**МИНИСТЕРСТВО НАУКИ И ВЫСШЕГО ОБРАЗОВАНИЯ РОСИЙСКОЙ ФЕДЕРАЦИИ**

**Федеральное государственное бюджетное образовательное учреждение высшего образования «Кабардино-Балкарский государственный университет им. Х.М. Бербекова» (КБГУ)**

**ИНСТИТУТ ИСКУССТВЕННОГО ИНТЕЛЛЕКТА И ЦИФРОВЫХ ТЕХНОЛОГИЙ КАФЕДРА КОМПЬЮТЕРНЫХ ТЕХНОЛОГИЙ И ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ**

**КУРСОВАЯ РАБОТА**

по дисциплине

Разработка программных приложений

на тему:

**Шифратор, дешифратор????**

Выполнил:

студент 3 курса направления 09.03.03. Прикладная информатика (профиль «Корпоративные информационные системы»)

Дышеков А. С.

Руководитель: ???????? Елеев И.З \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

**Нальчик 2023**

**СОДЕРЖАНИЕ**

[**ВВЕДЕНИЕ** ?](#_Toc154671060)

[**1 ТЕОРЕТИЧЕСКОЕ ИССЛЕДОВАНИЕ** ?](#_Toc154671061)

[**1.1** **Основы криптографии** ?](#_Toc154671062)

[**1.2. Симметричные шифры**](#_Toc154671063) ?

[**1.3 Ассиметричные шифры и шифры с открытым ключом** ?](#_Toc154671064)

[**2** **ПРОЕКТИРОВАНИЕ И СОЗДАНИЕ ПРИЛОЖЕНИЯ**  ?](#_Toc154671065)

[**2.1 Разработка шифра Вижера** ?](#_Toc154671066)

[**2.2** **Разработка алгоритма шифрования Цезаря** ?](#_Toc154671067)

[**2.3 Реализация шифра Плейфера** ?](#_Toc154671068)

[**Заключение** ?](#_Toc154671069)

[**Список литературы** ?](#_Toc154671070)

# **ВВЕДЕНИЕ**

Шифрование и дешифрование - ключевые понятия в области криптографии, играющей важную роль в защите информации и обеспечении конфиденциальности данных. Шифраторы и дешифраторы представляют собой инструменты, используемые для зашифровки и расшифровки информации с целью обеспечения безопасности и конфиденциальности коммуникаций.

В современном цифровом мире, где данные передаются и хранятся в электронном формате, важно обеспечить защиту конфиденциальности и целостности информации. Шифраторы — это программы или устройства, которые преобразуют исходный текст или данные в нечитаемую форму, чтобы они стали непонятными для несанкционированных пользователей. Дешифраторы, напротив, представляют собой инструменты для обратного преобразования зашифрованной информации в исходный вид.

Исторически шифраторы и дешифраторы были разработаны для обеспечения конфиденциальности военных и политических сообщений. Однако с развитием информационных технологий и расширением сферы применения электронных коммуникаций, шифрование и дешифрование стали неотъемлемой частью повседневной жизни, применяемой во множестве областей, включая финансы, банковское дело, медицину и телекоммуникации.

Целью исследования является рассмотрение различных методов шифрования и дешифрования, их применение в современном мире, а также анализ их эффективности и безопасности. В рамках работы рассмотрены как классические методы криптографии, такие как шифр Цезаря и шифр Виженера, так и современные алгоритмы, используемые в цифровой безопасности.

В процессе создания программы рассмотрены следующие аспекты:

Теоретического работа, включает в себя основы криптографии. Здесь изучены основные принципы криптографии, ее цели и принципы работы. Далее рассмотрены симметричные шифры и ассиметричные шифры с открытым ключом. Это позволит понять основные подходы к шифрованию и дешифрованию данных.

Затем разработан шифра Виженера, который является классическим примером полиалфавитного шифра. Далее пойдет разработка алгоритма шифрования Цезаря, одного из самых простых и понятных методов шифрования. Завершающим этапом будет, шифр Плейфера, который является примером полиграммного шифра. Данное исследование важно для понимания основных принципов криптографии, обеспечения безопасности информации и развития средств защиты данных в условиях быстрого технологического прогресса и увеличения угроз кибербезопасности.

# **1 ТЕОРЕТИЧЕСКОЕ ИССЛЕДОВАНИЕ**

* 1. **Основы криптографии**

Криптография является наукой, посвященной защите информации от несанкционированного доступа и использования. В этом разделе изучены основы криптографии, рассматривая ее определение, цели и ключевые принципы.

