ГБОУ Гимназия №1505

«Московская городская педагогическая гимназия-лаборатория»

**Реферат**

**История криптографии**

*Автор*: ученица 9 класса «Б»

Зафт Маргарита

*Руководитель:* Коноркин И.О.

Москва

# 1. Оглавление

[1. Оглавление 2](#_Toc416071663)

[2. Введение 3](#_Toc416071664)

[3. Моноалфавитный и полиалфавитный методы шифрования 5](#_Toc416071665)

[3.1. Моноалфавитные методы шифрования 5](#_Toc416071666)

[3.1.1. Атбаш 5](#_Toc416071667)

[3.1.2. Шифр Цезаря 5](#_Toc416071668)

[3.1.3. Решетка Кардано 6](#_Toc416071669)

[3.2. Полиалфавитные шифры 7](#_Toc416071670)

[3.2.1. Шифр Виженера 7](#_Toc416071671)

[3.2.2. Шифр Гронсфельда 8](#_Toc416071672)

[4. Электромеханические устройства в шифровании 9](#_Toc416071673)

[4.1. Шифровальная машина KRYHA 9](#_Toc416071674)

[4.2. Шифровальноеустройство М-94. 10](#_Toc416071675)

[4.3. Шифровальная машина Enigma 10](#_Toc416071676)

[5. Шифрование с открытым ключом 11](#_Toc416071677)

[6. Заключение 13](#_Toc416071678)

[7. Список литературы 14](#_Toc416071679)

# 2. Введение

Мой реферат посвящен такой немаловажной теме, как история развития криптографии. Зародившись еще в третьем тысячелетии до нашей эры, она развивалась, проходя множество этапов, что позволило ей находиться на том уровне, в котором мы привыкли видеть ее сегодня. Криптография – наука, позволяющая сохранить аутентичность и конфиденциальность информации – является неотъемлемой и необходимой частью нашей повседневной жизни. Для засекречивания и расшифровки данных криптография зачастую использует ключи – секретную информацию, позволяющую шифровать/дешифровать информацию в криптографическом алгоритме.

Из-за высокой востребованности в наши дни, криптография постоянно развивается, модернизируется, и, как следствие, сильно отличается от той, что существовала в древности. Тем не менее, с течением времени основная цель криптографии осталось той же: защитить информацию от прочтения нежелательными получателями и обеспечить ей возможность быть правильно интерпретированной по достижению цели. Особенно сильный скачок в развитии данной науки произошел с появлением первых ЭВМ. Если информацию, зашифрованную человеком, еще можно было дешифровать без использования ключа, даже потратив на это большое количество времени и средств, то из-за сложности современных алгоритмов, осуществляемых машинами, утраченный ключ может привести к невозможности расшифровки информации или потребовать столь длительное время на дешифровку, что актуальность этой информации исчезнет.

На данный момент история насчитывает четыре основные периода развития криптографии. В первом из них преобладает принцип моноалфавитного шифрования, заключающийся в замене одних мелких единиц языка, как слово или буква, другими. Во втором люди применяли полиалфавитный шифр, заключающийся в циклическом использовании моноалфавитного. Третий период появился благодаря началу использования электромеханических устройств, при этом шифр так и остался полиалфавитным. В течении этих трех периодов использовалась криптография с закрытым ключом. В четвертом же периоде появилась криптография с использованием открытого ключа.

Проблемой моего реферата является то, что многие люди, пользуясь различными методами шифрования каждый день, не осознают значимость такой науки как криптография и не догадываются о ее богатой истории. Поэтому моей целью является ознакомление с понятием «криптография» в целом и изучение прогресса в ее развитии. Для достижения данной цели понадобилось выполнить ряд задач:

* Ознакомиться с литературой по теме шифрования данных;
* Разобраться с основами криптографии;
* Подробно изучить историю криптографии;
* Разбить ее на 3 этапа;
* Законспектировать полученные мной результаты в реферат.

При написании данного реферата я планирую собирать данные из различных источников информации. Основными для меня будут такие книги, как:

* "История криптографии. Часть I" А.В. Бабаш, Г.П. Шанкин
* "Книга шифров. Тайная история шифров и их расшифровки" Сингх С.
* "Криптография от папируса до компьютера" Жельников В.

