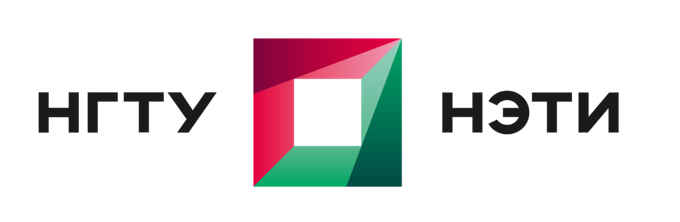
# Министерство науки и Высшего образования Российской Федерации

Федеральное государственное бюджетное образовательное   
учреждение высшего образования

«Новосибирский государственный технический университет»



Кафедра теоретической и прикладной информатики

Лабораторная работа № 1  
по дисциплине «Программные средства защиты информации»

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
|  | Факультет: | ПМИ |  |  | |
| Группа: | ПМИМ-21 |  |  | |
| Бригада: | 3 | | |  | |
| Студенты: | Бортников. Н, Ефименко А., Кутузова И. | | |  | |
|  |  |  |  | |
| Преподаватель: | Авдеенко Т.В. |  |  | |

Новосибирск

2022

1. **Формулировка задания**

**Задание:**

I. Реализовать приложение для шифрования, позволяющее выполнять следующие действия:

1. Шифровать данные в режиме однократного гаммирования:

1) шифруемый текст должен храниться в файле;

2) ключ шифрования должен задаваться случайным образом;

3) зашифрованный текст должен сохраняться в один файл, а использовавшийся при шифровании ключ – в другой;

4) в процессе шифрования предусмотреть возможность просмотра и изменения ключа, шифруемого и зашифрованного текстов в двоичном, шестнадцатеричном и символьном виде.

2. Шифровать данные при помощи каждого заданного в варианте скремблера:

1) шифруемый текст должен храниться в одном файле, начальное значение скремблера – в другом;

2) зашифрованный текст должен сохраняться в файл;

3) в процессе шифрования предусмотреть возможность просмотра и изменения начального значения скремблера, шифруемого и зашифрованного текстов в двоичном, шестнадцатеричном и символьном виде.

3. Проводить исследование генерируемой каждым скремблером последовательности псевдослучайных чисел при заданном начальном ключе:

1) получать период скремблера;

2) проверять равномерность последовательности по критерию;

3) исследовать последовательность на свойства сбалансированности, цикличности, корреляции.

II. Реализовать приложение для дешифрования, позволяющее выполнять следующие действия:

1. Дешифровать данные в режиме однократного гаммирования:

1) зашифрованный текст должен храниться в одном файле, ключ – в другом;

2) расшифрованный текст должен сохраняться в файл;

3) в процессе дешифрования предусмотреть возможность просмотра и изменения ключа, зашифрованного и расшифрованного текстов в двоичном, шестнадцатеричном и символьном виде.

2. Расшифровать данные при помощи каждого заданного в варианте скремблера:

1) зашифрованный текст должен храниться в одном файле, начальное значение скремблера – в другом;

2) зашифрованный текст должен сохраняться в файл;

3) в процессе дешифрования предусмотреть возможность просмотра и изменения начального значения скремблера, зашифрованного и расшифрованного текстов в двоичном, шестнадцатеричном и символьном виде.

III. С помощью реализованных приложений выполнить следующие задания:

1. Протестировать правильность работы разработанных приложений.

2. Определить ключ, с помощью которого зашифрованный текст может быть преобразован в некоторый осмысленный фрагмент текста, представляющий собой один из возможных вариантов прочтения открытого текста.

3. Определить и выразить аналитически, каким образом, имея зашифрованные тексты двух телеграмм, злоумышленник может получить обе телеграммы, не зная ключа и не стремясь его определить. Привести пример.

4. Исследовать генерируемые каждым скремблером последовательности псевдослучайных чисел при различных начальных значениях скремблера.

5. Сделать выводы о проделанной работе.

**Вариант 3:**

|  |  |
| --- | --- |
| Скремблеры | |
|  |  |

1. **Описание разработанного программного средства**

Решение задачи реализовано в виде программы, написанной на языке C#. Интерфейс, через который осуществляется работа с ней, имеет следующий вид:

1. **Тестирование**

* Тест 1

1. **Вывод**
2. **Код программы**
3. **Защита**
4. Преимущества и недостатки однократного гаммирования.