Определение криптографии и ее цели: Криптография происходит от греческих слов "kryptos" (скрытый) и "grapho" (пишу) и представляет собой науку о создании средств защиты информации. Ее целью является обеспечение конфиденциальности, целостности и аутентичности данных.

Роль криптографии в обеспечении безопасности данных: В современном цифровом мире, где данные передаются и хранятся в электронном формате, криптография играет ключевую роль в обеспечении безопасности информации. Она используется для защиты информации как в публичных сетях, так и в локальных системах.

Основные принципы криптографии:

Конфиденциальность: Один из основных принципов криптографии, который обеспечивает, что информация доступна только тем, кто имеет на то право. Это достигается путем использования различных методов шифрования.

Целостность: гарантирует, что данные не были изменены незаконным образом в процессе их передачи или хранения. Методы хэширования и электронных подписей обеспечивают целостность данных.

Аутентичность: подтверждает истинность и идентификацию отправителя или получателя данных. Это обеспечивается использованием методов аутентификации, таких как цифровые сертификаты и подписи.

Изучение этих основ криптографии является важным шагом в понимании принципов защиты информации и обеспечения безопасности данных в современном мире.

История криптографии является богатой и увлекательной, охватывая множество эпох и культур.

Древний мир и классическая криптография:

С древних времен люди использовали шифры и методы для сокрытия информации. Одним из ранних примеров является шифр Цезаря, где каждая буква в сообщении сдвигалась на определенное количество позиций в алфавите.

Египтяне, древние греки и римляне также разрабатывали свои методы криптографии, включая использование замены символов и перестановки.

Средние века и ренессанс:

В этот период криптография стала более сложной, а методы шифрования стали более изощренными.

Шифр Плейфера, разработанный в 19 веке, является примером раннего использования полиалфавитных шифров.

Военные конфликты и развитие криптографии:

В ходе военных действий всегда было важно обеспечить конфиденциальность коммуникаций. Вторая мировая война стала временем интенсивного развития криптографии.

Энигма, немецкая шифровальная машина, была одним из самых известных шифров, подвергнутых взлому во время войны.

Криптография в эпоху компьютеров и цифровой эры:

Появление компьютеров изменило ландшафт криптографии. Математические методы стали широко использоваться для создания сложных алгоритмов шифрования.

RSA и AES стали одними из наиболее популярных алгоритмов шифрования, используемых в современных компьютерных системах.

Развитие квантовой криптографии:

Квантовая криптография представляет новое направление в области криптографии, использующее принципы квантовой механики для обеспечения абсолютной безопасности коммуникаций.

Квантовое распределение ключей (QKD) стало одним из ключевых методов в этой области.

История криптографии свидетельствует о том, как человечество всегда стремилось защитить свои секреты и коммуникации. С развитием технологий методы криптографии становились все более сложными и надежными, что делает их одним из важнейших инструментов в сфере информационной безопасности.

Типы криптографии

Симметричная криптография: Симметричная криптография использует один и тот же ключ для шифрования и расшифрования данных. Этот ключ должен быть известен как отправителю, так и получателю сообщения. Примеры алгоритмов симметричной криптографии включают DES (Data Encryption Standard), AES (Advanced Encryption Standard) и IDEA (International Data Encryption Algorithm).

Асимметричная криптография: В асимметричной криптографии используется пара ключей: публичный и приватный. Публичный ключ используется для шифрования данных, а приватный ключ используется для их расшифрования. Примеры алгоритмов асимметричной криптографии включают RSA (Rivest-Shamir-Adleman) и ECC (Elliptic Curve Cryptography).

Хэш-функции и цифровые подписи: Хэш-функции используются для преобразования произвольного входного сообщения в фиксированный размерный хэш. Они широко используются для проверки целостности данных и создания цифровых подписей. Цифровые подписи используют асимметричные криптографические методы для обеспечения аутентификации и подтверждения авторства сообщения. Это позволяет убедиться, что данные не были подделаны и что отправитель сообщения является тем, кем он утверждает быть.

## **1.2. Симметричные шифры**

В мире цифровых коммуникаций и передачи данных, криптография играет ключевую роль в обеспечении безопасности и конфиденциальности информации. Одним из фундаментальных понятий криптографии являются симметричные шифры.

Симметричные шифры представляют собой класс криптографических алгоритмов, где для шифрования и дешифрования используется один и тот же секретный ключ. Этот ключ должен быть известен только участникам обмена информацией и служит основным средством обеспечения конфиденциальности сообщений.

