**МИНИСТЕРСТВО ЦИФРОВОГО РАЗВИТИЯ,
СВЯЗИ И МАССОВЫХ КОММУНИКАЦИЙ РОССИЙСКОЙ ФЕДЕРАЦИИ**

**ФЕДЕРАЛЬНОЕ ГОСУДАРСТВЕННОЕ БЮДЖЕТНОЕ ОБРАЗОВАТЕЛЬНОЕ
УЧРЕЖДЕНИЕ ВЫСШЕГО ОБРАЗОВАНИЯ
«САНКТ-ПЕТЕРБУРГСКИЙ ГОСУДАРСТВЕННЫЙ УНИВЕРСИТЕТ
ТЕЛЕКОММУНИКАЦИЙ ИМ. ПРОФ. М.А. БОНЧ-БРУЕВИЧА»
(СПбГУТ)**

Санкт-Петербургский колледж телекоммуникаций им. Э.Т. Кренкеля

СПбГУТ))) Документ подписан простой электронной подписью

Сертификат: 008a56eb36a1808f06
Владелец: Машков Георгий Михайлович
Действителен с 07.05.2022 по 06.05.2027

УТВЕРЖДАЮ
Заместитель директора
по учебной работе
_____ Н.В. Калинина
17 марта 2022 г

МЕТОДИЧЕСКИЕ УКАЗАНИЯ ПО ВЫПОЛНЕНИЮ ПРАКТИЧЕСКИХ РАБОТ

по междисциплинарному курсу
МДК.02.02. КРИПТОГРАФИЧЕСКАЯ ЗАЩИТА ИНФОРМАЦИИ

по специальности

10.02.04 Обеспечение информационной безопасности телекоммуникационных систем

среднего профессионального образования

Санкт-Петербург
2022

МДК.02.02. Криптографическая защита информации. Методические указания по выполнению практических работ.

Составил: Кривоносова Н.В. – Санкт-Петербург, 2022.

Методические указания содержат описания практических занятий, предусмотренных рабочей программой **МДК.02.02. Криптографическая защита информации**. Каждая работа рассчитана на 2 академических часа, общий объём составляет 24 часа. Методические указания предназначены для обучающихся очной формы обучения по специальности 10.02.04 Обеспечение информационной безопасности телекоммуникационных систем.

Рассмотрено и одобрено предметной (цикловой) комиссией информационной безопасности телекоммуникационных систем Санкт-Петербургского колледжа телекоммуникаций им. Э.Т. Кренкеля.

СОДЕРЖАНИЕ

Практическая работа 1
СТЕГАНОГРАФИЧЕСКИЕ МЕТОДЫ СКРЫТИЯ ИНФОРМАЦИИ

1. **Цель работы**: ознакомление с технологиями стеганографического скрытия информации, понять принципы их работы и применение в современном мире.

2. **Задачи работы:**
   - Изучить теоретические основы стеганографии и методы скрытия информации в мультимедийных файлах;
   - Ознакомиться с программными средствами для реализации стеганографической передачи информации;
   - Научиться использовать выбранные программные средства для создания стеганографических сообщений;
   - Применить полученные знания для решения задач по скрытию информации в графических и звуковых файлах.

Студент должен:
Иметь практический опыт:
- установке, настройке, испытаниях и конфигурировании программных и программно-аппаратных в том числе криптографических средств защиты информации в оборудовании ИТКС;

Уметь:
- проводить контроль показателей и процесса функционирования программных и программно-аппаратных, в том числе криптографических средств защиты информации;
- проводить восстановление процесса и параметров функционирования программных и программно-аппаратных, в том числе криптографических средств защиты информации;
- проводить техническое обслуживание и ремонт программных и программно-аппаратных, в том числе криптографических средств защиты информации.

Знать:
- возможные угрозы безопасности информации в ИТКС;
- способы защиты информации от несанкционированного доступа (далее – НСД) и специальных воздействий на неё;
- типовые программные и программно-аппаратные средства защиты информации в информационно-телекоммуникационных системах и сетях;

ПК:
- ПК 2.1. Производить установку, настройку, испытания и конфигурирование программных и программно-аппаратных, в том числе криптографических средств защиты информации от несанкционированного доступа и специальных воздействий в оборудование информационно – телекоммуникационных систем и сетей..

3. **Подготовка к работе**
   Познакомьтесь с материалами теоретической части работы, изложенных в приложении 1
   Подготовить бланк отчета

4. **Задание и порядок выполнения работы**
   - Изучить теоретические основы стеганографии и методы скрытия информации в мультимедийных файлах;
   - Ознакомиться с программными средствами для реализации стеганографической передачи информации;

- Научиться использовать выбранные программные средства для создания стеганографических сообщений;
- Применить полученные знания для решения задач по скрытию информации в графических и звуковых файлах.

5. Содержание отчета

1. название и цель работы;
2. перечень осваиваемых компетенций;
3. задание;
4. исходные данные по заданию/варианту;
5. ход выполнения работ;
6. выводы по работе;

Приложение 1

Краткие сведения из теории

Стеганография - наука о том, как скрыть наличие сообщения в некотором другом сообщении. Сегодня стеганографические методы часто используются в информационной безопасности для передачи секретной информации, такой как личные данные, финансовые документы и т.д. Кроме того, стеганография также используется в целях защиты авторских прав, например, для помещения невидимых водяных знаков в графические файлы. Стеганография может быть использована в различных типах файлов, включая изображения, аудио, видео и текстовые файлы. Некоторые методы стеганографии основаны на замене битов данных, в то время как другие методы используют изменение цветовых значений в графических файлах.

Приложение 2

Самостоятельная работа к практическому занятию

Самостоятельная работа по теме занятия включает в себя:

- изучение теоретического материала лекционных занятий, учебной литературы, Интернет-ресурсов, раздела «Краткие сведения из теории» настоящего описания ПЗ;
- выполнение практических заданий.

Практическая работа 2
ПРИМЕНЕНИЕ МЕТОДОВ ШИФРОВАНИЯ ПЕРЕСТАНОВКОЙ

1. Цель работы: ознакомление с применением методов шифрования перестановкой.

2. Задачи работы:

- Изучить теоретические основы шифрования перестановкой.
- Ознакомиться с примерами шифров, основанных на перестановке символов.
- Практически реализовать алгоритм шифрования перестановкой на языке программирования.
- Протестировать работу алгоритма на различных входных данных.

Студент должен:

Иметь практический опыт:

- установке, настройке, испытаниях и конфигурировании программных и программно-аппаратных в том числе криптографических средств защиты информации в оборудовании ИТКС;

Уметь:

- выявлять и оценивать угрозы безопасности информации в ИТКС;
- настраивать и применять средства защиты информации в операционных системах, в том числе средства антивирусной защиты;
- проводить установку и настройку программных и программно-аппаратных, в том числе криптографических средств защиты информации;
- проводить техническое обслуживание и ремонт программных и программно-аппаратных, в том числе криптографических средств защиты информации.

Знать:

- возможные угрозы безопасности информации в ИТКС;
- способы защиты информации от несанкционированного доступа (далее – НСД) и специальных воздействий на неё;

ПК:

- ПК 2.1. Производить установку, настройку, испытания и конфигурирование программных и программно-аппаратных, в том числе криптографических средств защиты информации от несанкционированного доступа и специальных воздействий в оборудование информационно – телекоммуникационных систем и сетей..
- ПК 2.2. Поддерживать бесперебойную работу программных и программно-аппаратных, в том числе криптографических средств защиты информации в информационно – телекоммуникационных системах и сетях.

3. Подготовка к работе

Познакомьтесь с материалами теоретической части работы, изложенных в приложении 1

Подготовить бланк отчета

4. Задание и порядок выполнения

1. Написать программу на языке программирования, которая принимает на вход строку символов и ключ для шифрования перестановкой.
2. Реализовать алгоритм шифрования перестановкой символов в строке с помощью заданного ключа.
3. Вывести зашифрованную строку на экран.
4. Реализовать алгоритм дешифрования зашифрованной строки с помощью заданного ключа.
5. Вывести дешифрованную строку на экран.

5. Содержание отчета

1. название и цель работы;
2. перечень осваиваемых компетенций;
3. задание;
4. исходные данные по заданию/варианту;
5. ход выполнения работ;
6. выводы по работе;
7. ответы на контрольные вопросы.

Приложение 1

Краткие сведения из теории

Шифрование перестановкой – это один из методов шифрования, при котором символы исходного текста переставляются в заданном порядке, чтобы получить зашифрованный текст. Для шифрования и дешифрования используется ключ – последовательность чисел или символов, определяющая порядок перестановки символов. Основной принцип шифрования перестановкой заключается в том, что зашифрованная информация не имеет смысла для тех, кто не знает ключа для дешифровки. Однако этот метод не является достаточно надежным и безопасным для защиты конфиденциальной информации.

Приложение 2

Самостоятельная работа к практическому занятию

Самостоятельная работа по теме занятия включает в себя:

- изучение теоретического материала лекционных занятий, учебной литературы, Интернет-ресурсов, раздела «Краткие сведения из теории» настоящего описания ПЗ;
- выполнение практических заданий.

Практическая работа 3
ПРИМЕНЕНИЕ МЕТОДОВ ШИФРОВАНИЯ ЗАМЕНОЙ

1. **Цель работы**: Ознакомление с принципами работы методов шифрования заменой, их применением в современных системах защиты информации, а также с возможностью реализации таких методов с использованием программных инструментов.
2. **Задачи работы:**
   - Описать принципы работы методов шифрования заменой.
   - Проанализировать основные преимущества и недостатки таких методов.
   - Ознакомить студентов с наиболее распространенными алгоритмами шифрования заменой, такими как ROT13, Caesar, Шифр Плейфера и другими.
   - Предложить простое практическое задание на реализацию одного из алгоритмов шифрования заменой, например, ROT13 или Caesar.
   - Проанализировать уровень защищенности данных при использовании методов шифрования заменой.

Студент должен:
Иметь практический опыт:

- установке, настройке, испытаниях и конфигурировании программных и программно-аппаратных в том числе криптографических средств защиты информации в оборудовании ИТКС;

Уметь:

- выявлять и оценивать угрозы безопасности информации в ИТКС;
- настраивать и применять средства защиты информации в операционных системах, в том числе средства антивирусной защиты;
- проводить установку и настройку программных и программно-аппаратных, в том числе криптографических средств защиты информации;

Знать:

- возможные угрозы безопасности информации в ИТКС;
- способы защиты информации от несанкционированного доступа (далее – НСД) и специальных воздействий на неё;
- типовые программные и программно-аппаратные средства защиты информации в информационно-телекоммуникационных системах и сетях;

ПК:

- ПК 2.1. Производить установку, настройку, испытания и конфигурирование программных и программно-аппаратных, в том числе криптографических средств защиты информации от несанкционированного доступа и специальных воздействий в оборудование информационно – телекоммуникационных систем и сетей..
- ПК 2.2. Поддерживать бесперебойную работу программных и программно-аппаратных, в том числе криптографических средств защиты информации в информационно – телекоммуникационных системах и сетях.

3. **Подготовка к работе**
   Познакомьтесь с материалами теоретической части работы, изложенных в приложении 1
   Подготовить бланк отчета

4. **Задание и порядок выполнения работы**
   Реализовать алгоритм шифрования Caesar.
   Описание задания:
   1. Создать программу на любом языке программирования, которая будет принимать на вход строку и число - сдвиг для алгоритма шифрования Caesar.

2. Программа должна возвращать зашифрованную строку с помощью алгоритма шифрования Caesar с указанным сдвигом.
3. Зашифрованную строку нужно вывести на экран.

5. Содержание отчета

1. название и цель работы;
2. перечень осваиваемых компетенций;
3. задание;
4. исходные данные по заданию/варианту;
5. ход выполнения работ;
6. выводы по работе;
7. ответы на контрольные вопросы.

Приложение 1

Краткие сведения из теории

Методы шифрования заменой основаны на замене символов открытого текста на другие символы в соответствии с заранее определенной таблицей замены. В основе методов лежит представление символов текста в виде чисел или битов, что позволяет выполнять операции с ними, такие как сдвиги, побитовые операции и др.

Наиболее распространенные методы шифрования заменой - это шифры подстановки, которые заменяют символы открытого текста на символы шифрованного текста в соответствии с определенным правилом. Примерами таких шифров являются ROT13, Caesar и Шифр Плейфера.

