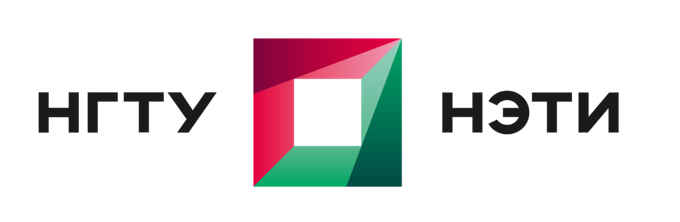
# Министерство науки и Высшего образования Российской Федерации

Федеральное государственное бюджетное образовательное   
учреждение высшего образования

«Новосибирский государственный технический университет»



Кафедра теоретической и прикладной информатики

Лабораторная работа № 3  
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

2023

1. **Формулировка задания**

**Задание:**

I. Реализовать приложение для шифрования, позволяющее выполнять перечисленные действия.

1. Шифровать данные по заданному в варианте алгоритму:

1) шифруемый текст должен храниться в одном файле, а ключ

шифрования – в другом;

2) зашифрованный текст должен сохраняться в файл;

3) в процессе шифрования предусмотреть возможность просмотра и изменения ключа, шифруемого и зашифрованного текстов в шестнадцатеричном и символьном виде;

4) программа должна показывать время шифрования.

2. Исследовать лавинный эффект (исследования проводить на од-

ном блоке текста):

1) для бита, который будет изменяться, приложение должно позволять задавать его позицию (номер) в открытом тексте или в ключе;

2) приложение должно уметь после каждого раунда шифрования подсчитывать число бит, изменившихся в зашифрованном тексте при изменении одного бита в открытом тексте либо в ключе;

3) приложение может строить графики зависимости числа бит, изменившихся в зашифрованном тексте, от раунда шифрования, либо графики можно строить в стороннем ПО, но тогда приложение для шифрования должно сохранять в файл необходимую для построения графиков информацию.

II. Реализовать приложение для дешифрования, позволяющее дешифровать данные по заданному в варианте алгоритму.

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 шестнадцатеричном и символьном виде.

III. Реализовать приложение, вычисляющее значения 1–4 критериев для алгоритмов DES и ГОСТ. Можно взять стороннюю реализацию того алгоритма, который не указан в варианте.

IV. С помощью реализованных приложений выполнить следующие задания.

1. Протестировать правильность работы разработанных приложений.

2. Исследовать лавинный эффект при изменении одного бита в открытом тексте и в ключе: построить графики зависимостей числа бит, изменившихся в зашифрованном сообщении, от раунда шифрования (всего должно быть построено два графика).

3. Сравнить значения критериев 1–4 для алгоритмов DES и ГОСТ при изменении одного бита в блоке открытого текста и одного бита в ключе при использовании одного и того же сообщения. Сообщение должно состоять хотя бы из пяти блоков (чем больше, тем точнее будут оценки критериев 1–4).