Остальные же послужат дополнительными источниками, направленными на подтверждение полученных сведений и углубление познаний в теме.

# 3. Моноалфавитный и полиалфавитный методы шифрования

В первой главе мы рассмотрим моноалфавитный и полиалфавитный методы шифрования, которые использовались людьми до начала использования электромеханических устройств в шифровании. Эти методы являлись основоположниками современной криптографии.

## 3.1. Моноалфавитные методы шифрования

Моноалфавитный шифр, или, как его по-другому называют, шифр простой замены, простой подстановочный шифр, являет собой самый простой и самый древний метод шифрования, который, по сути, появился вместе с зарождением письменности. Его принцип состоит в том, чтобы заменять одни символы другими.

Самыми известными моноалфавитными шифрами являются Атбаш и Шифр Цезаря.

### *3.1.1. Атбаш*

Атбаш — это шифр подстановки, который изначально использовался только для иврита, но, в целом, применим к любому языку. Его суть состоит в том, что все буквы алфавита заменяются на буквы, имеющие тот же порядковый номер, но с конца.

То есть, данный шифр можно записать, как D(i)=n-i, где n — количество букв в алфавите, i — изначальный порядковый номер буквы, которую нам надо заменить, а D(i) — получаемый номер, который соответствует новому значению буквы, на которое мы ее заменяем. Получается, что алфавит выстраивается в обратном порядке.

История Атбаша насчитывает почти 20 веков, так как, предположительно, он появился примерно в 500 году до нашей эры и использовался вплоть до 1300 года нашей эры. Доподлинно неизвестно, кто изобрел Атбаш, но считается, что его придумала иудейская секта повстанцев, Ессеи. Ими было разработано множество различных шифров и кодов, так как это было важно, чтобы избежать преследования. Позже эти знания были переданы Гностикам (Гностицизм — условное название ряда позднеантичных религиозных течений, использующих мотивы Ветхого Завета, восточной мифологии и ряда раннехристианских учений), которые в последствии передали их Катарам (христианское религиозное движение). Позднее Катарские дворяне были завербованы Орденом Тамплиеров, которым, соответственно, были переняты знания шифров. Шифр перестал существовать с роспуском Ордена Тамплиеров.

### *3.1.2. Шифр Цезаря*

Шифр Цезаря, по-другому именуемый код Цезаря или сдвиг Цезаря, является одним из самых простых и наиболее известных методов шифрования. Он заключается в том, что алфавит «сдвигается», а каждая конкретная буква соответствует другой букве с определенным интервалом. В классическом шифре Цезаря использовался сдвиг вправо на три. То есть в целом шифр сдвига можно записать, как D(i)=i+k, при |k|<n, где i — порядковый номер начальной буквы, k — любое выбранное целое число, n — количество букв в отдельно взятом алфавите, а D(i) — получаемый порядковый номер буквы, на которую мы заменяем старую букву. При этом, если оказывалось, что D(i)<1, то отсчет начинался заново с конца алфавита, а если D(i)>n, то с начала.

Шифр, как не трудно догадаться, был назван в честь Гая Юлия Цезаря. Он был первым задокументированным человеком, который использовал эту схему, как уже говорилось раннее, сдвигая буквы на три, хотя доподлинно известно, что другие шифры с подстановкой использовались еще до него. Согласно «Жизни двенадцати цезарей» Светония, он использовался в целях защиты военных сообщений. Нельзя оценить, насколько эффективным был данный шифр во времена великого правителя, но разумно предположить, что он был достаточно надежен. Большинство врагов Цезаря были безграмотными, поэтому шифр мог восприниматься как сообщения на иностранном языке.

Так же этот шифр использовался племянником Цезаря, Августом. Подтверждение этому так же есть в книге Гая СветонияТранквилла «Жизнь двенадцати царей, Книга вторая».

Шифр подстановки так же использовался на мезузах (свиток определенного типа пергамента из кожи кошерного животного, содержащий часть текста молитва Шма, который прикреплялся к внешнему косяку двери в еврейском доме), чтобы зашифровать имя Бога. Есть предположение, что это делалось потому, что существовали времена, когда еврейскому народу не разрешали иметь мезузу.