Приложение 2

Самостоятельная работа к практическому занятию

Самостоятельная работа по теме занятия включает в себя:

- изучение теоретического материала лекционных занятий, учебной литературы, Интернет-ресурсов, раздела «Краткие сведения из теории» настоящего описания ПЗ;
- выполнение практических заданий.

Практическая работа 4
ПРИМЕНЕНИЕ МЕТОДОВ ШИФРОВАНИЯ МНОГОАЛФАВИТНОЙ ЗАМЕНЫ

1. **Цель работы**: ознакомить студентов с методами шифрования многозначной замены и их применением в криптографии

2. **Задачи работы:**
   - Понять принципы многозначной замены в криптографии.
   - Изучить алгоритмы шифрования многозначной замены.
   - Освоить практические навыки использования методов шифрования многозначной замены.
   - Провести анализ преимуществ и недостатков методов шифрования многозначной замены.

Студент должен:
Иметь практический опыт:
- установке, настройке, испытаниях и конфигурировании программных и программно-аппаратных в том числе криптографических средств защиты информации в оборудовании ИТКС;
- поддержании бесперебойной работы программных и программно-аппаратных в том числе криптографических средств защиты информации в ИТКС;

Уметь:
- выявлять и оценивать угрозы безопасности информации в ИТКС;
- настраивать и применять средства защиты информации в операционных системах, в том числе средства антивирусной защиты;
- проводить установку и настройку программных и программно-аппаратных, в том числе криптографических средств защиты информации;

Знать:
- возможные угрозы безопасности информации в ИТКС;
- способы защиты информации от несанкционированного доступа (далее – НСД) и специальных воздействий на неё;
- типовые программные и программно-аппаратные средства защиты информации в информационно-телекоммуникационных системах и сетях;

ПК:
- ПК 2.1. Производить установку, настройку, испытания и конфигурирование программных и программно-аппаратных, в том числе криптографических средств защиты информации от несанкционированного доступа и специальных воздействий в оборудование информационно – телекоммуникационных систем и сетей..

3. **Подготовка к работе**
   Познакомьтесь с материалами теоретической части работы, изложенных в приложении 1
   Подготовить бланк отчета

4. **Задание и порядок выполнения работы**
   Задание состоит из создания программы, которая будет шифровать и дешифровать текст методом многозначной замены. В программе должны быть реализованы алгоритмы шифрования и дешифрования, а также возможность ввода и вывода текста.

5. **Содержание отчета**
   1. название и цель работы;
   2. перечень осваиваемых компетенций;
   3. задание;

4. исходные данные по заданию/варианту;
5. ход выполнения работ;
6. выводы по работе;
7. ответы на контрольные вопросы.

Приложение 1

Краткие сведения из теории

Метод многозначной замены - это метод шифрования, при котором каждый символ открытого текста заменяется на определенный символ или символьную последовательность из заранее определенного набора символов. Каждая буква или группа букв заменяется на другую букву или группу букв, соответственно, при дешифровке происходит обратная замена.

Одним из примеров метода многозначной замены является шифр Цезаря, при котором каждая буква алфавита сдвигается на определенное число позиций. Например, при сдвиге на 3 позиции буква A заменяется на D, B на E и т.д.

Другим примером метода многозначной замены является шифр Виженера, который использует ключевое слово для генерации последовательности символов, которые затем используются для замены букв открытого текста. Основным преимуществом этого метода является то, что он значительно сложнее для взлома, чем шифр Цезаря.

Приложение 2

Самостоятельная работа к практическому занятию

Самостоятельная работа по теме занятия включает в себя:

- изучение теоретического материала лекционных занятий, учебной литературы, Интернет-ресурсов, раздела «Краткие сведения из теории» настоящего описания ПЗ;
- выполнение практических заданий.

Практическая работа 5
КРИПТОАНАЛИЗ МЕТОДОВ ПЕРЕСТАНОВКИ

1. Цель работы: ознакомление с основами криптоанализа методов перестановки.

2. Задачи работы:

- Описать принцип работы метода перестановки.
- Объяснить, как осуществляется криптоанализ метода перестановки.
- Продемонстрировать практические навыки криптоанализа метода перестановки.

Студент должен:

Иметь практический опыт:

- защите информации от НСД и специальных воздействий в ИТКС с использованием программных и программно-аппаратных в том числе криптографических средств защиты в соответствии с предъявляемыми требованиями.

Уметь:

- проводить конфигурирование программных и программно-аппаратных, в том числе криптографических средств защиты информации;
- проводить контроль показателей и процесса функционирования программных и программно-аппаратных, в том числе криптографических средств защиты информации;
- проводить техническое обслуживание и ремонт программных и программно-аппаратных, в том числе криптографических средств защиты информации.

Знать:

- криптографические средства защиты информации конфиденциального характера, которые применяются в информационно-телекоммуникационных системах и сетях;
- порядок тестирования функций программных и программно-аппаратных, в том числе криптографических средств защиты информации;

ПК:

- ПК 2.1. Производить установку, настройку, испытания и конфигурирование программных и программно-аппаратных, в том числе криптографических средств защиты информации от несанкционированного доступа и специальных воздействий в оборудование информационно – телекоммуникационных систем и сетей..

3. Подготовка к работе

Познакомьтесь с материалами теоретической части работы, изложенных в приложении 1

Подготовить бланк отчета

4. Задание и порядок работы

1. Зашифруйте произвольный текст методом перестановки.
2. Попробуйте разгадать зашифрованный текст без знания ключа.
3. Предложите свой метод криптоанализа, который может помочь в расшифровке текста.

5. Содержание отчета

1. название и цель работы;
2. перечень осваиваемых компетенций;
3. задание;
4. исходные данные по заданию/варианту;
5. ход выполнения работ;
6. выводы по работе;

Приложение 1

Краткие сведения из теории

Метод перестановки - это метод шифрования, при котором порядок символов в открытом тексте меняется с помощью заранее заданного ключа. В качестве ключа может использоваться, например, перестановка букв в алфавите или порядок следования слов в предложении.

Криптоанализ метода перестановки осуществляется путем анализа статистики распределения символов в зашифрованном тексте. Например, если в языке текста некоторые символы встречаются чаще, чем другие, то можно предположить, что зашифрованные символы с наибольшей частотой встречаются вместо наиболее частых символов языка. Этот подход основан на частотном анализе и может быть использован для криптоанализа различных методов шифрования, в том числе и методов перестановки.

Приложение 2

Самостоятельная работа к практическому занятию

Самостоятельная работа по теме занятия включает в себя:

- изучение теоретического материала лекционных занятий, учебной литературы, Интернет-ресурсов, раздела «Краткие сведения из теории» настоящего описания ПЗ;
- выполнение практических заданий.

Практическая работа 6
КРИПТОАНАЛИЗ МЕТОДОВ ЗАМЕНЫ

1. **Цель работы**: ознакомиться с основными методами криптоанализа методов замены.
2. **Задачи работы:**
   - Изучить принципы работы методов замены.
   - Ознакомиться с основными методами криптоанализа методов замены.
   - Применить методы криптоанализа для расшифровки зашифрованного текста.

Студент должен:
Иметь практический опыт:

- защите информации от НСД и специальных воздействий в ИТКС с использованием программных и программно-аппаратных в том числе криптографических средств защиты в соответствии с предъявляемыми требованиями.

Уметь:

- проводить контроль показателей и процесса функционирования программных и программно-аппаратных, в том числе криптографических средств защиты информации;

Знать:

- криптографические средства защиты информации конфиденциального характера, которые применяются в информационно-телекоммуникационных системах и сетях;
- порядок тестирования функций программных и программно-аппаратных, в том числе криптографических средств защиты информации;
- порядок и правила ведения эксплуатационной документации на программные и программно-аппаратные, в том числе криптографических средств защиты информации.

ПК:

- ПК 2.1. Производить установку, настройку, испытания и конфигурирование программных и программно-аппаратных, в том числе криптографических средств защиты информации от несанкционированного доступа и специальных воздействий в оборудование информационно – телекоммуникационных систем и сетей..
- ПК 2.2. Поддерживать бесперебойную работу программных и программно-аппаратных, в том числе криптографических средств защиты информации в информационно – телекоммуникационных системах и сетях.

3. **Подготовка к работе**
   Познакомьтесь с материалами теоретической части работы, изложенных в приложении 1
   Подготовить бланк отчета

4. **Задание и порядок выполнения работы**
   - Зашифруйте произвольный текст методом замены, используя, например, шифр Цезаря или шифр Виженера.
   - Попробуйте расшифровать зашифрованный текст без знания ключа с помощью методов криптоанализа, например, методом частотного анализа или методом индекса совпадений.

5. **Содержание отчета**
   1. название и цель работы;
   2. перечень осваиваемых компетенций;
   3. задание;
   4. исходные данные по заданию/варианту;
   5. ход выполнения работ;
   6. выводы по работе;

Приложение 1

Краткие сведения из теории

Методы замены используются для шифрования сообщений путем замены символов в сообщении на другие символы или группы символов. Шифр Цезаря и шифр Виженера - это два примера методов замены. Криптоанализ методов замены - это процесс расшифровки зашифрованного сообщения, используя различные методы, такие как метод частотного анализа, метод индекса совпадений и др.

Приложение 2

Самостоятельная работа к практическому занятию

Самостоятельная работа по теме занятия включает в себя:

- изучение теоретического материала лекционных занятий, учебной литературы, Интернет-ресурсов, раздела «Краткие сведения из теории» настоящего описания ПЗ;
- выполнение практических заданий.

Практическая работа 7
КОМПЬЮТЕРНОЕ ШИФРОВАНИЕ

1. **Цель работы**: ознакомление студентов с основными принципами компьютерного шифрования и методами защиты информации..

2. **Задачи работы:**
   - Изучить основные понятия и принципы компьютерного шифрования.
   - Рассмотреть основные методы шифрования информации и их применение.
   - Освоить навыки использования программных средств для шифрования данных.
   - Понять принцип работы криптографических протоколов и алгоритмов.

Студент должен:
Иметь практический опыт:
- защите информации от НСД и специальных воздействий в ИТКС с использованием программных и программно-аппаратных в том числе криптографических средств защиты в соответствии с предъявляемыми требованиями.

Уметь:
- проводить конфигурирование программных и программно-аппаратных, в том числе криптографических средств защиты информации;
- проводить техническое обслуживание и ремонт программных и программно-аппаратных, в том числе криптографических средств защиты информации.

Знать:
- порядок тестирования функций программных и программно-аппаратных, в том числе криптографических средств защиты информации;
- организацию и содержание технического обслуживания и ремонта программно-аппаратных, в том числе криптографических средств защиты информации;
- порядок и правила ведения эксплуатационной документации на программные и программно-аппаратные, в том числе криптографических средств защиты информации.

ПК:
- ПК 2.2. Поддерживать бесперебойную работу программных и программно-аппаратных, в том числе криптографических средств защиты информации в информационно – телекоммуникационных системах и сетях.
- ПК 2.3. Осуществлять защиту информации от несанкционированных действий и специальных воздействий в информационно – телекоммуникационных системах и сетях с использованием программных и программно-аппаратных, в том числе криптографических средств в соответствии с предъявленными требованиями.

3. **Подготовка к работе**
   Познакомьтесь с материалами теоретической части работы, изложенных в приложении 1
   Подготовить бланк отчета

4. **Задание и порядок выполнения работы**
   Написать программу шифрования текстовой информации с использованием метода простой замены. Программа должна принимать на вход текстовый файл, а на выходе выдавать зашифрованный файл. При реализации программы студенты могут использовать язык программирования, который им более знаком.

5. **Содержание отчета**
   1. название и цель работы;
   2. перечень осваиваемых компетенций;
   3. задание;

4. исходные данные по заданию/варианту;
5. ход выполнения работ;
6. выводы по работе;

Приложение 1

Краткие сведения из теории

Компьютерное шифрование - это процесс преобразования информации в нечитаемый вид для защиты ее от несанкционированного доступа. Шифрование является одним из основных инструментов защиты информации в компьютерных системах.

Основные методы шифрования:

1. Методы перестановки - изменение порядка символов в тексте без изменения самих символов. Пример - метод колонок.
2. Методы замены - замена символов в тексте на другие символы. Пример - метод Цезаря.
3. Методы многократной замены - последовательное применение нескольких методов замены. Пример - шифр Виженера.
4. Симметричные криптосистемы - использование общего секретного ключа для шифрования и расшифрования информации.
5. Асимметричные криптосистемы - использование открытого и закрытого ключа для шифрования и расшифрования информации.