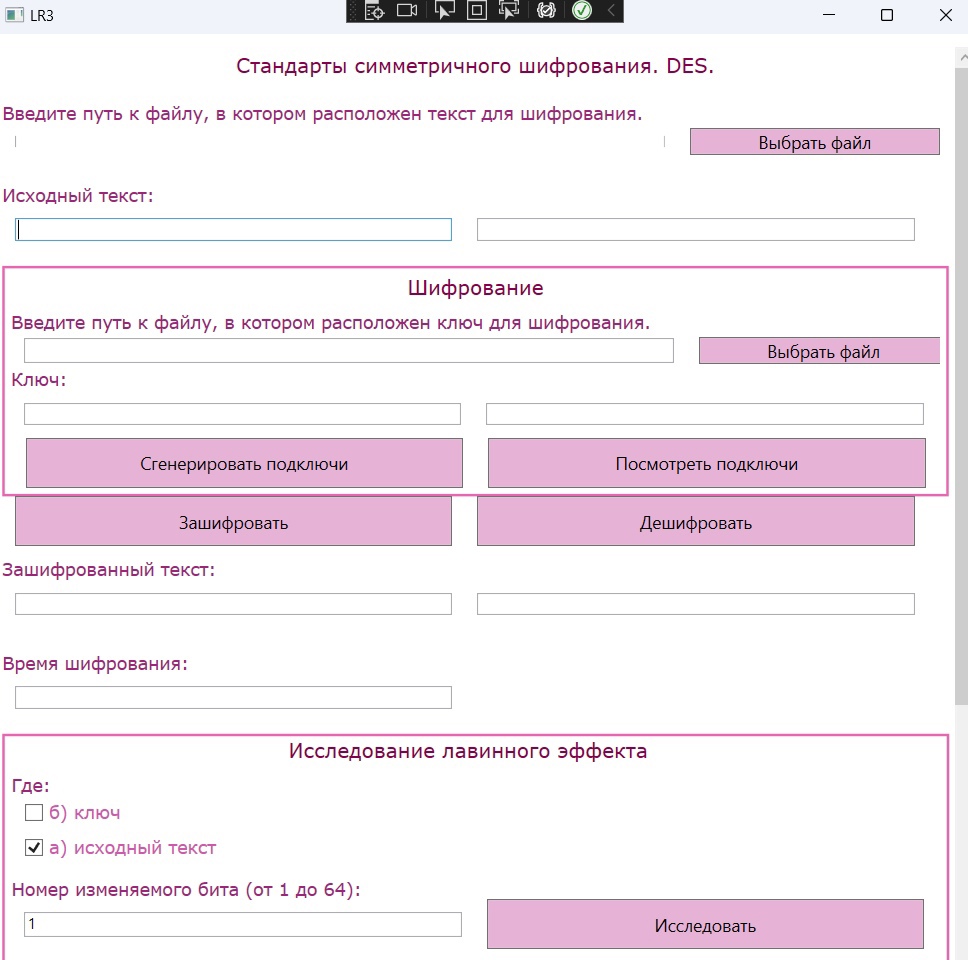
4. Сделать выводы о проделанной работе.

