Департамент образования города Москвы

Государственное бюджетное общеобразовательное учреждение города Москвы «Гимназия №1505»

«Московская городская педагогическая гимназия-лаборатория»

**РЕФЕРАТ**

на тему

**Алгоритмы шифрования. Исследование алгоритмов шифрования.**

Выполнил:

Нефедов Никита Витальевич

Руководитель:

Королёва. А. А.

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

Рецензент:

Барышев Ю.Н.

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

 Москва

 2018/2019 уч.г.

# Введение

**Актуальность:** Данные постоянно передаются из одной точки в другую. Они содержат в себе необходимую информацию, которая позволяет выполнять определенные действия для другого человека. Если раньше ценные данные необходимо было передавать исключительно из рук в руки, то сейчас данная операция решается легко при помощи двух компьютеров, которые подключены через сеть Интернет. Для этого также необходим специальный инструментарий, который позволяет передать информацию любых объемов даже на тысячи километров.

**Проблема:** Мы ежедневно отправляем друг другу сотни сообщений, даже не подозревая, что они могут быть прочитаны кем-то посторонним. Если передаваемая нами информация перехвачена, но не несёт в себе компрометирующего характера, если она не может нанести вреда никому другому и не представляет особой ценности, то потерять ее не жалко. Однако, когда речь идёт о государственных и других подобных секретных документах, то требования к уровню безопасности резко подскакивают вверх. Именно для защиты подобных файлов необходимы программы шифрования.

**Цель:** исследование алгоритмов шифрования, их типов, а также принципов работы.

Оглавление

[Введение 2](#_Toc5961815)

[Глава 1 4](#_Toc5961816)

[Машины шифрования XX века 5](#_Toc5961817)

[Глава 2 6](#_Toc5961818)

[Симметрическое шифрование 6](#_Toc5961819)

[Асимметрическое шифрование 7](#_Toc5961820)

[Хэширование 8](#_Toc5961821)

[Вывод 10](#_Toc5961822)

[Источники: 11](#_Toc5961823)

Глава 1
История возникновения и развития алгоритмов шифрования

Криптография – это наука о методах обеспечения конфиденциальности, целостности данных, аутентификации, а также невозможности отказа от авторства. Изначально криптография изучала способы обратимого преобразования текста на основе ключа или заданного алгоритма в шифрованный текст.

История криптографии началась более четырёх тысяч лет назад. Первые попытки шифрования текста были предприняты около третьего тысячелетия до н.э. Тогда были использованы моно алфавитные шифры, основная идея которых – замена букв исходного алфавита на другие буквы этого же алфавита, но со смещением, например: (n+3).

С греческого языка криптография переводится как – «тайнопись» и определятся как наука, позволяющая вести тайную коммуникацию. Первым известным человеком, написавшим работу о криптографии, считается Эней Тактик, завершивший свою исследовательскую деятельность ещё до н.э.. Также попытки шифровки различных дынных предпринимали Месопотамия и древняя Индия, однако первые работающие системы шифрования были изобретены в Китае. Также следует заметить, что часто различные шифры и изощрённые способы письма использовали писари Древнего Египта. Наиболее эффективное применения шифров, разумеется, в военных целях, так например, крайне успешен был применённый против Афин Спартой шифр - «Скитала». Подобные методы шифрования использовали вплоть до XV века.

Однако крипто анализ не стоял на месте и вскоре все документы стало крайне легко дешифровать. Поэтому в шестидесятых годах XV века итальянский учёный и архитектор Леон Баттиста Альберти, стремясь получить устойчивый к частотному крипто анализу шифр, изобрёл новый способ шифрования – поли алфавитный. Это означает что ключем к алгоритму является два и более секретных алфавита, переходы от одного к другому осуществлялись по некоторому заданному автором правилу. К сожалению, Баттисте не удалось довести эту систему до полноценной, это в скором времени предстояло его последователям.

Криптография особенно активно использовалась и развивалась в Средние века. Различными шифрами пользовались политики, военные дипломаты и даже купцы. Ярчайшим примером средневеково шифра является кодекс Copiale – это невероятно красиво оформленный рукописный текст (на котором были также имелись водяные знаки), дешифровка которого, до сих пор не увенчалась успехом. Эпоха Возрождения можно считать золотым веком криптографии: ее активным изучением занимались многие учёные наиболее успешным стал Фрэнсис Бэкон, которому удалось описать семь методов скрытого текста. Также он выдвинул идею двоичного способа шифрования, аналогичный использующемуся в современных компьютерных программах. Также весомое влияние на дальнейшее усовершенствование и развитие криптографии было оказало появлением первого телеграфа, поскольку факт передачи данных перестал быть секретным, что заставило отправителей сосредоточиться на шифровке данных.