Криптографические алгоритмы шифрования защищают информацию путем обеспечения конфиденциальности, целостности и аутентификации. Криптографические протоколы обеспечивают безопасную передачу информации между двумя или более узлами в сети.

Приложение 2

Самостоятельная работа к практическому занятию

Самостоятельная работа по теме занятия включает в себя:

- изучение теоретического материала лекционных занятий, учебной литературы, Интернет-ресурсов, раздела «Краткие сведения из теории» настоящего описания ПЗ;
- выполнение практических заданий.

Практическая работа 8
АЛГОРИТМ ДИФФИ-ХЕЛМАНА

1. **Цель работы**: ознакомиться с принципами работы алгоритма Диффи-Хелмана, используемого для обмена ключами.
2. **Задачи работы:**
   - Понимание принципов работы алгоритма Диффи-Хелмана.
   - Овладение навыками применения алгоритма в практике.
   - Понимание роли обмена ключами при обеспечении безопасности информации.

Студент должен:

Иметь практический опыт:

- защите информации от НСД и специальных воздействий в ИТКС с использованием программных и программно-аппаратных в том числе криптографических средств защиты в соответствии с предъявляемыми требованиями.

Уметь:

- проводить конфигурирование программных и программно-аппаратных, в том числе криптографических средств защиты информации;
- проводить восстановление процесса и параметров функционирования программных и программно-аппаратных, в том числе криптографических средств защиты информации;
- проводить техническое обслуживание и ремонт программных и программно-аппаратных, в том числе криптографических средств защиты информации.

Знать:

- криптографические средства защиты информации конфиденциального характера, которые применяются в информационно-телекоммуникационных системах и сетях;
- порядок тестирования функций программных и программно-аппаратных, в том числе криптографических средств защиты информации;
- порядок и правила ведения эксплуатационной документации на программные и программно-аппаратные, в том числе криптографических средств защиты информации.

ПК:

- ПК 2.2. Поддерживать бесперебойную работу программных и программно-аппаратных, в том числе криптографических средств защиты информации в информационно – телекоммуникационных системах и сетях.
- ПК 2.3. Осуществлять защиту информации от несанкционированных действий и специальных воздействий в информационно – телекоммуникационных системах и сетях с использованием программных и программно-аппаратных, в том числе криптографических средств в соответствии с предъявленными требованиями.

3. **Подготовка к работе**

   Познакомьтесь с материалами теоретической части работы, изложенных в приложении 1

   Подготовить бланк отчета

4. **Задание и порядок выполнения работы**

Написать программу на любом языке программирования, которая реализует алгоритм Диффи-Хеллмана для двух пользователей. Программа должна:

- Сгенерировать общие параметры (большое простое число и первообразный корень по модулю этого числа).
- Пользователь А выбирает свой секретный ключ и вычисляет открытый ключ.
- Пользователь В выбирает свой секретный ключ и вычисляет открытый ключ.
- Пользователь А вычисляет общий секретный ключ.

- Пользователь B вычисляет общий секретный ключ.
- Пользователь A и пользователь B выводят общий секретный ключ на экран.

5. Содержание отчета

1. название и цель работы;
2. перечень осваиваемых компетенций;
3. задание;
4. исходные данные по заданию/варианту;
5. ход выполнения работ;
6. выводы по работе;

Приложение 1

Краткие сведения из теории

Алгоритм Диффи-Хеллмана — это криптографический алгоритм, который позволяет двум пользователям безопасно обмениваться секретными ключами через открытый канал связи. Алгоритм был разработан Уитфилдом Диффи и Мартином Хеллманом в 1976 году.

Алгоритм Диффи-Хеллмана основан на математической задаче дискретного логарифма. Для выполнения алгоритма необходимо сгенерировать большое простое число p и первообразный корень по модулю p. Затем каждый пользователь выбирает свой секретный ключ и вычисляет открытый ключ. Обмен открытыми ключами позволяет каждому пользователю вычислить общий секретный ключ, который можно использовать для шифрования и расшифрования сообщений.

Приложение 2

Самостоятельная работа к практическому занятию

Самостоятельная работа по теме занятия включает в себя:

- изучение теоретического материала лекционных занятий, учебной литературы, Интернет-ресурсов, раздела «Краткие сведения из теории» настоящего описания ПЗ;
- выполнение практических заданий.

Практическая работа 9
СТАНДАРТ СИММЕТРИЧНОГО ШИФРОВАНИЯ AES RIJNDAEL

1. **Цель работы**: Ознакомление с принципами работы стандарта симметричного шифрования AES Rijndael.
2. **Задачи работы:**
   - Научиться использовать AES Rijndael для шифрования и расшифровки данных.
   - Понять преимущества и недостатки стандарта AES Rijndael в сравнении с другими симметричными шифрами.

Студент должен:

Иметь практический опыт:

- поддержании бесперебойной работы программных и программно-аппаратных в том числе криптографических средств защиты информации в ИТКС;
- защите информации от НСД и специальных воздействий в ИТКС с использованием программных и программно-аппаратных в том числе криптографических средств защиты в соответствии с предъявляемыми требованиями.

Уметь:

- проводить контроль показателей и процесса функционирования программных и программно-аппаратных, в том числе криптографических средств защиты информации;
- проводить восстановление процесса и параметров функционирования программных и программно-аппаратных, в том числе криптографических средств защиты информации;
- проводить техническое обслуживание и ремонт программных и программно-аппаратных, в том числе криптографических средств защиты информации.

Знать:

- организацию и содержание технического обслуживания и ремонта программно-аппаратных, в том числе криптографических средств защиты информации;
- порядок и правила ведения эксплуатационной документации на программные и программно-аппаратные, в том числе криптографических средств защиты информации.

ПК:

- ПК 2.2. Поддерживать бесперебойную работу программных и программно-аппаратных, в том числе криптографических средств защиты информации в информационно – телекоммуникационных системах и сетях.
- ПК 2.3. Осуществлять защиту информации от несанкционированных действий и специальных воздействий в информационно – телекоммуникационных системах и сетях с использованием программных и программно-аппаратных, в том числе криптографических средств в соответствии с предъявленными требованиями.

3. **Подготовка к работе**

   Познакомьтесь с материалами теоретической части работы, изложенных в приложении 1

   Подготовить бланк отчета

4. **Задание и порядок выполнения работы**

1. Написать программу на любом языке программирования, которая принимает на вход строку текста и ключ, а затем шифрует её с помощью AES Rijndael.
2. Добавить возможность расшифровки зашифрованной строки с помощью того же ключа.
3. Протестировать программу на нескольких примерах.

5. Содержание отчета

1. название и цель работы;
2. перечень осваиваемых компетенций;
3. задание;
4. исходные данные по заданию/варианту;
5. ход выполнения работ;
6. выводы по работе;

Приложение 1

Краткие сведения из теории

AES Rijndael - это симметричный блочный шифр, который используется для шифрования и расшифровки данных. Он был утвержден как стандарт в 2001 году и используется повсеместно. AES Rijndael может использовать блоки данных размером от 128 до 256 бит и ключи длиной 128, 192 или 256 бит. Он основан на замене байтов и перестановке байтов в блоке данных с помощью различных подстановок и циклических сдвигов. AES Rijndael также использует матричные операции и алгоритмы для генерации ключей. Он считается одним из самых надежных симметричных шифров.

Приложение 2

Самостоятельная работа к практическому занятию

Самостоятельная работа по теме занятия включает в себя:

- изучение теоретического материала лекционных занятий, учебной литературы, Интернет-ресурсов, раздела «Краткие сведения из теории» настоящего описания ПЗ;
- выполнение практических заданий.

Практическая работа 10
ГЕНЕРАЦИЯ ПРОСТЫХ ЧИСЕЛ, ИСПОЛЬЗУЕМЫХ В АСИММЕТРИЧНЫХ СИСТЕМАХ ШИФРОВАНИЯ

1. **Цель работы**: изучить методы генерации простых чисел , используемых в асимметричных системах шифрования.
2. **Задачи работы:**
   - Изучить принципы работы асимметричных систем шифрования.
   - Изучить методы генерации простых чисел, используемых в асимметричных системах шифрования.
   - Реализовать алгоритм генерации простых чисел на языке программирования.
   - Продемонстрировать работу алгоритма на примере генерации нескольких простых чисел.

Студент должен:
Иметь практический опыт:
- защите информации от НСД и специальных воздействий в ИТКС с использованием программных и программно-аппаратных в том числе криптографических средств защиты в соответствии с предъявляемыми требованиями.

Уметь:
- проводить конфигурирование программных и программно-аппаратных, в том числе криптографических средств защиты информации;
- проводить контроль показателей и процесса функционирования программных и программно-аппаратных, в том числе криптографических средств защиты информации;
- проводить техническое обслуживание и ремонт программных и программно-аппаратных, в том числе криптографических средств защиты информации.

Знать:
- типовые программные и программно-аппаратные средства защиты информации в информационно-телекоммуникационных системах и сетях;
- криптографические средства защиты информации конфиденциального характера, которые применяются в информационно-телекоммуникационных системах и сетях;
- порядок и правила ведения эксплуатационной документации на программные и программно-аппаратные, в том числе криптографических средств защиты информации.

ПК:
- ПК 2.3. Осуществлять защиту информации от несанкционированных действий и специальных воздействий в информационно – телекоммуникационных системах и сетях с использованием программных и программно-аппаратных, в том числе криптографических средств в соответствии с предъявленными требованиями.

3. **Подготовка к работе**
   Познакомьтесь с материалами теоретической части работы, изложенных в приложении 1
   Подготовить бланк отчета

4. **Задание и порядок выполнения работы**
   Написать программу на языке программирования, которая будет генерировать случайное простое число. Программа должна принимать на вход длину числа в битах, которую задает пользователь, и выводить на экран сгенерированное простое число.
5. **Содержание отчета**
   1. название и цель работы;

2. перечень осваиваемых компетенций;
3. задание;
4. исходные данные по заданию/варианту;
5. ход выполнения работ;
6. выводы по работе;

Приложение 1

Краткие сведения из теории

Асимметричные криптосистемы (системы открытого шифрования, с открытым ключом - public key systems) – смысл данных криптосистем состоит в том, что для зашифрования и расшифрования используются разные преобразования. Одно из них – зашифрование – является абсолютно открытым для всех. Другое же – расшифрование – остается секретным за счет секретности ключа расшифрования. Таким образом, любой, кто хочет что-либо зашифровать, пользуется открытым преобразованием. Но расшифровать и прочитать это сможет лишь тот, кто владеет секретным ключом.

В настоящий момент во многих асимметричных криптосистемах вид преобразования определяется ключом. У пользователя есть два ключа – секретный и открытый. Открытый ключ публикуется в общедоступном месте, и каждый, кто захочет послать сообщение этому пользователю – зашифровывает текст открытым ключом. Расшифровать сможет только упомянутый пользователь с секретным ключом. Таким образом, отпадает проблема передачи секретного ключа, как в симметричных системах.

Однако, несмотря на все свои преимущества, эти криптосистемы достаточно трудоемки и медлительны. Стойкость асимметричных криптосистем базируется, в основном, на алгоритмической трудности решить за приемлемое время какую-либо задачу. Если злоумышленнику удастся построить такой алгоритм, то дискредитирована будет вся система и все сообщения, зашифрованные с помощью этой системы. В этом состоит главная опасность асимметричных криптосистем в отличие от симметричных.

Алгоритм Диффи-Хеллмана

Алгоритм Диффи-Хеллмана (Diffie-Hellman) использует функцию дискретного возведения в степень. Сначала генерируются два больших простых числа n и q. Эти два числа не обязательно хранить в секрете. Далее один из партнеров P1 генерирует случайное число x и посылает другому участнику будущих обменов P2 значение

A = qx mod n

По получении A партнер P2 генерирует случайное число y и посылает участнику обмена P1 вычисленное значение

B = qy mod n

Партнер P1, получив B, вычисляет Kx = Bx mod n, а партнер P2

вычисляет Ky = Ay mod n. Алгоритм гарантирует, что числа Ky и Kx равны и могут быть использованы в качестве секретного ключа для шифрования.

Ведь даже перехватив числа A и B, трудно вычислить Kx или Ky.