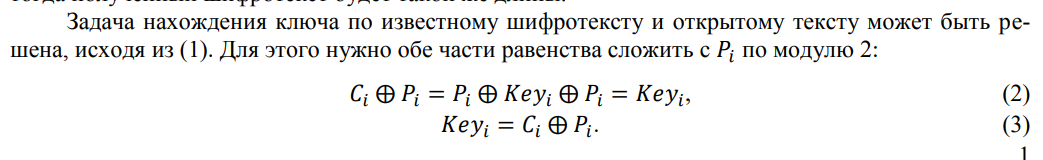


Простота реализации

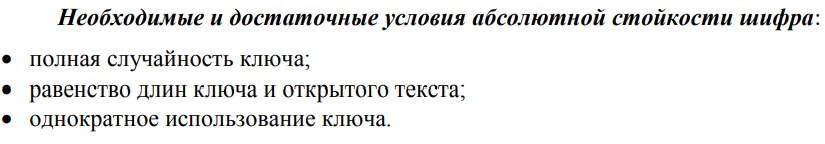
1. Почему размерность открытого текста должна совпадать с ключом?

Ну… чтобы приблизиться к абсолютно стойкому шифру. В противном случае для получения открытого текста потребуется подобрать длину гаммы, проанализировать блоки шифротекста угаданной длины, подобрать биты гаммы.

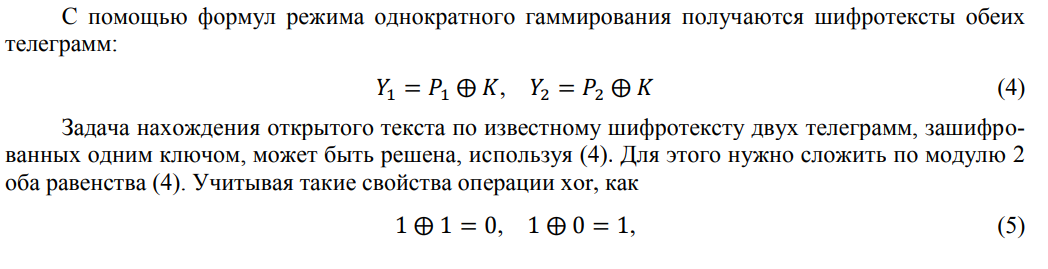
1. Как по открытому тексту и шифротексту получить ключ?

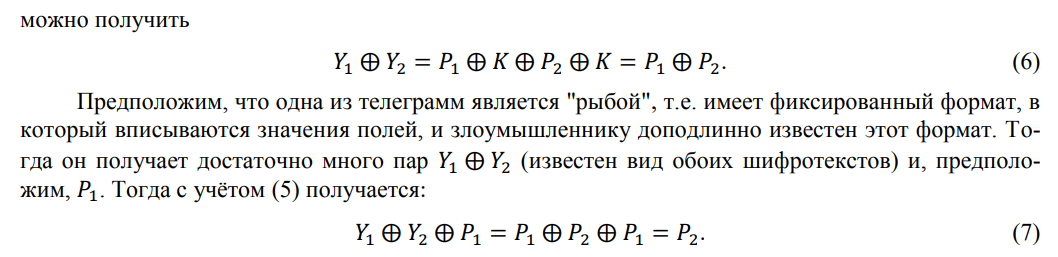


1. Необходимые и достаточные условия абсолютной стойкости шифра.



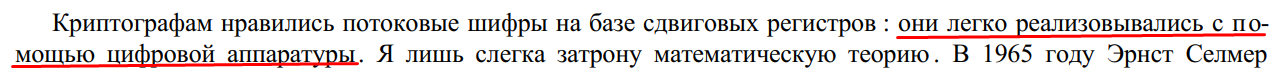
1. Как, зная текст одного из сообщений ( или ), определить другое, не пытаясь определить ключ?

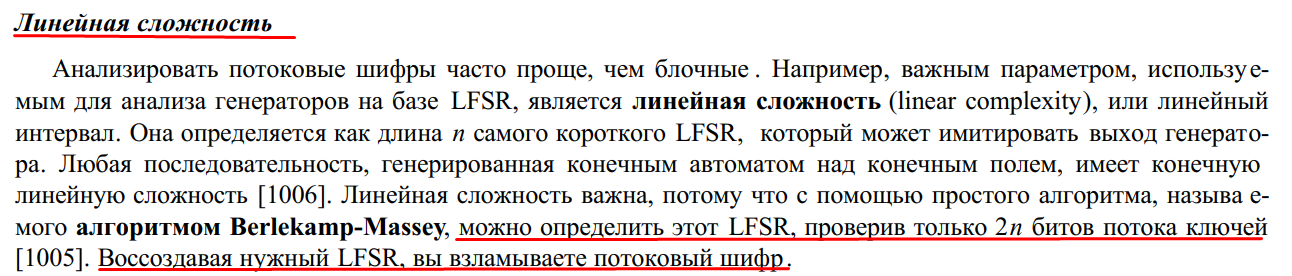




1. Преимущества и недостатки использования скремблера.

Тут че то не нашла инфы





1. Свойства, которыми должна обладать псевдослучайная последовательность, генерируемая скремблером.