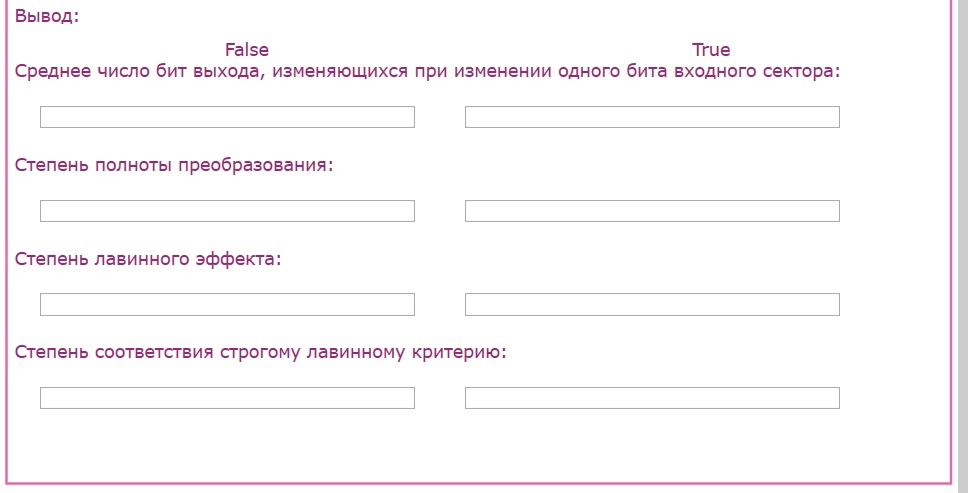
**Вариант 3:**

|  |
| --- |
| DES (нечетный) |

1. **Описание разработанного программного средства**

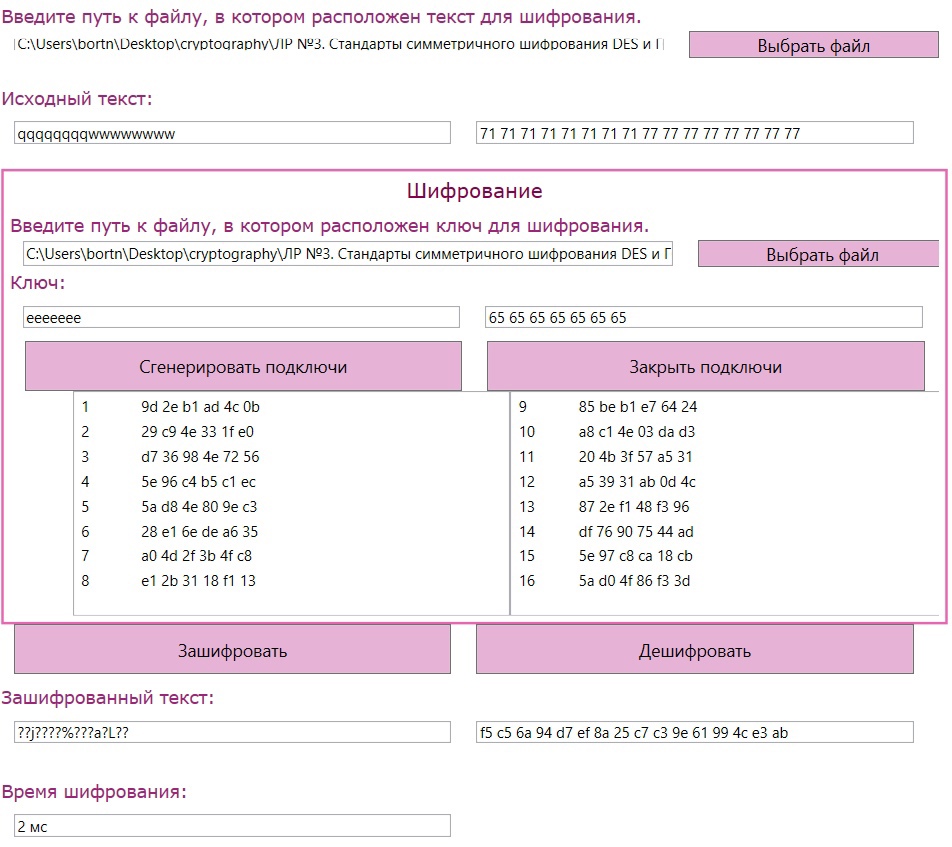
Решение задачи реализовано в виде программы, написанной на языке C#. Интерфейс, через который осуществляется работа с ней, имеет следующий вид:



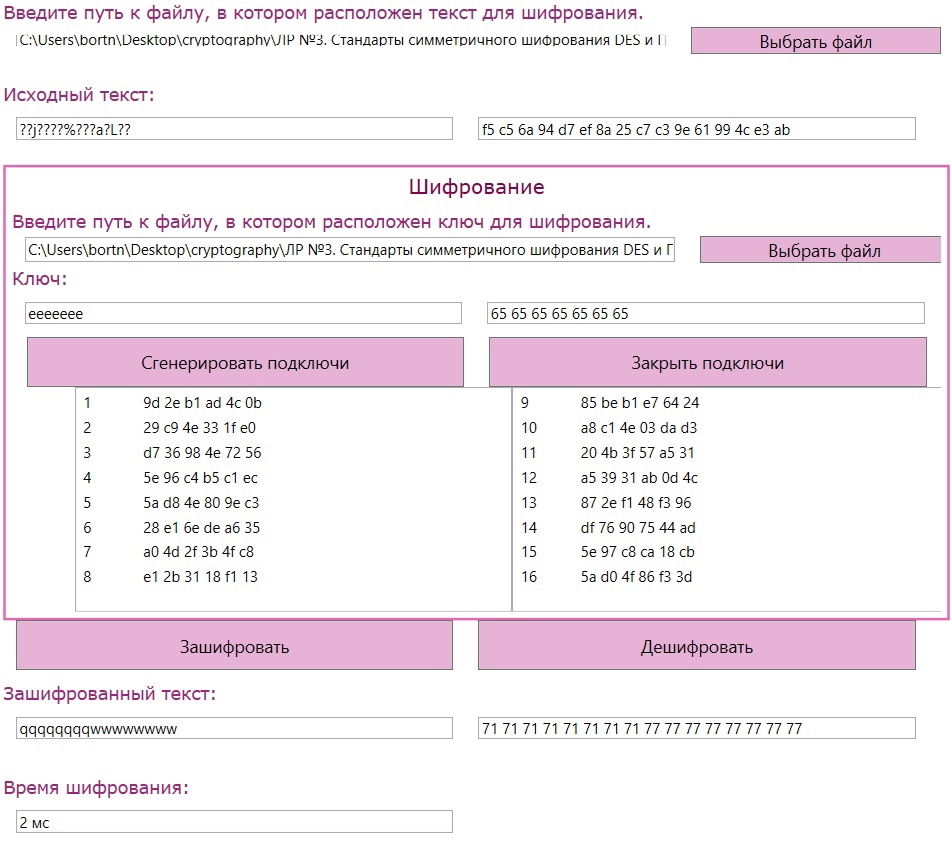


1. **Тестирование**

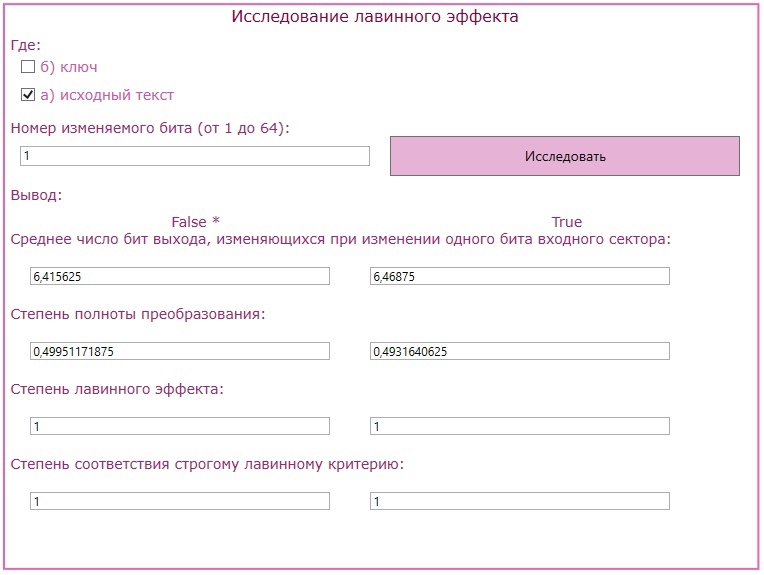
* Тест 1. Шифрование

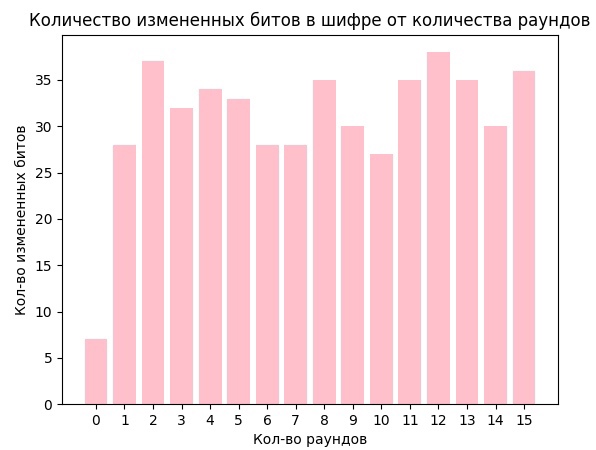


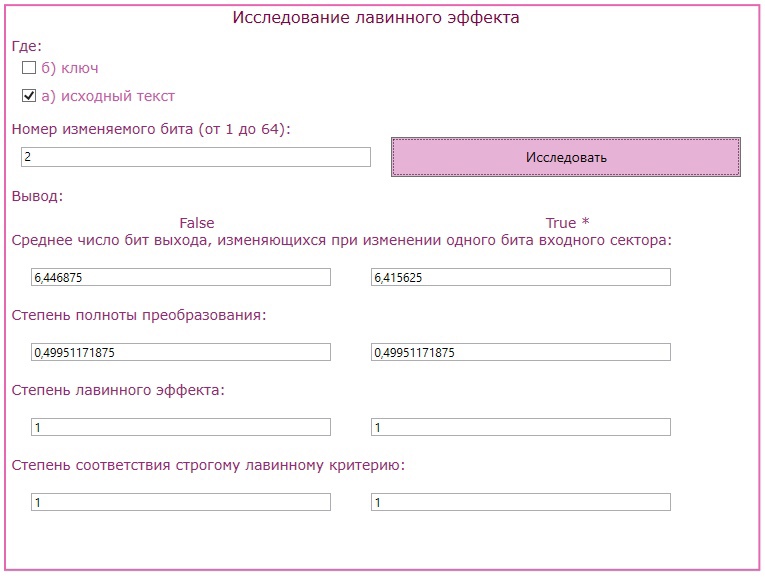
* Тест 2. Дешифрование

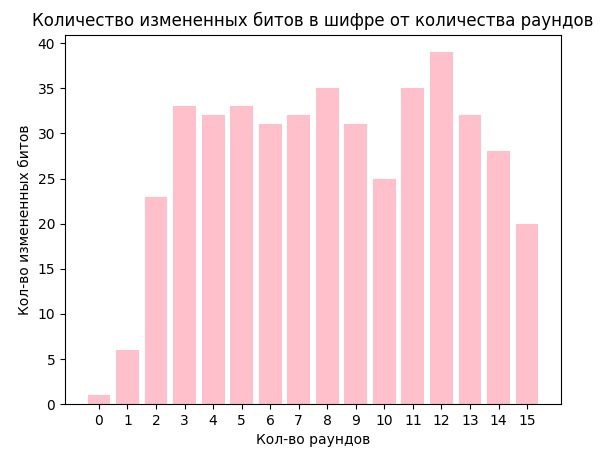


* Тест 3. Исследование лавинного эффекта исходного текста