Процесс работы симметричных шифров начинается с выбора конкретного шифровального алгоритма и генерации секретного ключа. Этот ключ затем используется как для шифрования, так и для дешифрования сообщений. Отправитель шифрует исходное сообщение, применяя ключ к выбранному алгоритму, что превращает его в непонятный для посторонних шифротекст. Получатель, в свою очередь, использует тот же самый ключ и алгоритм, чтобы расшифровать полученный шифротекст обратно в исходное сообщение. Важно отметить, что безопасность симметричных шифров напрямую зависит от безопасности самого ключа, поскольку любой недобросовестный доступ к ключу может привести к компрометации конфиденциальности передаваемых данных.

Шифр Цезаря – это один из самых простых и наиболее известных шифров в истории криптографии. Его принцип основан на сдвиге каждой буквы в тексте на определенное число позиций в алфавите. Имя "Цезарь" происходит от имени римского императора Гая Юлия Цезаря, который, по преданию, использовал этот метод для обмена сообщениями со своими союзниками.

Принцип работы шифра Цезаря прост: каждая буква в открытом тексте сдвигается на определенное число позиций в алфавите. Например, при сдвиге на 3 позиции буква "А" становится "D", "Б" становится "Е", и так далее. При этом последняя буква алфавита циклически переходит на начало алфавита.

Шифр Цезаря примечателен своей простотой, но он также является крайне уязвимым к различным атакам. Поскольку количество возможных ключей в этом шифре ограничено количеством символов в алфавите (например, 26 для английского алфавита), шифр Цезаря легко поддается перебору. Другие методы криптоанализа также могут быть использованы для взлома этого шифра, включая частотный анализ букв и анализ контекста.

Не смотря на свою простоту, шифр Цезаря имеет свои приложения в обучении основам криптографии и стеганографии. Однако, в практическом применении этот шифр обычно не используется из-за своей низкой криптографической стойкости.

Шифр Виженера, изобретенный Блезом де Виженером в 16 веке, представляет собой полиалфавитный шифр, который считается одним из наиболее криптостойких методов шифрования до появления современных алгоритмов. Развитие этого шифра стало важным шагом в истории криптографии, так как он позволил существенно улучшить уровень защиты передаваемой информации.

Принцип работы шифра Виженера основан на использовании ключевого слова или фразы, которая повторяется до тех пор, пока не будет достигнута длина открытого текста. Каждая буква ключа используется для сдвига соответствующей буквы открытого текста на определенное количество позиций в алфавите. Этот процесс позволяет создавать непростые шифры, где каждая буква может быть зашифрована по-разному в зависимости от ее позиции в сообщении и ключевом слове.

Особенности шифра Виженера включают в себя его способность устойчиво противостоять частотному анализу, который успешно применяется к более простым шифрам, таким как шифр Цезаря. Благодаря использованию ключевого слова и полиалфавитного подхода, шифр Виженера усложняет задачу криптоаналитику, делая взлом более трудоемким.

Криптографическая стойкость шифра Виженера зависит от длины ключа и его случайности. Хорошо подобранный ключ, не использующий простых или повторяющихся паттернов, может сделать шифр Виженера очень сложным для взлома. Однако при использовании коротких или угадываемых ключей, а также при наличии повторяющихся фраз, уязвимость этого шифра возрастает.

Несмотря на свою криптостойкость, шифр Виженера все же подвержен некоторым атакам, включая частотный анализ, метод Касиски и атаку методом словаря. Эти методы могут быть эффективны, особенно при неправильном использовании шифра, например, при выборе слабого ключа. Все это делает важным правильное использование шифра Виженера в соответствии с современными стандартами криптографии.

В заключении главы можно сделать вывод, что симметричные шифры представляют собой значимый класс криптографических алгоритмов, используемых для обеспечения конфиденциальности данных в цифровом мире. Они играют ключевую роль в сфере кибербезопасности, обеспечивая защиту информации при передаче и хранении.

## **Ассиметричные шифры и шифры с открытым ключом**

В мире криптографии, асимметричные шифры и шифры с открытым ключом представляют собой один из наиболее интригующих и эффективных методов обеспечения безопасности данных.

Асимметричные шифры представляют собой фундаментальный класс криптографических алгоритмов, которые отличаются от симметричных шифров тем, что для шифрования и дешифрования данных используются различные ключи. Этот подход устраняет ряд ограничений, с которыми сталкиваются симметричные шифры, и расширяет возможности шифрования и защиты данных.

Асимметричные шифры, также известные как шифры с открытым ключом, основаны на использовании пары ключей: открытого и закрытого. Открытый ключ используется для шифрования данных, тогда как закрытый ключ служит для их расшифрования. Этот подход позволяет безопасно обмениваться данными в открытых сетях, так как открытый ключ может быть распространен публично, в то время как закрытый ключ остается в тайне у владельца.