Алгоритм RSA

Первое практическое воплощение принцип открытого шифрования получил в системе RSA, разработанной в 1977 году в Массачусетском Технологическом Институте (США) и получившей свое название от первых букв фамилий авторов: Рональд Ривест (R.Rivest), Эди Шамир (A.Shamir),

Леонард Адлеман (L.Adleman).

Идея авторов состояла в том, что взяв целое число N в виде произведения двух больших простых чисел N=P*Q, легко подобрать пару чисел Y и X, таких, чтобы для любого целого числа M, меньшего N, справедливо соотношение:

(MX)Y =M mod N

В качестве открытого ключа шифрования в системе RSA выступают ключ Y и модуль N, а секретным ключом для расшифрования сообщений является число X.

Процедура шифрования сообщения M, рассматриваемого как целое число (такое допущение возможно вследствие того, что любой контент может быть представлен в числовой форме при обработке в средствах вычислительной техники), меньшее N (при необходимости длинное сообщение разбивается на отрезки, шифруемые независимо), состоит в вычислении значения:

C=MY mod N

Расшифрование осуществляется аналогично с использованием секретного ключа X:

M=CX mod N

Математически строго можно доказать, что определение по паре чисел

(N, Y) секретного ключа X, не проще разложения на простые множители числа N, то есть нахождения P и Q. Задача же разложения на множители целого числа изучается в математике с древнейших времен и известна как сложная вычислительная задача. На настоящий момент разложение числа из нескольких сотен десятичных знаков потребует от современных вычислительных машин сотен лет непрерывной работы.

Методы проверки чисел на простоту

Одна из главных проблем асимметричного шифрования – генерация больших простых чисел. Простейшим методом проверки простоты натурального числа N является метод пробных делений: для d=2, 3, 4 … мы проверяем выполнение условия (d, N)>1 (здесь (d, N) – наибольший общий делитель чисел d и N). Число операций, требуемых для этого метода, имеет порядок корня из N.

Поэтому уже для чисел порядка 1030–1040 он не применим.

В отличие от таких “детерминированных“ тестов существуют еще “вероятностные“ тесты проверки простоты. Для исследуемого числа проверяется выполнение некоторых, связанных со случайными числами, условий. Если какое-либо из этих условий не выполнено, то N – составное число. Если же все условия выполнены, то с некоторой вероятностью можно утверждать, что N – простое число. Эта вероятность тем ближе к 1, чем большее количество случайных чисел мы проверим.

Обычно эти условия основаны на малой теореме Ферма, утверждающей, что для любого положительного числа b, не превосходящего некоторого простого числа p :

$b(p–1) = 1(\mathrm{mod}\ p)$.

Например, $26 = 64 = 63+1 = 1(\mathrm{mod}\ 7)$. Если требуется определить, является ли целое число r простым, то можно выбрать любое положительное целое число b, меньшее r, и проверить, выполнено ли равенство

$b(r–1) = 1(\mathrm{mod}\ r)$.

Если равенство не выполнено, то на основании теоремы Ферма можно быть совершенно уверенным, что r – не простое число. Если же равенство выполнено, то можно лишь предполагать, что r – простое число и поэтому назвать его “псевдопростым по основанию b“. Вероятность P (x) того, что составное число x окажется псевдопростым по случайному основанию, убывает с ростом x.

К сожалению, существуют так называемые числа Кармайкла – такие составные числа, которые обладают свойством:

$b(r–1) = 1(\mathrm{mod}\ r)$ для всех b из интервала [1, r], которые взаимно просты с r.

Примером числа Кармайкла является число 561 = 3*11*17.

Классический результат теории чисел – теорема Чебышева – показывает, что доля положительных целых чисел, меньших некоторого целого m и являющихся простыми, близка к 1/(ln m). Например, доля целых чисел, меньших 10100 и являющихся простыми, близка к 1/(ln10100) = 1/230.

Таким образом, если мы выберем случайно большое целое положительное нечетное число x и будем последовательно проверять на простоту числа x, x+1, x+2, … , то, в среднем, мы впервые встретим простое число на шаге с номером ln x.

Приложение 2

Самостоятельная работа к практическому занятию

Самостоятельная работа по теме занятия включает в себя:

- изучение теоретического материала лекционных занятий, учебной литературы, Интернет-ресурсов, раздела «Краткие сведения из теории» настоящего описания ПЗ;
- выполнение практических заданий.

Практическая работа 11
КРИПТОГРАФИЧЕСКИЕ ХЭШ-ФУНКЦИИ. АУТЕНТИФИКАЦИЯ

1. **Цель работы**: изучение средств аутентификации в информационных системах, их принципов работы и основных типов.

2. **Задачи работы:**
   - Рассмотреть понятие аутентификации и ее роль в обеспечении безопасности информационных систем.
   - Изучить основные методы аутентификации, такие как парольная аутентификация, аутентификация по токенам, биометрическая аутентификация и др.
   - Разобраться в принципах работы аутентификационных систем и их преимуществах и недостатках.
   - Изучить понятие авторизации и ее роль в обеспечении безопасности информационных систем.
   - Рассмотреть методы авторизации, такие как списки контроля доступа (ACL), ролевая авторизация и др.
   - Изучить принципы работы авторизационных систем и их преимущества и недостатки.
   - Рассмотреть вопросы интеграции аутентификации и авторизации в информационных системах и возможные проблемы при этом.

Студент должен:
Иметь практический опыт:
- установке, настройке, испытаниях и конфигурировании программных и программно-аппаратных в том числе криптографических средств защиты информации в оборудовании ИТКС;

Уметь:
- проводить конфигурирование программных и программно-аппаратных, в том числе криптографических средств защиты информации;
- проводить восстановление процесса и параметров функционирования программных и программно-аппаратных, в том числе криптографических средств защиты информации;
- проводить техническое обслуживание и ремонт программных и программно-аппаратных, в том числе криптографических средств защиты информации.

Знать:
- криптографические средства защиты информации конфиденциального характера, которые применяются в информационно-телекоммуникационных системах и сетях;
- порядок тестирования функций программных и программно-аппаратных, в том числе криптографических средств защиты информации;
- порядок и правила ведения эксплуатационной документации на программные и программно-аппаратные, в том числе криптографических средств защиты информации.

ПК:
- ПК 2.3. Осуществлять защиту информации от несанкционированных действий и специальных воздействий в информационно – телекоммуникационных системах и сетях с использованием программных и программно-аппаратных, в том числе криптографических средств в соответствии с предъявленными требованиями.

3. **Подготовка к работе**
   Познакомьтесь с материалами теоретической части работы, изложенных в приложении 1
   Подготовить бланк отчета

4. Задание и порядок выполнения работы

Написать отчет о сравнении методов аутентификации

5. Содержание отчета

1. название и цель работы;
2. перечень осваиваемых компетенций;
3. задание;
4. исходные данные по заданию/варианту;
5. ход выполнения работ;
6. выводы по работе;

Приложение 1

Краткие сведения из теории

Криптографическая хеш-функция является одной из группы хэш-функций, которые подходят для криптографических приложений, таких как SSL /TLS, Как и другие хеш-функции, криптографические хеш-функции - это односторонние математические алгоритмы, используемые для отображения данных любого размера в битовую строку фиксированного размера. Криптографические хеш-функции широко используются в практике защиты информации, такой как цифровые подписи, коды аутентификации сообщений и другие формы аутентификации.

Криптографические хеш-функции должны иметь следующие свойства (источник: википедия):

1. Одно и то же сообщение всегда приводит к одному и тому же хеш-значению (т.е. детерминистический).

2. Хеш-значение вычисляется быстро.

3. Невозможно иметь два сообщения с одинаковым значением хеш-функции (так называемое «столкновение»).

4. Невозможно намеренно создать сообщение, которое дает заданное значение хеш-функции.

5. Небольшие изменения в сообщении должны значительно изменить результирующее значение хеш-функции, чтобы оно казалось не связанным с исходным хеш-значением.

Наиболее часто используемые криптографические хеш-функции включают MD5, SHA-1 и SHA-2.

Уникальность каждого хеша жизненно важна для целостности криптографической хеш-функции. Это то, что действительно отличает криптографические хеш-функции от других хеш-функций - уверенность в том, что конкретное сообщение идентифицируется уникальным и недопустимо дублируемым способом.

Схемы цифровой подписи (например, для подписание документа, подпись кода или S/MIME e-mail) обычно требуют, чтобы криптографический хеш вычислялся для сообщения и включался в подпись. Программное обеспечение получателя затем независимо вычисляет хеш для проверки целостности сообщения.

Веб-сайты также часто публикуют хэш-значение для загружаемых файлов. Когда пользователь загружает файл, он может использовать свое собственное программное обеспечение для независимого вычисления хеша, проверяя целостность файла.

Безопасность пароля также зависит от криптографических хэшей. Пароли, представленные пользователями, хэшируются, а затем сравниваются с сохраненным хэшем.

Криптографические хеш-функции широко используются в таких протоколах безопасности, как SSL /TLS и SSH, и в других приложениях, которые полагаются на целостность данных. Криптовалюты используют алгоритмы хеширования для обновления блокчейна новыми блоками защищенных и проверяемых данных транзакций. (Например, BitCoin использует SHA-2 для подтверждения транзакции.)

Что такое SHA-1?

SHA-1 (безопасный алгоритм хеширования 1) - это криптографическая хеш-функция, которая может преобразовывать произвольно длинную строку данных в дайджест с фиксированным размером 160 бит. Этот дайджест обычно отображается в виде шестнадцатеричного числа из 40 символов.

Алгоритм SHA-1 теперь считается небезопасным, Сертификаты SHA-1 больше не соответствуют базовым требованиям форума CA / B или поддерживаются текущими версиями основных веб-браузеров.

Серия хэш-функций алгоритма безопасного хеширования (SHA) состоит из различных наборов (SHA-0, SHA-1, SHA-2, SHA-3).

Что такое SHA-2?

SHA-2 (безопасный алгоритм хеширования 2) относится к семейству криптографических хеш-функций, которые могут преобразовывать произвольно длинные строки данных в дайджесты фиксированного размера (224, 256, 384 или 512 бит). 256-битный SHA-2, также известный как SHA-256, является наиболее часто используемой версией. Дайджест обычно отображается как шестнадцатеричное число с фиксированным значением. (Например, SHA-256 возвращает код из 64 символов.)

SHA-2 вытеснил SHA-1 в протоколах безопасности, таких как SSL /TLS.

Приложение 2

Самостоятельная работа к практическому занятию

Самостоятельная работа по теме занятия включает в себя:

- изучение теоретического материала лекционных занятий, учебной литературы, Интернет-ресурсов, раздела «Краткие сведения из теории» настоящего описания ПЗ;
- выполнение практических заданий.

Практическая работа 12
ШИФРОВАНИЕ МЕТОДОМ СКОЛЬЗЯЩЕЙ ПЕРЕСТАНОВКИ

1. **Цель работы**: ознакомление студентов с применением методов шифрования скользящей перестановкой.
2. **Задачи работы:**
   - Изучить теоретические основы шифрования перестановкой.
   - Ознакомиться с примерами шифров, основанных на перестановке символов.
   - Практически реализовать алгоритм шифрования перестановкой на языке программирования.
   - Протестировать работу алгоритма на различных входных данных.

Студент должен:

Иметь практический опыт:

- защите информации от НСД и специальных воздействий в ИТКС с использованием программных и программно-аппаратных в том числе криптографических средств защиты в соответствии с предъявляемыми требованиями.

Уметь:

- проводить восстановление процесса и параметров функционирования программных и программно-аппаратных, в том числе криптографических средств защиты информации;
- проводить техническое обслуживание и ремонт программных и программно-аппаратных, в том числе криптографических средств защиты информации.

Знать:

- организацию и содержание технического обслуживания и ремонта программно-аппаратных, в том числе криптографических средств защиты информации;
- порядок и правила ведения эксплуатационной документации на программные и программно-аппаратные, в том числе криптографических средств защиты информации.

ПК:

- ПК 2.3. Осуществлять защиту информации от несанкционированных действий и специальных воздействий в информационно – телекоммуникационных системах и сетях с использованием программных и программно-аппаратных, в том числе криптографических средств в соответствии с предъявленными требованиями.