В XIX веке были случаи, когда обычные любители, участвовали в секретных коммуникациях, которые были зашифрованы с помощью шифра Цезаря в «Таймс». Даже позднее, в 1915 году, данный шифр использовался в качестве аналога более сложным шифрам в российской армии.

### *3.1.3. Решетка Кардано*

Еще одним знаменитым методом шифрования является Решетка Кардано (рис. 2.1). Она была создана в середине шестнадцатого века ДжерламоКардано. Эта решетка может применяться как для криптографии, так и для стенографии (наука о секретной передаче информации, где сам факт передачи хранится в тайне).

Решетка представляет собой обычный квадрат с прорезями для вставки букв. Предложение или фраза, которую надо зашифровать, записывается по символу в каждую клетку. Затем решетка переворачивается на 90° и смещается на следующее место, после чего в нее вновь вписываются последующие символы сообщения. После того, как все сообщение записано, пустые места заполняются любыми другими символами так, чтобы получилась криптограмма или стенограмма.

Проблема такого метода шифрования заключается в том, что он подходит только для небольших сообщений, и большие исходные тексты для него неприменимы.



Рис. 3.1

## 3.2. Полиалфавитные шифры

Абу аль - Кинди первым предложил использовать многоалфавитный шифр. Наиболее распространенными полиафлавитными шифрами являются шифр Виженера и шифр Гронсфельда.

### *3.2.1. Шифр Виженера*

В целом, шифр Виженера изобретался неоднократно. Впервые он был описан итальянцем ДжованБаттистаБеллазо в середине XVI веке. Немногим позже, в 1586 году БлезВиженер представил своё описание того же самого метода шифрования перед комиссией Генриха III во Франции.

 Рис. 3.2

Для более удобного шифрования используется так называемая таблица Виженера. Вот так она выглядит для русского (рис. 3.2) и английского (рис. 3.3) языков.

Сверху по горизонтали записаны буквы шифруемые, а слева по вертикали написаны буквы ключа. В качестве ключа берется какое-либо слово или фраза. Чем больше символов будет в ключе, тем сложнее будет его расшифровать. Все символы шифруются циклически. То есть к символам по очереди применяется моноалфавитный метод шифрования. Когда ключ заканчивается, то к следующему символу кодируемого сообщения применяется вновь первый символ кода. Таким образом, если у нас есть ключ длиной в n символов, то мы применяем шифровальную строку первого символа ключа к первому символу кодируемого сообщения, строку второго символа ко второму и так далее. Когда мы доходим до n+1 символа кодируемого сообщения, то снова используем первый символ для кодирования. Таким образом, если мы хотим зашифровать слово «криптография» с помощью слова «ключ» для удобства мы можем нарисовать вот такую таблицу:

|  |  |  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| Кодируемое слово | к | р | и | п | т | о | г | р | а | ф | и | я |
| Ключ | к | л | ю | ч | к | л | ю | ч | к | л | ю | ч |
| Получаемый текст | х | ь | ж | ж | э | ъ | б | з | ч | а | ж | ц |



Естественно, что для дешифровки надо использовать данный алгоритм в обратном порядке.

### 3.2.2. Шифр Гронсфельда

Шифр Гронсфельда (рис. 3.4), который был гораздо более популярен в Европе, состоит примерно в том же. Единственное его отличие от шифра Виженера состоит в том, что вместо буквенного ключа в нем используется числовой. То есть все буквы слева заменяются на числа.
Количество чисел зависит от количества букв в алфавите. Соответственно каждое из заданных чисел ключа и является сдвигом алфавита. Рис. 3.3

Во времена Первой мировой войны стали использоваться новые, более сложные методы шифрования, но о них будет рассказано в следующей главе.

Однако эти методы шифрования были несовершенны, так как подвержены частотному анализу. Этот метод криптоанализа основывается на предположении, что отдельные символы используются в языке чаще других. С его помощью можно узнать, какой символ соответствует какому. Рис. 3.4

# 4. Электромеханические устройства в шифровании

Новым шагом в криптографии стало использование электромеханических машин. Наиболее веской причиной для их использования были мировые войны двадцатого века. В них электромеханические устройства использовались как для шифрования, так и в последствии для дешифрования текстов. Это позволило создавать более сложные шифры и взламывать их.