Процесс работы асимметричных шифров включает в себя несколько этапов. Первый этап – генерация ключевой пары, состоящей из открытого и закрытого ключей. Затем открытый ключ распространяется для шифрования данных, тогда как закрытый ключ используется для их расшифрования. Критически важно сохранять закрытый ключ в секрете, поскольку доступ к нему дает возможность расшифровать зашифрованные данные.

В следующих разделах главы рассмотрим более подробно принципы работы асимметричных шифров, их преимущества и недостатки, а также практическое применение в сфере кибербезопасности.

Шифр Плейфера - это классический шифр, разработанный Шарлем Уэсткоттом в 1854 году. Он использует таблицу, известную как квадрат Плейфера, для шифрования и дешифрования текста. Квадрат Плейфера - это 5x5 таблица, заполненная буквами алфавита без учета буквы "J", которая обычно заменяется на "I".

Принцип работы шифра Плейфера заключается в том, что каждая буква сообщения заменяется соответствующей парой букв в таблице. Для шифрования каждая пара букв заменяется другой парой букв, определяемой положением букв в таблице. Дешифрование происходит в обратном порядке.

Особенности шифра Плейфера:

Простота реализации: Шифр Плейфера легко реализовать в видемеханического устройства или программного обеспечения.

Эффективность: В связи с использованием квадрата Плейфера, этот шифр позволяет эффективно шифровать сообщения, используя относительно небольшое количество символов.

Недостаток повторяющихся символов: Шифр Плейфера склонен к "склеиванию" повторяющихся символов в зашифрованном тексте, что может увеличить возможность криптоанализа.

Криптографическая стойкость и атаки на шифр:

Шифр Плейфера, как и многие классические шифры, уязвим для различных методов криптоанализа, включая частотный анализ и анализ биграмм. Его криптографическая стойкость намного ниже, чем у современных шифров.

Атаки на шифр Плейфера могут включать в себя попытку анализа частоты букв и биграмм в зашифрованном тексте, а также использование известных шаблонов и структур в естественном языке для разгадывания шифра.

В целом, шифр Плейфера, хоть и был эффективным в свое время, сегодня редко используется в практике криптографии из-за своей низкой стойкости к криптоанализу.

Шифр RSA был разработан в 1977 году Рональдом Ривестом, Ади Шамиром и Леонардом Адлеманом и является одним из самых известных и широко используемых асимметричных алгоритмов шифрования. Его безопасность основана на трудности факторизации больших простых чисел.

Принцип работы шифра RSA основан на использовании открытого и закрытого ключей. Открытый ключ используется для шифрования сообщений, а закрытый ключ - для их расшифровки.

Генерация ключей: В начале процесса генерируются два простых числа, которые служат закрытым ключом. Затем вычисляется открытый ключ на основе этих простых чисел.

Шифрование: Открытый ключ используется для шифрования сообщений. Каждое сообщение преобразуется в числовое значение и шифруется с помощью открытого ключа.

Расшифровка: Закрытый ключ используется для расшифровки зашифрованных сообщений. Только владелец закрытого ключа может расшифровать сообщения, зашифрованные его открытым ключом.

Особенности шифра RSA:

Безопасность: Шифр RSA основан на математических принципах теории чисел, таких как трудность факторизации больших простых чисел, что делает его крайне надежным.

Использование в цифровой подписи: Шифр RSA широко используется для создания цифровых подписей, которые подтверждают подлинность и целостность цифровых документов и сообщений.

Вычислительная сложность: Подбор приватного ключа, который является произведением двух больших простых чисел, является вычислительно сложной задачей, что делает алгоритм надежным.

Применение шифра RSA в современной криптографии:

Шифрование данных: RSA используется для шифрования данных при передаче по незащищенным сетям, таким как интернет.

Цифровые подписи: Шифр RSA широко применяется для создания и проверки цифровых подписей в коммерческих, финансовых и административных системах.

Аутентификация: RSA используется для аутентификации и защиты ключей доступа в различных протоколах и системах.

Шифр RSA остается одним из наиболее важных и надежных инструментов криптографии и широко применяется в различных областях информационной безопасности и защиты данных.

Асимметричные шифры, включая RSA, являются важным инструментом для обеспечения конфиденциальности и аутентификации в цифровой среде обмена информацией.

1. **ПРОЕКТИРОВАНИЕ И СОЗДАНИЕ ПРИЛОЖЕНИЯ**

## **2.1 Разработка шифра Вижера**

* 1. **Разработка алгоритма шифрования Цезаря**

## **Реализация шифра Плейфера**

# **Заключение**

Начало формы

# **Список литературы**