3. **Подготовка к работе**

   Познакомьтесь с материалами теоретической части работы, изложенных в приложении 1

   Подготовить бланк отчета

4. **Задание и порядок выполнения работы**
   1. Написать программу на языке программирования, которая принимает на вход строку символов и ключ для шифрования скользящей перестановкой.
   2. Реализовать алгоритм шифрования скользящей перестановкой символов в строке с помощью заданного ключа.
   3. Вывести зашифрованную строку на экран
   4. Реализовать алгоритм дешифрования зашифрованной строки с помощью заданного ключа.
   5. Вывести дешифрованную строку на экран.

5. **Содержание отчета**
   1. название и цель работы;
   2. перечень осваиваемых компетенций;

3. задание;
4. исходные данные по заданию/варианту;
5. ход выполнения работ;
6. выводы по работе;

Приложение 1

Краткие сведения из теории

Шифр, преобразования из которого изменяют только порядок следования символов исходного текста, но не изменяют их самих, называется шифром перестановки

Рассмотрим преобразование из ШП, предназначенное для зашифрования сообщения длиной символов. Его можно представить с помощью таблицы

где номер места шифртекста, на которое попадает первая буква исходного сообщения при выбранном преобразовании, номер места для второй буквы и т. д. В верхней строке таблицы выписаны по порядку числа от 1 до а в нижней - те же числа, но в произвольном порядке. Такая таблица называется подстановкой степени

Зная подстановку, задающую преобразование, можно осуществить как зашифрование, так и расшифрование текста. Например, если для преобразования используется подстановка

и в соответствии с ней зашифровывается слово то получится Попробуйте расшифровать сообщение полученное в результате преобразования с помощью указанной выше подстановки.

В качестве упражнения читателю предлагается самостоятельно выписать подстановки, задающие преобразования в описанных ниже трех

примерах шифров перестановки. Ответы помещены в конце раздела.

Читатель, знакомый с методом математической индукции, может легко убедиться в том, что существует (обозначается читается факториал») вариантов заполнения нижней строки таблицы (6). Таким образом, число различных преобразований шифра перестановки, предназначенного для зашифрования сообщений длины меньше либо равно (заметим, что в это число входит и вариант преобразования, оставляющий все символы на своих местах!).

С увеличением числа значение растет очень быстро. Приведем таблицу значений для первых 10 натуральных чисел:

(см. скан)

При больших для приближенного вычисления можно пользоваться известной формулой Стирлинга

Примером ШП, предназначенного для зашифрования сообщений длины является шифр, в котором в качестве множества ключей взято множество всех подстановок степени а соответствующие им преобразования шифра задаются, как было описано выше. Число ключей такого шифра равно

Для использования на практике такой шифр не удобен, так как при больших значениях приходится работать с длинными таблицами.

Широкое распространение получили шифры перестановки, использующие некоторую геометрическую фигуру. Преобразования из этого шифра состоят в том, что в фигуру исходный текст вписывается по ходу одного «маршрута», а затем по ходу другого выписывается с нее. Такой шифр называют маршрутной перестановкой. Например, можно вписывать исходное сообщение в прямоугольную таблицу, выбрав такой маршрут: по горизонтали, начиная с левого верхнего угла поочередно слева направо и справа налево. Выписывать же сообщение будем по другому маршруту: по вертикали, начиная с верхнего правого угла и двигаясь поочередно сверху вниз и снизу вверх.

Зашифруем, например, указанным способом фразу:

используя прямоугольник размера

(см. скан)

Зашифрованная фраза выглядит так:

Теоретически маршруты могут быть значительно более изощренными, однако запутанность маршрутов усложняет использование таких шифров.

Ниже приводятся описания трех разновидностей шифров перестановки, встречавшихся в задачах олимпиад.

Шифр «Сцитала». Одним из самых первых шифровальных приспособлений был жезл («Сцитала»), применявшийся еще во времена войны Спарты против Афин в V веке до н. э. Это был цилиндр, на который виток к витку наматывалась узкая папирусная лента (без просветов и нахлестов), а затем на этой ленте вдоль его оси записывался необходимый для передачи текст. Лента сматывалась с цилиндра и отправлялась адресату, который, имея цилиндр точно такого же диаметра, наматывал ленту на него и прочитывал сообщение. Ясно, что такой способ шифрования осуществляет перестановку местами букв сообщения.

Шифр «Сцитала», как видно из решения задачи 2.1, реализует не более перестановок по прежнему, - длина сообщения). Действительно, этот шифр, как нетрудно видеть, эквивалентен следующему шифру маршрутной перестановки: в таблицу, состоящую из столбцов, построчно записывают сообщение, после чего выписывают буквы по столбцам. Число задействованных столбцов таблицы не может превосходить длины сообщения.

Имеются еще и чисто физические ограничения, накладываемые реализацией шифра «Сцитала». Естественно предположить, что диаметр жезла не должен превосходить 10 сантиметров. При высоте строки в 1 сантиметр на одном витке такого жезла уместится не более 32 букв Таким образом, число перестановок, реализуемых «Сцита-лой», вряд ли превосходит 32.

Шифр «Поворотная решетка». Для использования шифра, называемого поворотной решеткой, изготавливается трафарет из прямоугольного листа клетчатой бумаги размера клеток. В трафарете вырезано тк клеток так, что при наложении его на чистый лист бумаги того же размера четырьмя возможными способами его вырезы полностью покрывают всю площадь листа.

Буквы сообщения последовательно вписываются в вырезы трафарета (по строкам, в каждой строке слева направо) при каждом из четырех его возможных положений в заранее установленном порядке.

Поясним процесс шифрования на примере. Пусть в качестве ключа используется решетка приведенная на рис. 1.

Зашифруем с ее помощью текст

Наложив решетку на лист бумаги, вписываем первые 15 (по числу

вырезов) букв сообщения: Сняв решетку, мы увидим текст, представленный на рис. 2. Поворачиваем решетку на 180°. В окошечках появятся новые, еще не заполненные клетки. Вписываем в них следующие 15 букв. Получится запись, приведенная на рис. 3. Затем переворачиваем решетку на другую сторону и зашифровываем остаток текста аналогичным образом (рис. 4, 5).

Получатель сообщения, имеющий точно такую же решетку, без труда прочтет исходный текст, наложив решетку на шифртекст по порядку четырьмя способами.

Можно доказать, что число возможных трафаретов, то есть количество ключей шифра «решетка», составляет (см. задачу 1.1). Этот шифр предназначен для сообщений длины Число всех перестановок в тексте такой длины составит что во много раз

больше числа Однако, уже при размере трафарета число возможных решеток превосходит 4 миллиарда.

Широко распространена разновидность шифра маршрутной перестановки, называемая «шифром вертикальной перестановки» (ШВП). В нем снова используется

прямоугольник, в который сообщение вписывается обычным способом (по строкам слева направо). Выписываются буквы по вертикали, а столбцы при этом берутся в порядке, определяемом ключом. Пусть, например, этот ключ таков: (5,4,1,7,2,6,3), и с его помощью надо зашифровать сообщение:

Впишем сообщение в прямоугольник, столбцы которого пронумерованы в соответствии с ключом:

(см. скан)

Теперь, выбирая столбцы в порядке, заданном ключом, и выписывая последовательно буквы каждого из них сверху вниз, получаем такую криптограмму:

Число ключей ШВП не более где число столбцов таблицы. Как правило, гораздо меньше, чем длина текста (сообщение укладывается в несколько строк по букв), а, значит, и много меньше

Пользуясь приведенной выше формулой Стирлинга при больших попытайтесь оценить, во сколько раз число возможных перестановок столбцами меньше числа всех перестановок на тексте длины кратном

В случае, когда ключ ШВП не рекомендуется записывать, его можно извлекать из какого-то легко запоминающегося слова или предложения. Для этого существует много способов. Наиболее распространенный состоит в том, чтобы приписывать буквам числа в соответствии с обычным алфавитным порядком букв. Например, пусть ключевым словом будет Присутствующая в нем буква А получает номер 1. Если какая-то буква входит несколько раз, то ее появления нумеруются последовательно слева направо. Поэтому второе вхождение буквы А получает номер 2. Поскольку буквы в этом слове нет, то буква В получает номер 3 и так далее. Процесс продолжается до тех

пор, пока все буквы не получат номера. Таким образом, мы получаем следующий ключ:

Перейдем к вопросу о методах вскрытия шифров перестановки. Проблема, возникающая при восстановлении сообщения, зашифрованного ШП, состоит не только в том, что число возможных ключей велико даже при небольших длинах текста. Если и удастся перебрать все допустимые варианты перестановок, не всегда ясно, какой из этих вариантов истинный. Например, пусть требуется восстановить исходный текст по криптограмме и нам ничего не известно, кроме того, что применялся шифр перестановки. Какой вариант «осмысленного» исходного текста признать истинным: или А может быть Приведем пример еще более запутанной ситуации. Пусть требуется восстановить сообщение по криптограмме

полученной шифром перестановки. Возможны, как минимум, два варианта исходного сообщения:

Эти варианты имеют прямо противоположный смысл и в имеющихся условиях у нас нет возможности определить, какой из вариантов истинный.

Иногда, за счет особенностей реализации шифра, удается получить информацию об использованном преобразовании (перестановке). Рассмотрим шифр «Сцитала» из задачи 2.1. Выше уже рассматривался вопрос о количестве перестановок, реализуемых «Сциталой». Их оказалось не более 32. Это число невелико, поэтому можно осуществить перебор всех вариантов. При достаточной длине сообщения, мы, скорее всего, получим единственный читаемый вариант текста. Однако, используя информацию о расположении линий, оставленных шифровальщиком, удается определить диаметр стержня, а значит, и возникающую перестановку букв (см. задачу 2.1).

В рассмотренном примере шифровальщик по неосторожности оставил на папирусе следы, позволяющие нам легко прочитать сообщение. Возможны и другие ситуации, когда не очень «грамотное» использование шифра облегчает вскрытие переписки.

В задаче 5.2 содержится пример текста, зашифрованного ШВП. По условию пробелы между словами при записи текста в таблицу опускались. Поэтому заключаем, что все столбцы, содержащие пробел в последней строке, должны стоять в конце текста. Таким образом, возникает разбиение столбцов на две группы (содержащие 6 букв, и

Аналогичная ситуация возникает и при «неполном» использовании шифра «решетка» (см. задачу 4.1). Пусть имеется решетка размера и зашифрованное с ее помощью сообщение длины к, не содержащее пробелов. Незаполненные к мест в решетке при условии, что к соответствуют вырезам в четвертом положении решетки. На основе такой информации, происходит резкое уменьшение числа допустимых решеток (их будет Читателю предлагается самостоятельно подсчитать число допустимых решеток при

На примере решения задачи 5.2 продемонстрируем еще один подход к вскрытию шифров вертикальной перестановки - лингвистический. Он основан на том, что в естественных языках некоторые комбинации букв встречаются очень часто, другие - гораздо реже, а многие вообще не встречаются (например -

Будем подбирать порядок следования столбцов друг за другом так, чтобы во всех строках этих столбцов получались «читаемые» отрезки текста. В приведенном решении задачи восстановление текста начинается с подбора цепочки из трех столбцов первой группы, содержащей в последней строке сочетание так как естественно предположить, что сообщение заканчивается точкой. Далее подбираются столбцы, продолжающие участки текста в других строках, и т. д.

Сочетание лингвистического метода с учетом дополнительной информации довольно быстро может привести к вскрытию сообщения.

В заключение рассказа о шифрах перестановки приведем историю с зашифрованным автографом А. С. Пушкина, описанную в романе В. Каверина «Исполнение желаний».

Главный герой романа - студент-историк Трубачевский, - занимавшийся работой в архиве своего учителя - академика Бауэра С. И., - нашел в одном из секретных ящиков пушкинского бюро фрагмент недописанной X главы «Евгения Онегина». Это был перегнутый вдвое полулист плотной голубоватой бумаги с водяным знаком 1829 года. На листе было написано следующее.

(см. скан)

(см. скан)

Без особых усилий Трубачевский прочитал рукопись, и ничего не понял. Он переписал ее, получилась бессвязная чепуха, в которой одна строка, едва начавшая мысль, перебивается другой, а та - третьей, еще более бессмысленной и бессвязной. Он попробовал разбить рукопись на строфы, - опять не получилось. Стал искать рифмы, - как будто и рифм не было, хотя на белый стих все это мало похоже. Просчитал строку - четырехстопный ямб, размер, которым написан «Евгений Онегин».