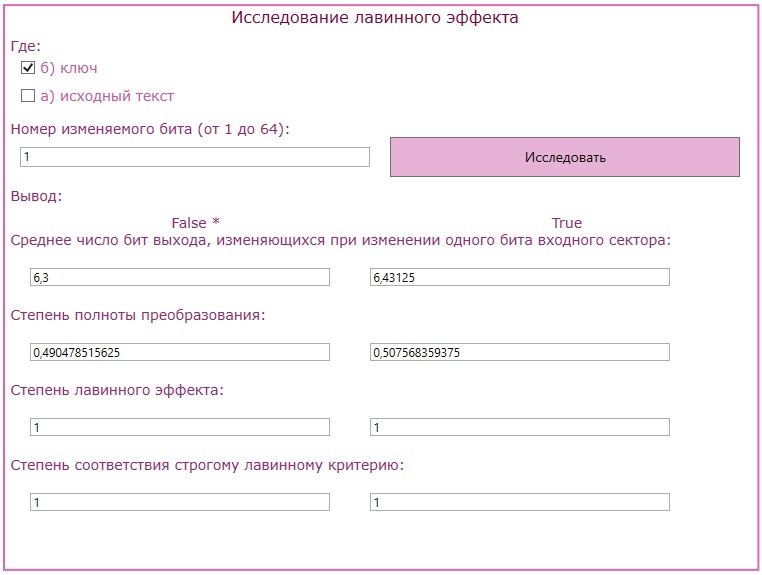


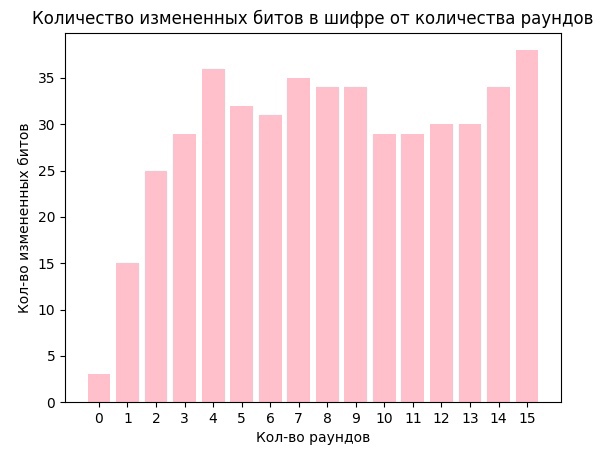


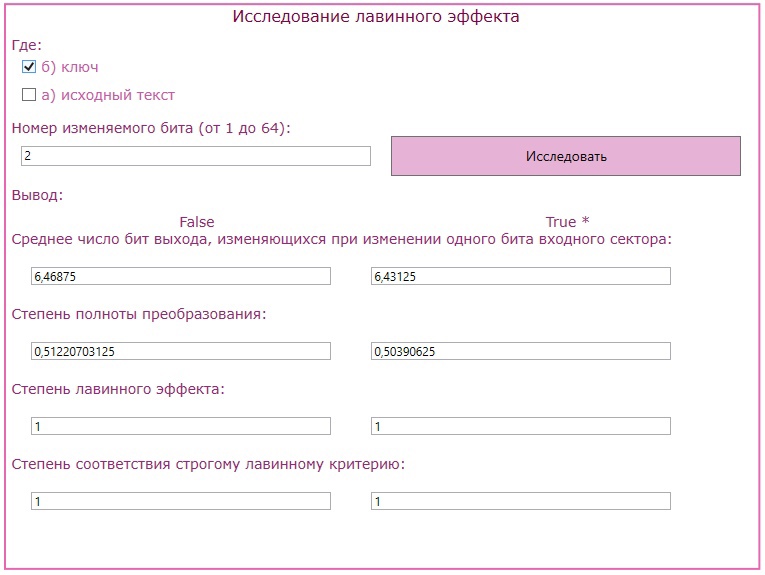


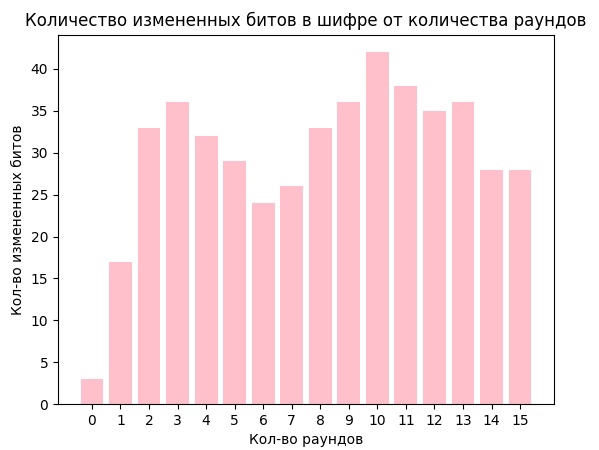


* Тест 4. Исследование лавинного эффекта ключа









1. **Вывод**

* На лабораторной работе мы реализовали приложение, позволяющее шифровать и дешифровать информацию алгоритмом DES. Был реализован и проверен лавинный эффект.

1. **Защита**
2. Преимущества и недостатки однократного гаммирования.

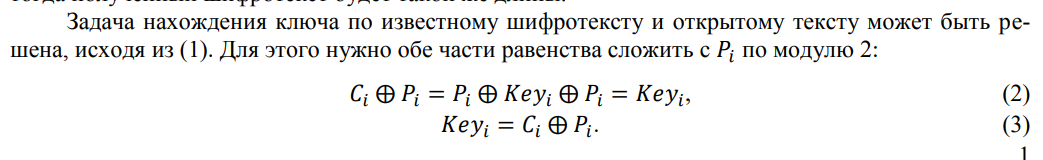


Простота реализации

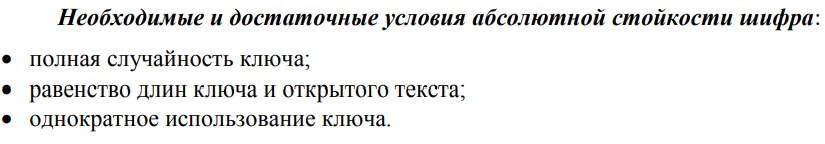
1. Почему размерность открытого текста должна совпадать с ключом?

