УДК 004.056.55

# Анализ современных методов шифрования информации

*Ересь Артём Владимирович*
*Приамурский государственный университет им. Шолом-Алейхема*
*Студент*

**Аннотация**
В данной работе рассмотрены современные методы шифрования информации. Проведен анализ этих методов, показаны сферы их использования, преимущества и недостатки.
**Ключевые слова:** Информация, методы шифрования, анализ.

# Analysis of the modern cryptography techniques of information

*Yeres Artem Vladimirovich*
*Sholom-Aleichem Priamursky State University*
*Student*

**Abstract**
In this paper, modern methods of encryption of information are considered. The analysis of these methods is carried out, the spheres of their use, advantages and disadvantages are shown.
**Key words**: Information, cryptography techniques, analysis.

В современном мире насчитывается более 3 миллиардов пользователей сети Интернет, то есть это почти треть населения планеты. В каждой сфере жизни человека присутствуют информационные технологии, огромный поток информации проходит через всемирную паутину. Достаточная ее часть имеет конфиденциальный характер. В условия быстрого развития информационных технологии вопрос защиты информации вызывает всё больший интерес с каждым годом. Для обеспечения секретности используются специальные методы, именуемые методами шифрования. Системы шифрования ставит перед собой цели по максимальному усложнению доступа к информации, лицам имеющим запрет на получение этой информации.

С помощью шифрования можно обеспечить такие характеристики информации как:

1. Целостность;
2. Идентифицируемость;
3. Конфиденциальность.

Целью данной работы является анализ современных методов шифрования информации. Мы рассмотрим основные понятия в шифровании и основные способы защиты информации.

В настоящее время вопрос шифрования информации имеют огромную популярность в сфере научно-исследовательской деятельности. Исследователь Е.В Мешкова в своей работе описывает процесс симметричного шифрования, где демонстрирует его основные характеристики [1]. В работе группы исследователей И.И. Баранковой, К.Р Гуринец., А.А. Хусаинова, Р.Ж. Санарбаева рассмотрены способы шифрования с помощью преобразования информации [2]. В своей статье С. Фаррелл привел примеры приложений с шифрованием, описал причины их разработки [3]. Р.Л. Политанский, П.М. Шпатарь, А.В. Гресь, А.Д. Верига предложили систему передачи данных, для функционирования которой, использованы зашифрованные данные. На примере был показан принцип работы системы [4]. Описали способ шифрования данных и их передачи между пользователями - А.И. Акмолдина и С.А. Куйтыбаева [5].

Для начала рассмотрим основные понятия в защите информации. Шифрование - процесс позволяющие скрыть информацию, при этом лишь владелец будет иметь возможность ее использования. Кодирование - информация с помощью специальной системы преобразовывается в код. Дешифрование - противоположный шифрованию процесс. Ключ - средство, необходимое для шифрования и дешифрования.

Истоки шифрования были положены достаточно давно, когда в мире появилась потребность скрыть информацию, ограничить круг людей имеющих к ней доступ. Основным аспектом для шифрования является запрет для использования и просмотра некой информации, для круга пользователей не имеющих ключа. Пользователь, имеющий ключ, сможет с легкостью прочесть сообщение.

Еще примерно 4-5 тысячелетий назад шифрование начало свое зарождение. Спустя некоторое время, примерно со средних веков по наши дни, шифрование стало использоваться для защиты различной информации. В государствах появилась необходимость засекретить некоторую документацию, связанную с управлением, обороной и законодательной деятельностью. Это дало сильный толчок в развитии такой науки как криптография. На сегодняшний день потребность в получении все более новых способов для защиты различной растет.

Криптография - наука о методах обеспечения невозможности прочтения информации, лицам не имеющим доступа; подтверждении авторства. Процесс проверки шифра на уязвимость для атак из вне называется криптоанализом. Криптостойкостью называется характеристика зашифрованного сообщения, отражающая его защищенность от взлома. Показателями этого считаются количество всех существующих ключей и время необходимое для взлома.

В наши дни различают два типа шифрования: симметричное и ассиметричное.