Трубачевский с азартом взялся за рукопись, пытался читать ее, пропуская по одной строке, потом по две, по три, надеясь случайно угадать тайную последовательность, в которой были записаны строки. У него ничего не получалось. Тогда он стал читать третью строку вслед за первой, пятую за третьей, восьмую за пятой, предположив, что пропуски должны увеличиваться в арифметической прогрессии. Все то же! Отчаявшись, он бросил эту затею. Однако, она не давала ему покоя ни на лекции, ни в трамвае... Как шахматист, играющий в уме, он не только знал наизусть каждую строчку, он видел ее в десяти комбинациях сразу.

Прошло время. Однажды, когда он смотрел на светлые пятна окон подходящего к перрону поезда, каким-то внутренним зрением он

увидел перед собой всю рукопись - и с такой необыкновенной отчетливостью, как это бывает только во сне.

Простая перестановка без ключа - один из самых простых методов шифрования. Буквы перемешиваются по каким-либо правилам, но эти правила могут быть разными - и простыми и сложными.

Транспозиция

Допустим, у нас есть фраза: «МОЖНО, НО НЕЛЬЗЯ» . И мы хотим её зашифровать. Самый простой способ - это записать всю фразу задом наперёд: «ЯЗЬЛЕН ОН, ОНЖОМ» . Можно порядок слов в предложении оставить исходным, но каждое слово записать задом наперёд: «ОНЖОМ, ОН ЯЗЬЛЕН» . А можно менять местами каждые две буквы: «ОМНЖ,ООНЕНЬЛЯЗ» . Это называется «транспозиция» или простая перестановка в чистом виде.

Транспонирование

В этом шифре используется таблица. Сообщение записывается в таблицу по строкам, а для образования шифрованного текста считывается по столбцам. Ну или наоборот - записывается на столбцам, а считывается по строкам. Мы как бы переворачиваем таблицу относительно её диагонали, проходящей через верхний левый и нижний правый углы. Математики называют такой способ переворота таблицы транспонированием.

Для шифрования нужно нарисовать подходящего размера таблицу, вписать туда построчно шифруемый текст, а затем выписать его по столбцам в одну строку. Для расшифровки нужно лишь будет сообщить ключ шифра в виде размера таблицы. На рисунке ниже из ABCDEFGHIJKL получается ADGJBEHKCFIL . Согласитесь, понять без картинки, что это был алфавит, уже практически невозможно.

Итак, например, нам нужно зашифровать текст «Я памятник себе воздвиг нерукотворный, к нему не зарастёт народная тропа» . В нём 72 символа. 72 - удобное число, оно делится без остатка на 2,4,6,8,12,18,24,36, поэтому можно использовать таблицы 2x36, 3x24, 4x18, 6x12, 8x9, 9x8, 12x6, 18x4, 24x3, 36x2:). Определяемся с ключом (размером таблицы), вписываем текст по строкам, а затем переписываем его по столбцам.

На рисунке выше показаны варианты с таблицами 9×8, 8×9, 4×18 и 18×4. Для третьего варианта (таблица 4×18) получится вот такой текст:

«Ямиеввнкой у атрар якбоиеор,н зс ояопт езгртн енатнд панс д увыкмерёанта (4:18) »

В данном случае я взял текст «как есть», то есть с пропусками между словами и со знаками препинания. Но если текст осмысленный, то знаки препинания и пропуски между словами можно и не использовать.

Штакетник

Упрощённый вариант транспонирования (с двухстрочной таблицей) - «штакетник». Напоминает «по конструкции» забор-шахматку.

Это очень простой способ шифровки, часто применяемый школьниками. Фраза записывается в две строки: в верхней пишутся нечётные буквы, в нижней - чётные. Затем нужно выписать подряд сначала верхнюю строку, затем нижнюю. Такое шифрование легко проделать и в уме, не выписывая сначала две строки.

«Я памятник себе воздвиг нерукотворный» превращается в «ЯАЯНКЕЕОДИНРКТОНЙ ПМТИСБВЗВГЕУОВРЫ».

Скитала

Известно, что в V веке до нашей эры правители Спарты, наиболее воинственного из греческих государств, имели хорошо отработанную систему секретной военной связи и шифровали свои послания с помощью «скиталы», первого простейшего криптографического устройства, реализующего метод простой перестановки.

Шифрование выполнялось следующим образом. На стержень цилиндрической формы, который и назывался «скитала», наматывали спиралью (виток к витку) полоску пергамента и писали на ней вдоль стержня несколько строк текста сообщения. Затем

снимали со стержня полоску пергамента с написанным текстом. Буквы на этой полоске оказывались расположенными хаотично. Для восстановления текста требовалась скитала такого же диаметра.

По сути скитала - это наша обычная плоская таблица, обёрнутая вокруг цилиндра.

Считается, что автором способа взлома шифра скиталы является Аристотель, который наматывал ленту на конусообразную палку до тех пор, пока не появлялись читаемые куски текста. Изначально древний аппарат использовался в качестве сохранения секретных рецептов. Сейчас вместо узкой полоски пергамента можно использовать серпантин, а роль скиталы выполнит карандаш.

Сдвиг

Похожий результат можно получить, если буквы сообщения писать через определенное число позиций до тех пор, пока не будет исчерпан весь текст. Ниже пример готовой головоломки, составленной по таким правилам. «Три дробь четыре» - это подсказка, что зашифровано три слова, читать надо каждую четвёртую букву (4-8-12-16-..), по достижению конца переходить снова к началу со сдвигом на 1 букву влево (3-7-11-15-..) и т.д. На рисунке ниже зашифровано «Идите назначенным маршрутом».

Одиночная перестановка по ключу

Более практический метод шифрования, называемый одиночной перестановкой по ключу, очень похож на предыдущий. Он отличается лишь тем, что колонки таблицы не сдвигаются, а переставляются по ключевому слову, фразе или набору чисел длиной в строку таблицы. Кодируемая фраза записывается в подходящую таблицу построчно. Затем над таблицей вставляется пустая строка и в неё вписывается ключевое слово/фраза/последовательность чисел. Затем это ключевое слово/фраза/последовательность сортируется по алфавиту/значению, вместе с ней сортируются столбцы, тем самым перемешивая всю таблицу. Затем зашифрованная фраза выписывается построчно из этой перемешанной таблицы.

Например, можно сделать головоломку на основе судоку. Разгадывающему даётся текст «-УРОМКУЛО ЬУЁЗЕБЯДЛ НЗЯАТЛЫЙА ЦЬБАДНЕПУ ЕММДНИТОЁ ИЧТЮКЬНОО УНЁЙВЫЧЁС ХИЕПОТОДЦ ПРМГОУИК-» и предлагается решить судоку, в которой одна из строк помечена.

Решать эту головоломку придётся так: сначала нужно записать текст в таблицу 9×9, затем разгадать судоку, нарисовать пустую таблицу 9×9, надписать над ней ключевую строку из помеченной строки, и затем в таблицу под номерами вписать столбцы согласно их порядковым номерам в исходной таблице.

Для детей можно использовать этот же метод, но попроще, даже без цифр, а сразу нарисовав порядок перестановки в виде путей.

Двойная перестановка

Для дополнительной скрытности можно повторно шифровать сообщение, которое уже было зашифровано. Этот способ известен под названием «двойная перестановка». Для этого размер второй таблицы подбирают так, чтобы длины её строк и столбцов были не такие, как в первой таблице. Лучше всего, если они будут взаимно простыми. Кроме того, в первой таблице можно переставлять столбцы, а во второй строки.

Маршрутная перестановка

Обычное транспонирование таблицы (заполняем по строкам, читаем по столбцам) можно усложнить и считывать не по столбцам, а змейкой, зигзагом, по спирали или каким-то другим способом, т.е. задавать маршрут обхода таблицы. Такие способы заполнения таблицы если и не усиливают стойкость шифра, то делают процесс шифрования гораздо более занимательным. Правда, процесс расшифровки при этом усложняется, особенно, если маршрут неизвестен, и его ещё надо узнать.

На рисунке сверху последовательность символов «АБВГДЕЁЖЗИЙКЛМНОПРСТУФХЦЧШЩЪЫЬЭЮЯ.,?» вписана построчно в таблицу 6×6, а затем считана по маршруту, указанному линиями. Получаются следующие шифровки:

АЁЛСЧЭБЖМТШЮВЗНУЩЯГИОФЪ.ДЙПХЫ,ЕКРЦЬ?
АЁЛСЧЭЮЯ.,?ЬЦРКЕДГВБЖМТШЩЪЫХПЙИЗНУФО
АБЁЛЖВГЗМСЧТНИДЕЙОУШЭЮЩФПКРХЪЯ.ЫЦЬ,?
АЁЛСЧЭЮШТМЖБВЗНУЩЯ.ЪФОИГДЙПХЫ,?ЬЦРКЕ
НЗВБАЁЖМЛСТШЧЭЮЯЩУФЪ.,?ЬЫХЦРПЙКЕДГИО

А здесь нужно обходить таблицу «ходом коня», причём маршрут уже нарисован, так что это совсем для маленьких:)

Но если подать эту головоломку так, как показано ниже, то будет уже совсем не просто, так как вариантов обхода ходом коня может быть много, и нужно будет найти из всех этих вариантов единственный правильный.

Зашифровано «Пушкин. Медный всадник».

Перестановка "Волшебный квадрат"

Волшебными (или магическими) квадратами называются квадратные таблицы со вписанными в их клетки последовательными натуральными числами от 1 до n 2 (где n - размерность квадрата), которые дают в сумме по каждому столбцу, каждой строке и каждой диагонали одно и то же число.

В известном ещё в Древнем Китае квадрате Ло-Шу третьего порядка (3×3) константа квадрата 15 повторяется 8 раз:

по трём горизонталям: 2+9+4 = 7+5+3 = 6+1+8 = 15

по трём вертикалям: 2+7+6 = 9+5+1 = 4+3+8 = 15

по двум диагоналям: 2+5+8 = 4+5+6 = 15

Кстати, константу нечетного квадрата легко посчитать, умножив среднее число ряда, из которого составлен квадрат, на порядок квадрата. Для квадрата 3-го порядка (3×3) константа равна 1234 5 6789 *3=15.

Далее, чтобы зашифровать какое-то послание, нужно сначала подобрать или составить подходящий по размеру волшебный квадрат, затем нарисовать пустую таблицу такого же размера, и вписать буквы текста по очереди в таблицу в соответствии с номерами в волшебном квадрате. Затем просто выписываем построчно буквы из таблицы в одну длинную строку. Порядок квадрата должен быть равен округлённому в большую сторону корню из длины шифруемой строки, чтобы строка полностью вошла в квадрат. Если строка короче, то остаток можно заполнить произвольными буквами или цифрами.

На первый взгляд кажется, будто магических квадратов очень мало. Тем не менее, их число очень быстро возрастает с увеличением размера квадрата. Так, существует лишь один магический квадрат размером 3x3, если не принимать во внимание его повороты и отражения. Счёт волшебным квадратам 4-го порядка уже идёт на сотни, 5-го - на сотни тысяч. Поэтому магические квадраты больших размеров могли быть хорошей основой для надежной системы шифрования того времени, так как ручной перебор всех вариантов ключа для этого шифра был немыслим.

Есть очень простой метод составления нечётных волшебных квадратов, т.е. размером 3×3, 5×5, 7×7 и т.д. Это метод «террас» или «пирамидок».

Рисуется квадрат нужного размера и к нему пририсовываются ступенчатые «террасы» (обозначены пунктиром). Далее по диагоналям сверху вниз направо квадрат заполняется последовательными числами. После этого «террасы» переносятся внутрь квадрата: правые - налево, левые - направо, верхние - вниз, а нижние - наверх. Получается волшебный квадрат!

На базе этого метода можно составлять разные головоломки. Если использовать метод напрямую, то получится вот такая головоломка:

Чтобы решить эту головоломку, нужно буквы из «террас» перенести в квадрат, тогда в квадрате прочитается полное сообщение. Здесь зашифрована фраза «За мостом засада, пройти нельзя, переходите речку в брод.»

А если использовать метод наоборот, то получится головоломка типа такой.

Чтобы её решить, надо вытащить соответствующие буквы из квадрата в «террасы».

Для квадратов 4×4, 6×6 и т.д. таких простых способов их составления не существует, поэтому проще использовать готовые. Например, квадрат Дюрера.