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.

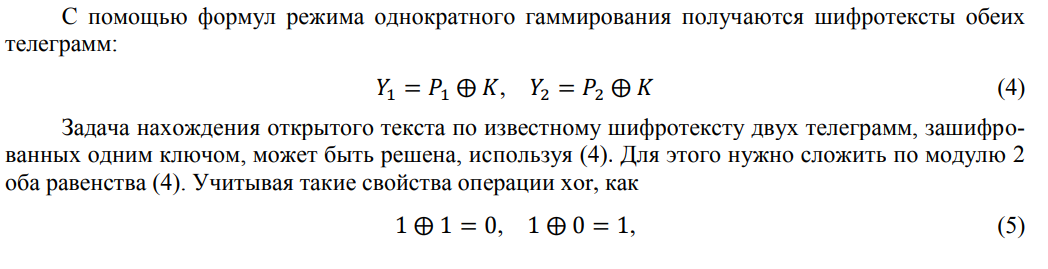
1. Как по открытому тексту и шифротексту получить ключ?

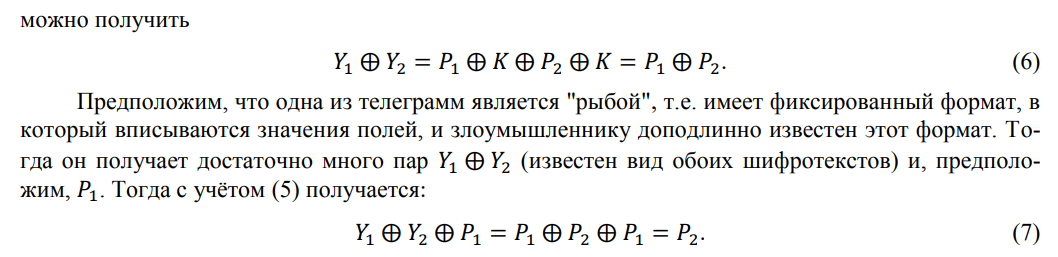


1. Необходимые и достаточные условия абсолютной стойкости шифра.



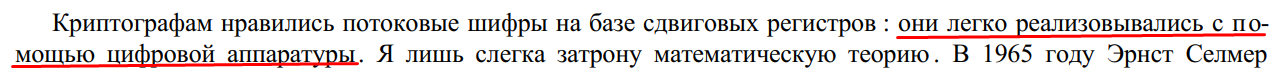
1. Как, зная текст одного из сообщений ( или ), определить другое, не пытаясь определить ключ?

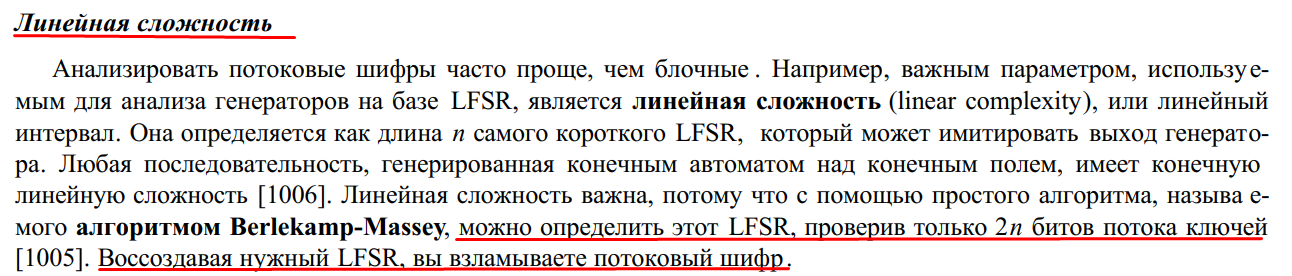




1. Преимущества и недостатки использования скремблера.

Тут че то не нашла инфы





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