## Машины шифрования XX века

С начала и до середины XX века активно практикуется внедрение электромеханических устройств в работу шифровальщиков. Однако при этом продолжалось использование поли и моно алфавитных шифров. Несомненно, Вторая мировая война послужила своеобразным толчком к развитию компьютерных систем — через криптографию. Использованные шифровальные машины (немецкая «Энигма», английская «Бомба Тьюринга») ясно показали жизненную необходимость информационного контроля. Также послевоенное время правительства многих стран наложили мораторий на использование криптографии. Необходимые исследования были опубликованы исключительно в виде секретных докладов — таких, как, например книга Клода Шеннона «Теория связи в секретных системах», подходящая к криптографии как к новой математической науке.

С середины семидесятых годов начинается переход к строгой математической криптографии, появляются совершенно конкретные определения количества информации, энтропии, передачи данных и функций шифрования. Также одними из необходимых этапов считаются изучения защиты шифра от атак – линейных и дифференциальным. Первым об этом упоминает в своей работе Шеннон.

В 1967 выход книги «взломщики кодов» Дэвида Кана, обозначил новую точку отсчёта. В книге подробно были описаны история развития криптографии и дешифрования. После выхода книги Дэвида Кана, в открытой печати стали появляться и другие работы по криптографии. Однако до 1975 года криптография оставалась «классической», или же, более корректно, криптографией с секретным ключом.

Но прогресс не стоял на месте, и вот уже был сформирован современный подход к науке, были четко определены основные требования к зашифрованной информации: конфиденциальность, защита и целостность. Криптография была разделена на две взаимодействующие части: криптосинтез и криптоанализ. То есть криптографы обеспечивают информации защиту, а криптоаналитики, напротив, ищут пути взлома системы.

Глава 2
О современных криптографических алгоритмах

С течением времени, информации становилось всё больше и больше. Алгоритмы шифрования устаревали и приходилось изобретать новые.

На данный момент есть несколько типов программ шифрования, условно их можно поделить на три группы:

1 Программы, при работе с которыми необходим только один ключ.

2 Программы, при работе с которыми необходимы несколько ключей.

3 Программы, при работе с которыми не нужны ключи.



Далее я расскажу об одном типе шифрования из каждой группы.

## Симметрическое шифрование



При симметрическом шифровании данные, которые пользователь может прочитать, конвертируются в нечитаемый набор символов. Шифровка данных происходит с помощью ключа. После успешного шифрования, данные абсолютно безопасно можно передать другому пользователю или на ресивер. Для дальнейшей работы с данными необходим ключ, который использовался изначально. Соответственно, ключ является основным инструментом для работы с зашифрованными данными. Ключ практически невозможно подобрать, однако надо понимать, что ключ не должен попадать в руки третьим лицам, тогда информация снова становится незащищена. Ключ, в современных системах обычно представляет строку данных, которые получены из надежного пароля, или из совершенно случайного источника. Ключ вводится в используемую программу шифрования и данные могут быть расшифрованы. Скремблирование данных достигается с помощью симметричного алгоритма шифрования, такие как Стандарт шифрования данных (DES), расширенный стандарт шифрования (AES), или международный алгоритм шифрования данных (IDEA).

В настоящий момент одним из самых популярных алгоритмов шифрования является AES. AES обладает достаточно примитивной защитой длина его ключа составляет 256 бит. Однако это очень криптостойкий алгоритм, поскольку вскрыть такой шифр, то есть подобрать ключ к нему, не представляется возможным. Действительно, если длина ключа составляет 256 бит, то всего существует 2256 = 1,15792·1077 различных комбинаций ключей.

Также стоит отметить, что симметричное шифрование больше подходит для безопасного хранения информации. Есть целый ряд программ, которые могут осуществлять генерацию ключа и последующее его хранение. При этом ключ лучше всего хранить на USB-флэшке или диске потому что просто запомнить его не представляется возможным. В наиболее современных алгоритмах длина ключа обычно составляет 256 бит.

Подобный алгоритм шифрования очень распространён. В России также используется алгоритм аналогичный этому. Российский алгоритм – это блочный шифр, что означает, что алгоритм шифрует 64-битные блоки, а не отдельные никак не связанные символы. Алгоритм предусматривает 32 цикла, а его ключ имеет длину в 256 бит, за счёт такой защиты, алгоритм можно считать крайне надёжным и безопасным. Конечно, шифр можно разобрать, однако при использовании даже самых мощных современных компьютеров, на поиск ключа уйдёт не менее сотни лет.

## Асимметрическое шифрование



Аналогично симметрическому, работает асимметрический ключ, он также используется для шифровки передаваемых данных, однако, вместо того, чтобы использовать тот же ключ, что использовался для шифровки, используется абсолютно другой. Важно отметить, что ключ используемый для зашифровки, доступен всем пользователям и не представляет особой ценности, так ка было сказано выше, с его помощью невозможно подобрать «частный» ключ. Именно он используется для конечной расшифровки данных, и он необходим только получателю.