Преобразования из этого шифра состоят в том, что в фигуру исходный текст вписывается по ходу одного ``маршрута"", а затем по ходу другого выписывается с нее. Такой шифр называют маршрутной перестановкой .

Например, можно вписывать исходное сообщение в прямоугольную таблицу, выбрав такой маршрут: по горизонтали, начиная с левого верхнего угла поочередно слева направо и справа налево.

Выписывать сообщение будем по другому маршруту: по вертикали, начиная с верхнего правого угла и двигаясь поочередно сверху вниз и снизу вверх.

При расшифровании надо определить число длинных столбцов, т.е. число букв в последней строке прямоугольника. Для этого нужно разделить число буев в сообщении на длину числового ключа. Остаток от деления и будет искомым числом.

Шифр ``Сцитала"" .

Одним из самых первых шифровальных приспособлений был жезл (``Сцитала""), применявшийся еще во времена войны Спарты против Афин в V веке до н. э.

Это был цилиндр, на который виток к витку наматывалась узкая папирусная лента (без просветов и нахлестов), а затем на этой ленте вдоль его оси записывался необходимый для передачи текст. Лента сматывалась с цилиндра и отправлялась адресату, который, имея цилиндр точно такого же диаметра, наматывал ленту на него и прочитывал сообщение. Ясно, что такой способ шифрования осуществляет перестановку местами букв сообщения.

Шифр ``Сцитала"‘ реализует не более n перестановок (n - длина сообщения).

Действительно, этот шифр, как нетрудно видеть, эквивалентен следующему шифру маршрутной перестановки: в таблицу, состоящую из столбцов, построчно записывают сообщение, после чего выписывают буквы по столбцам. Число задействованных столбцов таблицы не может превосходить длины сообщения.

Имеются еще и чисто физические ограничения, накладываемые реализацией шифра ``Сцитала"". Естественно предположить, что диаметр жезла не должен превосходить 10 сантиметров. При высоте строки в 1 сантиметр на одном витке такого жезла уместится не более 32 букв (10p < 32). Таким образом, число перестановок, реализуемых ``Сциталой"", вряд ли превосходит 32.

Шифр ``Поворотная решетка"".

Для использования шифра, называемого поворотной решеткой, изготавливается трафарет из прямоугольного листа клетчатой бумаги размера клеток.

В трафарете вырезано 2m x 2k клеток так, что при наложении его на чистый лист бумаги того же размера четырьмя возможными способами его вырезы полностью покрывают всю площадь листа.

Буквы сообщения последовательно вписываются в вырезы трафарета (по строкам, в каждой строке слева направо) при каждом из четырех его возможных положений в заранее установленном порядке.

Шифры замены. Математическая модель. Примеры.

Поточные шифры (Цезаря)

Блочные шифры (Порта и Пфейфера)

Основа – прямоугольная таблица, в которую записан систематически перемешанный алфавит.

Правило зашифрования:

Буквы биграммы (i ,j), i ¹ j , находятся в данной таблицк. При зашифровании биграмма (i ,j) заменяется биграммой (k ,l), где определяются с правилами:

Если i и j не лежат в одной строке или одном столбце, то их позиции образуют противоположные вершины прямоугольника. Тогда k и l – другая пара вершин, причем k – вершина, лежащая в той же строке, что и i .

Если i и j лежат в одной строке, то k и l – буквы той же строки, расположенные непосредственно справа от i и j соответственно. При этом если одна из букв – последняя в строке, то считается, что ее «правым соседом» является первая буква той же строки.

Аналогично если i и j лежат в одном столбце, то они заменяются «соседями снизу.»

Пример шифра Плейфера.

Пусть шифр использует прямоугольник 5x6, в который записан систематически перемешанный русский 30-буквенный алфавит на основе ключевого слова «командир».

В качестве «пустышки» будем использовать редкую букву ф .

Представим фразу в виде последовательности биграмм:

АВ ТО РО МФ МЕ ТО ДА ЯВ ЛЯ ЕТ СЯ УИ ТС ТО НФ

Шифртекст:

ВП ЗД ЗР ОХ ДБ ЗД КН ЭЕ ТЫ ТШ ШД ЩЖ ЖТ ЗД ОЧ

Криптоанализ шифра Плейфера опирается на частотный анализ биграмм, триграмм и четырехграмм шифртекста и особенности замены шифрвеличин на шифрообозначения, связанные с расположением алфавита в прямоугольнике.

Существенную информацию о заменах дает знание того, что используется систематически перемешанный алфавит.

Шифры перестановки. Математическая модель. Примеры.

Шифр, преобразования из которого изменяют только порядок следования символов исходного текста, но не изменяют их самих, называется шифром перестановки.

Пример

Рассмотрим, предназначенное для зашифрования сообщения длиной n символов. Его можно представить с помощью таблицы

где i1 - номер места шифртекста, на которое попадает первая буква исходного сообщения при выбранном преобразовании, i2 - номер места для второй буквы и т.д.

В верхней строке таблицы выписаны по порядку числа от 1 до, а в нижней - те же числа, но в произвольном порядке. Такая таблица называется подстановкой степени n . Зная подстановку, задающую преобразование, можно осуществить как зашифрование, так и расшифрование текста.

Зная подстановку, задающую преобразование, можно осуществить как зашифрование, так и расшифрование текста. Например, если для преобразования используется подстановка и в соответствии с ней зашифровывается слово МОСКВА, то получится КОСВМА.

Число различных преобразований шифра перестановки, предназначенного для зашифрования сообщений длины n , меньше либо равно n! (в это число входит и вариант преобразования, оставляющий все символы на своих местах!).

Шифры гаммирования. Математическая модель. Примеры.

Гамми́рование - симметричный метод шифрования, основанный на «наложении» гамма-последовательности на открытый текст. Обычно это суммирование в каком-либо конечном поле

Принцип шифрования заключается в формировании генератором псевдослучайных чисел (ГПСЧ) гаммы шифра и наложении этой гаммы на открытые данные обратимым образом, например путем сложения по модулю два. Процесс дешифрования данных сводится к повторной генерации гаммы шифра и наложении гаммы на зашифрованные данные. Ключом шифрования в данном случае является начальное состояние генератора псевдослучайных чисел. При одном и том же начальном состоянии ГПСЧ будет формировать одни и те же псевдослучайные последовательности.

Принципы построения блочных шифров. Схема Фейстеля.

Сеть Фейстеля:

Сеть Фейстеля - это общий метод преобразования произвольной функции F в перестановку на множестве блоков. Она состоит из циклически повторяющихся ячеек - раундов. Внутри каждого раунда блок открытого текста разделяется на две равные части. Раундовая функция

берет одну половину (на рис. правую), преобразует её с использованием ключа K i и объединяет результат с второй половиной посредством операции исключающее ИЛИ (XOR). Этот ключ задаётся первоначальным ключом K и различен для каждого раунда. Далее половинки меняются местами (иначе будет преобразовываться только одна половина блока) и подаются на следующий раунд. Преобразование сети Фейстеля является обратимой операцией.

Для функции F существуют определенные требования:

· её работа должна приводить к лавинному эффекту

· должна быть нелинейна по отношению к операции XOR

В случае невыполнения первого требования, сеть будет подвержена дифференциальным атакам (похожие сообщения будут иметь похожие шифры). Во втором случае действия шифра линейны и для взлома достаточно решения системы линейных уравнений.

Подобная конструкция обладает ощутимым преимуществом: процедурышифрования/расшифрования совпадают, только производные от первоначального ключи используются в обратном порядке. Это значит, что одни и те же блоки могут использоваться как для шифрования, так и для расшифрования, что, безусловно, упрощает реализацию шифра. Недостаток схемы заключается в том, что в каждом раунде обрабатывается только половина блока, что приводит к необходимости увеличивать число раундов.

Аатбаш, шифр Сцитала, решетка Кардано - известные способы скрыть информацию от чужих глаз. В классическом смысле шифр перестановки представляет собой анаграмму. Его суть заключается в том, что буквы открытого текста меняются по определенному правилу позициями. Иными словами, ключом шифра является смена очередности следования символов в открытом сообщении. Однако зависимость ключа от длины шифруемого текста породила множество неудобств для использования этого вида шифров. Но умные головы нашли интересные хитрые решения, которые описываются в статье.

Перевернутые группы

Для ознакомления с шифрованием методом перестановки упомянем один из простейших примеров. Алгоритм его заключается в разделение сообщения на n блоков, которые затем переворачиваются задом наперед и меняются местами. Рассмотрим пример.

"День уходил, и неба воздух темный".

Разделим это сообщение на группы. В данном случае n = 6.

"Деньух одили небав озд ухтем ный".

Теперь развернем группы, записав каждую с конца.

"хуьнед вабен дзо метху йын".

Переставим определенным образом местами.

"илидо метху йын хуьнед вабен дзо".

Для незнающего человека в таком виде сообщение представляет собой не более чем белиберду. Но, разумеется, тот, кому адресовано сообщение, ведает алгоритмом расшифровки.

Серединная вставка

Алгоритм данного шифрования немного сложнее перестановки:

Разделить сообщение на группы с четным количеством символов.

В середину каждой группы вставить дополнительные буквы.

Рассмотрим на примере.

"Земные твари уводил ко сну".

"Земн ыетв ариу води лкосну".

"Зеамн ыеабтв араиу воабди лкоасну".

В данном случае в середину групп были вставлены чередующиеся буквы "а"и "аб". Вставки могут быть разными, в разном количестве и не повторяться. Помимо этого, можно развернуть каждую группу, перемешать их и т.д.

Шифрограмма "Сэндвич"

Еще один занимательный и простой пример шифрования методом перестановки. Для его использования нужно открытый текст разделить на 2 половины и одну из них посимвольно вписать между букв другой. Покажем на примере.

"От их трудов; лишь я один, бездомный".

Разделим на половины с равным количеством букв.

"Отихтрудовлишь яодинбездомный".

Теперь запишем первую половину сообщения с большим интервалом между буквами.

"О т и х т р у д о в л и ш ь".

И в этих промежутках разместим буквы второй половины.

"Оятоидхитнрбуедзодволминшыьй".

Наконец сгруппируем буквы в своего рода слова (необязательная операция).

"Оятои дхи тнрбуе дзодвол миншыьй".

Зашифровать текст этим методом очень легко. Полученную строку-белиберду непосвященному придется разгадывать некоторое время.

Перестановки по "маршруту"

Такое название получили шифры, широко применявшиеся в древности. Маршрутом в их построении выступала какая-либо геометрическая фигура. Открытый текст записывался в такую фигуру по определенной схеме, а извлекался по обратной ей. Например, одним из вариантов может быть запись в таблицу открытого текста по схеме: змейка ползает в ячейках по часовой стрелке, а зашифрованное сообщение составляется путем списывания столбцов в одну строку, с первого по последний. Это также является шифрованием методом перестановки.

Покажем на примере, как зашифровать текст. Попробуйте сами определить маршрут записи и маршрут составления шифрограммы.

"Приготовлялся выдержать войну".

Будем записывать сообщение в таблицу размерами 3х9 клеток. Размерность таблицы можно определить, исходя из длины сообщения, или использовать некоторую фиксированную таблицу несколько раз.

Шифр будем составлять, начиная с правого верхнего угла таблицы.

"Ляунлвосйоятоввыгидтаерпрж".

Обращение описанных шагов не представляет труда. Достаточно просто сделать все наоборот. Данный способ является крайне удобным, потому что позволяет легко запомнить процедуру шифрования и расшифровки. А также он является интересным, потому что использовать для шифра можно любую фигуру. Например, спираль.

Вертикальные перестановки

Этот вид шифров также является вариантом маршрутной перестановки. Интересен он в первую очередь наличием ключа. Данный способ был широко распространен в прошлом и также использовал таблицы для шифрования. Сообщение записывается в таблицу обычным образом - сверху вниз, а шифрограмма выписывается по вертикалям, при этом соблюдается порядок, указанный ключом или паролем. Посмотрим на образец такого шифрования.

"И с тягостным путем, и с состраданьем"

Используем таблицу размерностью 4х8 клеток и запишем в нее наше сообщение обычным образом. А для шифровки используем ключ 85241673.

Теперь, используя ключ в качестве указания на порядок следования, выпишем столбцы в строку.

"Гусетмснтмаяпоьсысаоттмсеринид".