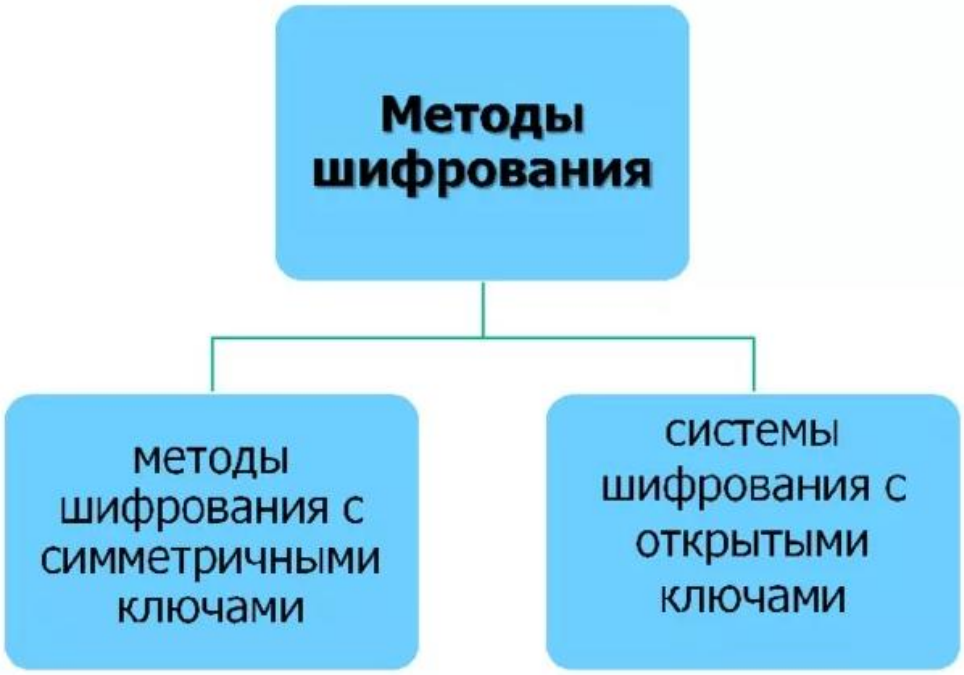


Рис. 1 Методы шифрования

При симметричном шифровании начальный легко читаемый текст, становится непонятен и не читаем. Это производится за счет использования ключа и именуется скремблированием данных. По окончании этого процесса информацию можно беспрепятственно передавать, не опасаясь за ее безопасность. В данной шифровании ключ - это главная часть для проведения процесса. Его необходимо скрыть от лишних глаз и закрыть к нему доступ для посторонних лиц, чтобы избежать возможную кражу этой информации.

Существенными недостатком для этого шифрования можно считать отсутствие защиты ключа и его ненадлежащее хранение. При получении этого ключа злоумышленник сможет получить полный доступ к информации, ущерб от этого будет нанесен владельцу информации.

В то же время асимметричный тип шифрования в отличие от симметричного для расшифровки использует совершенно другой ключ. К ключу шифрования может обратиться любой, но для проведения обратной операции имеет лишь владелец. Это несомненно является положительной стороной в этом типе, ведь криптостойкость имеет более высокий уровень.

Недостатком этого типа является возможность атаки с помощью перехвата информации во время ее передачи. По средством обмана и нехитрых операций злоумышленник может получить ключ, заставив при этом думать владельца, что отправителем является его собеседник, а не злоумышленник.

Существует так же методика хеширования, использующая в своей работе алгоритм хеш-функция. С помощью него можно генерировать предложенное сообщение в специальную строку. Данные используемые для генерации называются хеш. Очевидным преимуществом в плане безопасности является то, данные зашифрованные этим способом

возвращены в исходное состояние возможности не имеют. Благодаря этому, даже при получение злоумышленником хеша , он не будет иметь для него смысла и расшифровке не подлежит.

Существенным недостатком можно назвать то, что достаточно непросто расшифровать исходную информацию обратно. Однако это зависит от углубленности хеширования, в некоторых случаях возможна расшифровка с использование совпадений.

Среди основных современных методов шифрования информации, существуют такие как:

1. Подстановка - в исходном тексте происходит замена символов одного алфавита на символы того же либо другого алфавита. Для реализации создается специальная схема, в процессе используемая как ключ этого шифра.
2. Перестановка - расстановка символов соответствуя определенном ключу.
3. Гаммирование - в исходном тексте символы выделяются и складываются с последовательностью символов генерируемой системой (последовательность именуется гаммой).
4. Использование математических преобразований с помощью законов и формул.
5. Комбинирование подразумевает использование нескольких методов для шифрования текста.

Обратим внимание на то, что в основном при использовании одного метода, выявляется такой недостаток как низкая криптоустойчивость. Главным решением этого является использование нескольких методов одновременно. Несмотря на увлечение времени на процесс шифрования, все же это позволяет существенно повысить криптоустойчивость.

В жизни чаще всего применяются такие сочетания (цифра - номер метода в списке выше): 1+3, 2+3, 3+3, 1+2.

Таким образом, после рассмотрения методов шифрования информации можно сказать, что каждый из предложенных методов имеет свои положительные и отрицательные аспекты. Проанализировав, современные системы защиты информации можно сделать вывод, что информационные технологии не стоят на месте, и со временем появится больше методов защиты информации, что позволить уберечь вашу информацию от злоумышленников.

**Библиографический список**

1. Мешкова Е.В. Симметричное шифрование. Стандарт шифрования данных DES // Контентус. 2016. № 1 (42). С. 278-281.
2. Баранкова И.И., Гуринец К.Р., Хусаинов А.А., Санарбаев Р.Ж. Применение алгоритма шифрования методом цезаря для шифрования данных, представленных в текстовом формате // Актуальные проблемы современной науки, техники и образования. 2014. Т. 2. № 1. С. 152-155.

3. Фаррелл С. Приложения с шифрованием // Открытые системы. СУБД. 2010. № 5. С. 42.
4. Политанский Р.Л., Шпатарь П.М., Гресь А.В., Верига А.Д. Система передачи данных с шифрованием хаотическими последовательностями // Технология и конструирование в электронной аппаратуре. 2014. № 2-3. С. 28-32.
5. Акмолдина А.И., Куйтыбаева С.А. Защита данных. Шифрование данных // Сборник научных трудов по материалам международной научно-практической конференции. 2010. Т. 34. № 1. С. 13-14.