Обычно, программы в основе которых лежит асимметричное шифрование, используются для безопасной передачи данных от одного пользователя к другому с помощью интернета. Использование таких программ только для хранения данных просто не целесообразно. Очень легко привести правильный пример использования такой программы: вам необходимо получить данные в зашифрованном виде. Вы случайным образом создаёте 2 ключа и отправляете открытый ключ вашему товарищу по переписке. Ваш товарищ с помощью ключа шифрует данные, отправляет их вам. А вы в свою очередь расшифровываете полученную информацию (только с помощью второго ключа).

## Хэширование

Программы, в основе которых лежит хэширование, особое преобразование любого объема информации, в результате которого получается некое отображение, **образ**, называемый **хэшем** (hash). Хеширование данных использует алгоритм, называемый хэш-функцией. И имеет некоторые свойства: каждый хэш обозначает одни и те же данные, при этом не представляется возможным, зная хэш, получить исходные данные, а также получать данные из хэша в одиночку. Бесполезно пытаться подобрать входную информацию, чтобы получить аналогичных хэш. Метод хэширования отличается от двух других методов шифрования тем, что после шифровки информации, невозможно получить её заново в исходном виде. Подобный метод шифрования может гарантировать безопасность, поскольку даже если злоумышленник получит доступ к хэшу, он не сможет дешифровать данные содержащиеся в послании.

Если пользователь желает максимально поднять уровень защиты, он может комбинировать все три указанных выше способа шифрования.

Каждый из трёх методов имеет свои уязвимости, но при сочетании всех методов можно добиться абсолютной защиты данных. Подобная методика очень широко распространена среди крупных организаций. Использование симметричного и асимметричного методов даже имеют своё название – «цифровой конверт». Ассиметричная шифровка позволяет быстро расшифровывать данные, когда симметрическая шифровка используется преимущественно для более надёжной и скоростной передачи ключа. Рассмотрим работу программы шифрования электронной почты PGP основана на технике "цифровой конверт". Надёжность пароля достигается с помощью хэширования. Система хранить хэш пароля, а не сам пароль, соответственно при попадании хэша в руки злоумышленника, он никак не сможет им воспользоваться. В ходе проверки, система проверит хэш входящего пароля, и увидит, если результат совпадает с тем, что хранится. Сам же пароль можно обнаружить только в некоторые моменты (смена пароля или его проверка), что безусловно делает защиту более надёжной. Хеширование также используется для проверки подлинности данных с помощью секретного ключа. Хэш генерируется с использованием данных и этого ключа. Следовательно, видны только данные и хэш, а сам ключ не передается. Таким образом, если изменения будут сделаны либо с данными, либо с хэшем, они будут легко обнаружены. В заключение можно сказать, что эти методы могут быть использованы для эффективного кодирования данных в нечитаемый формат, который может гарантировать, что они останутся безопасными. Большинство современных систем обычно используют комбинацию этих методов шифрования наряду с сильной реализацией алгоритмов для повышения безопасности.

# Вывод

Прогресс не стоит на месте регулярно появляются новые программы шифрования, которые соревнуются между собой в степени защиты, используют огромное множество комбинаций, однако все они принадлежат одну из трёх типов (симметрический, асимметрический, хэшированый). Также существуют различные устройства для шифровки, в их основе лежит квантовая криптография.

Я считаю, что мне удалось выполнить поставленную цель и ознакомиться с алгоритмами шифрования. В следующем году я планирую на основе готовых алгоритмов (находящихся в открытом доступе в сети) написать собственную программу шифрования на языке C++.

# Источники:

Организация и технология защиты информации [электронный ресурс] Атлас профессий Хабаровского края Режим доступа: <http://atlasprofdv.ru/index.php/prof3/703-2014-06-26-23-05-20?page=&print=1&tmpl=component>

Необходимость шифрования данных в наше время [электронный ресурс] Азбука Морзе Режим доступа: <http://www.tiretochka.ru/news/166-neobxodimost-shifrovaniya-v-dannyx-nastoyashhee.html>

Криптография. История развития. Шифрование в сети Интернет [электронный ресурс] Студопедия Режим доступа: <https://studopedia.org/9-187186.html>

Классификация криптографических алгоритмов [электронный ресурс] Your Private Network Лаборатория Сетевой Безопасности Режим доступа: <http://ypn.ru/228/classification-of-cryptographic-algorithms/>

Симметричное и асимметричное шифрование [электронный ресурс] Программирование Режим доступа: <https://life-prog.ru/2_89996_simmetrichnoe-i-asimmetrichnoe-shifrovanie.html>

Программы для предотвращения несанкционированного доступа к информации [электронный ресурс] Сетевое издание «Компьютер пресс» Режим доступа: <https://compress.ru/article.aspx?id=18759>

Какие алгоритмы шифрования данных более безопасны [электронный ресурс] iteranet it журнал Режим доступа: [<http://iteranet.ru/it-novosti/2013/08/11/kakie-algoritmy-shifrovaniya-dannyx-bolee-bezopasny/>]