Важно заметить, что при этом способе шифрования пустые ячейки в таблице не следует заполнять случайными буквами или символами, надеясь, что это усложнит шифрограмму. На самом деле, наоборот, такое действие даст врагам подсказку. Потому что длина ключа окажется равной одному из делителей длины сообщения.

Обратная расшифровка вертикальной перестановки

Вертикальная перестановка представляет интерес тем, что расшифровка сообщения не является простым следованием алгоритму от обратного. Тому, кто знает ключ, известно, сколько в таблице столбцов. Чтобы дешифровать сообщение, нужно определить число длинных и коротких строк в таблице. Это позволит определить начало, откуда начинать записывать шифрограмму в таблицу, чтобы прочитать открытый текст. Для этого разделим длину сообщения на длину ключа и получим 30/8=3 и 6 в остатке.

Таким образом, нам стало известно, что в таблице 6 длинных столбцов и 2 коротких, заполненных буквами не до конца. Посмотрев на ключ, мы видим, что шифрование началось с 5-го столбца, и он должен быть длинным. Так мы находим, что первые 4 буквы шифрограммы соответствуют пятому по счету столбцу таблицы. Теперь можно записать все буквы по местам и прочесть тайное послание.

Данный тип относится к так называемым трафаретным шифрам, но по своей сути является шифрованием методом перестановки символов. В роли ключа выступает трафарет в форме таблицы с прорезанными отверстиями в нем. На самом деле трафаретом может быть любая фигура, но чаще всего используется квадрат или таблица.

Трафарет Кардано изготавливается по следующему принципу: вырезанные ячейки при повороте на 90° не должны перекрывать друг друга. То есть после 4 поворотов трафарета вокруг своей оси прорези в нем не должны совпадать ни разу.

Хотя послание может остаться и таким, но для передачи удобнее будет получить привычную на вид шифрограмму. Для этого пустые ячейки можно заполнить случайными буквами и выписать столбцы в одну строку:

"ЯВГВГМ ООЗГВС МУАКГЬ МБЗГНЬ ГОЩАГЕ СРЫУАГ"

Для того чтобы расшифровать это послание, получатель должен обладать точной копией трафарета, который был использован для шифрования. Данный шифр долгое время считался достаточно устойчивым. Также у него существует множество вариаций. Например, применение сразу 4 решеток Кардано, каждая из которых вращается своим образом.

Анализ шифров перестановки

Все перестановочные шифры уязвимы против частотного анализа. Особенно в случаях, когда длина сообщения сопоставима с длиной ключа. И этот факт не может быть изменен многократным применением перестановок, какими бы сложными они ни были. Поэтому в криптографии устойчивыми могут быть только те шифры, которые используют сразу несколько механизмов, помимо перестановки.

Шифры подстановки (замены) основаны на алгебраической операции, называемой подстановкой. Подстановкой называется взаимно-однозначное отображение конечного множества M на себя. Число N элементов множеств называется степенью подстановки. Количество n чисел действительно перемещаемых подстановкой называется длиной цикла подстановки.

Шифры перестановки – это шифр, преобразование из которого изменяют только порядок следования символов исходного текста, но не изменяют их самих.

Слабость шифров замены. Если в открытом сообщении часто встречается какой-то символ, то в шифрованном сообщении с такой же частотой встречается соответствующий символ. При больших объемах текста это приводит к успешному криптоанализу. Таким образом, на одном ключе нельзя шифровать достаточно длинные сообщения.

Сети (как элемент шифрования) – любой блочный шифр является комбинацией первых двух схем. Использование понятия «сети» в блочном шифровании заключается в многократном повторении исходных операций (повторения – циклы или раунды, а сами операции - слоями). Некоторые из слоев могут содержать ключи. Это позволяет:

Сделать шифр легко усложняемым (за счет увеличения количества раундов)

Сократить размера программного кода

Унифицировать алгоритмическую формулу шифрования

Сеть Фейсиля (Файсиля) – Feistel – это способ построения цикла шифрования в алгоритмах шифрования итеративных на основе регистра сдвига, с функцией обратной связи, зависящей от раундового ключа (оптимальное число раундов от 8 до 32)

DES – федеральный стандарт шифрования США (1997-2001).

Архитектура – классическая, сбалансированная сеть Фейсиля с начальными и конечными битовыми перестановками общего вида. Размер ключа – 56 бит. На его основе – международный стандарт ISO 8372-87. Алгоритм предназначен для шифрования данных 64-битовыми блоками.

DES представляет собой комбинацию двух основных методов:

Подстановка

Перестановка.

К тексту применяется единичная комбинация этих двух методов.

DES включает 16 раундов, то есть одна и та же комбинация методов применяется к открытому тексту 16 раз.

Наложение ключа-раунда производится операцией XOR

Исходный текст=>Начальная перестановка=>Шифрование * 16(<=Ключ) =>Конечная перестановка=>шифротекст

Цель начальной перестановки – равномерно распределить по блокам рядом стоящие биты.

Для зашифрования и расшифрования можно использовать одну и ту же функцию, но ключи используются в обратном порядке.

DES предусматривает 4 типа работы:

ECB-электронный шифр-блокнот. Открытый текст обрабатывается блоками по 64 бит, шифруемых одним ключом

CBC - цепочка блоков. Устраняет недостаток первого режима. Входное значение алгоритма зашифрования задается равным XOR-разности текущего блока открытого текста и полученного на предыдущем шаге блока шифрованного текста. Таким образом, все блоки исходного текста оказывается связанными (текст=>зашифрованный текст=>XOR=>текст=>зашифрованный текст)

CFB – обратная связь по шифро-тексту. Алгоритм преобразуется в поточный шифр, то есть каждый символ можно зашифровать и сразу передавать получателю

OFB – обратная связь по выходу. В регистр сдвига подается порция зашифрованного текста. Для каждого сеанса шифрования используется новое начальное состояние регистра.

Считается, что четырех режимов достаточно, чтобы использовать DES в практически любой области, для которой этот алгоритм подходит

Аппаратная реализация алгоритма на отдельной микросхеме позволяет достичь высокой скорости шифрования при незначительных габаритах устройства.

AES-федеральный стандарт шифрования США, используемый в настоящее время.

AES – улучшенный стандарт шифрования.

Требования:

Шифр должен быть блочным

Шифр должен иметь длину блока, равную 128 битам

Шифр должен поддерживать ключи длиной 128, 192, 256 бит

Алгоритм является нетрадиционным блочным шифром, поскольку не использует сеть Фейштеля для криптопреобразований.

Алгоритм представляет каждый блок кодируемых данных в виде двумерного массива байтов размером 4x4, 4x6 или 4x8 в зависимости от установленной длины блока.

Алгоритм состоит из определенного количества раундов (от 10 до 14 – это зависит от размера блока и длины ключа).

ГОСТ 28147089 – стандарт РФ на шифрование и имитозащиту данных.

Алгоритм предназначен для аппаратной и программной реализации, удовлетворяет необходимым криптографическим требования и не накладывает ограничений на степень секретности защищаемой информации.

Алгоритм реализует шифрование 64-битовых блоков данных с помощью 256-битового ключа, состоящего из восьми 32-битовых подключей.

На каждом i-м раунде используется K i -й подключ.

Алгоритмы шифрования ГОСТ 28147-89 обладают достоинствами других алгоритмов для симметричных систем и превосходят их своими возможностями.

На каждом i-м раунде алгоритма ГОСТ выполняется следующие операции:

L i =R i -1 , R i =L i -1 (плюсвкружочке)f(R i -1 , K i)

После выполнения этих 32 операций реализация алгоритма шифрования будет завершена.

Достоинством ГОСТ является наличие защиты от навязывания ложных данных (режим имитовставки), а также одинаковый цикл шифрования во всех 4 режимах (алгоритмах) ГОСТ.

Высокая криптостойкость обеспечивается за счет большой длины ключа (256 бит) и 32 раундов преобразования.

Стандарт включает режимы (алгоритмы):

Режим простой замены

Режим гаммирования

Режим гаммирования с обратной связью

Режим выработки имитовставки

Асимметричные алгоритмы шифрования.

В асимметричных алгоритмах шифрования (или криптографии с открытым ключом) для зашифрованной информации используют один ключ (открытый), а для расшифровывания – другой (секретный)

Эти ключи различны и не могут быть получены один из другого.

Схема обмена информацией:

Получатель вычисляет открытый и секретный ключи секретный ключ хранит в тайне, открытый же делает доступным (сообщает отправителю, группе пользователей сети, публикует)

Отправитель, используя открытый ключ получателя, зашифровывает сообщение, которое пересылается получателю

Получатель получает сообщение и расшифровывает его, используя свой секретный ключ

Использование асимметричного метода шифрования

Применение таких шифров стало возможным благодаря К. Шеннону, предложившему строить шифр таким способом, чтобы его раскрытие было эквивалентно решению математической задачи, требующей выполнения объемов вычислений, превосходящих возможности современных ЭВМ (например, операции с большими простыми числами и их произведениями; нахождение значения произведения P=x*y)

Криптосистема шифрования данных RSA.

В настоящее время наиболее развитым методом криптографической защиты информации с известным ключом является RSA, названный так по начальным буквам фамилий её изобретателей (Rivest, Shamir, Adleman)

Чтобы использовать алгоритмы RSA, надо сначала сгенерировать открытый и секретный ключи, выполнив следующие шаги:

Выбрать два очень больших простых числа p и q и определить n как результат умножения p на q (n=p*q)

Выбрать большое случайное число d. Это число должно быть взаимно простым с m результатом умножения (p-1)(q-1)

Определить такое число e, для которого является истинным следующее соотношения (e*d)mod(m)=1 или e=(1mod(m))/d

Открытым ключом будут числа e,n, а секретным ключом – числа d,n

Красным выделено создание ключа.

Асимметрические криптосистемы на базе эллиптических кривых.

На базе эллиптических кривых E можно реализовать не только криптоалгоритмы асимметричного шифрования, но и выработки общего секретного ключа для симметричного шифрования.

Криптосистемы на базе эллиптических кривых позволяют использовать существенно меньшие размеры ключей по сравнению с другими криптоалгоритмами при сохранении одинакового уровня криптостойкости.

Для перечисленных выше реализаций используются эллиптические кривые над полями Галуа GF(p) конечным числом p элементов двух видов:

Эллиптическая кривая над конечным полем типа E(GF(p)), где p – некоторое простое число

Эллиптическая кривая над конечным полем типа E(GF(2m)), где p=2m

Пример: Алгоритм асимметричного шифрования на базе эллиптических кривых ECES (Elliptic Curve Encryption Scheme)

Алгоритм Эль-Гамаля.

Система Эль-Гамаля – это криптосистема с открытым ключом, основанная на проблеме вычисления логарифма. Данный алгоритм используется как для шифрования, так и для цифровой подписи.

Множество параметров системы включает простое число p и целое g, степени которого по модулю p порождают большое число элементов Z p

Методы замены.

Шифр замены замещает одни символы другими, но сохраняет порядок их следования в сообщении.

4 типа замены (подстановки):

Моноалфавитная. Формула = Y i =k 1 X i +k 2 (modN), где Y i – i-символ алфавита, k 1 , k 2 – константы, X i – i-символ открытого текста, N - длина используемого алфавита.

Пример. Замена – открытый текст, Ключ – Ключ

Гомофоническая замена – замена одному символу открытого текста ставит в соответствие несколько символов шифртекста. Этот метод применяется для искажения статистических свойств шифротектста. Используется подстановка таблицей. Значения используются поочередно из столбца.

Полиалфавитная замена – использование нескольких алфавитов. Смена алфавита идет на каждом шаге шифрования. Используется ступеньчатая замена букв по таблице.

Полиграммная замена – формируется из одного алфавита с помощью специальных правил. Шифр располагается в матрице, а открытый текст разбивается на пары символов XiXi+1

Шифры перестановки.

Отличие шифра перестановки – изменяется только порядок следования символов сходного текста, но не изменяют их самих.

Пример. Текст «Грузите апельсины бочками Братья Карамазовы»

Шифротекст «Птр_аезгуионл_бысеьит_крабмчаизрямаакь_а__в____оы»

Приложение 2

Самостоятельная работа к практическому занятию

Самостоятельная работа по теме занятия включает в себя:

- изучение теоретического материала лекционных занятий, учебной литературы, Интернет-ресурсов, раздела «Краткие сведения из теории» настоящего описания ПЗ;
- выполнение практических заданий.