## 4.1. Шифровальная машина KRYHA

**В начале 1920 годов была изобретена KRYHA (рис. 4.1). Этамашинасостоялаиздвухконцентрическихколец, накоторыхнаписаналфавит.Внутреннеекольцоперемещалосьнаопределенноечисломест с помощьюрычага, приводившего в действие пружинный двигатель.Тогдакаждаябукваисходноготекста, алфавиткоторогобылнаписаннавнешнемкольце, соответствовалабуквенавнутреннемкольце, с помощьюкоторого и шифровалсяисходныйтекст.Этоустройствоиспользовалось в томчиследипломатамиГерманиивовременаВтороймировойвойны, которыенезнали, чтошифрбылраскрытамериканцами. Рис. 4.1

## 4.2. Шифровальноеустройство М-94.

Устройство состояло из 25 алюминиевых колец (рис. 4.2), соединенных стержнем длиной в 12 сантиметров. Каждое кольцо содержало буквы алфавита в произвольном порядке по окружности. Исключением являлось только первое кольцо, начинающееся со слов «ARMY OF THE USA» (армия США).

 Рис. 4.2

## 4.3. Шифровальная машина Enigma

В 1923 году было создано электромеханическое устройство под названием Энигма (рис. 4.3), которое служило для зашифровки и расшифровки текстовой информации. Наибольшее распространение машина получила в нацистской Германии во времена Второй мировой войны. Несмотря на слабость шифра с точки зрения современной криптографии, в средине двадцатого века только стечение благоприятных факторов позволило дешифровать Энигму.

Энигма – роторная машина. Она содержала в себе механическую и электрическую подсистемы. Клавиатура была подсоединена к роторам (набор крутящихся дисков, расположенных вдоль вала и прилегающих к нему), которые при нажатии клавиш сдвигались в сторону (самый правый сдвигался на одну позицию, а при определенных условиях перемещались и другие роторы). Это смещение приводило к разным криптографическим преобразованиям при каждом последующем нажатии на любую из клавиш клавиатуры.

 Рис. 4.3

Процесс шифрования протекал электрически. Механические части смещались, контакты замыкались, образовывался меняющийся механический контур. При нажатии на клавиши контур размыкался, цепь, через которую проходил ток, менялась и включал одну из ряда лампочек, которая отображала нужную букву.

Сам по себе метод шифрования был прост – элементарная замена, на за счет нескольких связанных роторов из-за их постоянного движения надежность шифра возрастала.

# 5. Шифрование с открытым ключом

Основная идея шифрования с ассиметричным ключом состоит в том, что для зашифровки данных прибегают к использованию одного ключа, а для дешифровки – другого. Из-за этого такой метод шифрования называют ассиметричным. Таким образом отправитель, который зашифровывает сообщение, не обязательно должен знать, каким образом сообщение может быть расшифровано. То есть, даже имея исходное зашифрованное сообщение, ключ и алгоритм шифрования, невозможно дешифровать сообщение без знания ключа расшифровки. Ключ, с помощью которого шифруется сообщение, называют открытым. Он может быть известен абсолютно всем. Дешифровка с его помощью невозможна. Ключ, с помощью которого ведется дешифрование называется закрытым. Его должен знать только получатель сообщения.

Для этого используются односторонние функции. В них, при знании значения аргумента можно вычислить функцию, но зная значение функции определить обратно аргумент без определенных условий невозможно. Сегодня насчитывают семь типов односторонних преобразований, с помощью которых возможно создание криптосистем с открытым ключом.

1. Разложение чисел на простые множители
2. Дискретное логарифмирование или возведение в степень
3. Задача об укладке ранца
4. Вычисление корней в алгебраических уравнениях
5. Использование конечных автоматов
6. Использование кодовых конструкций
7. Свойства эллиптических кривых

Любое шифрование с открытым ключом можно разбить на три этапа (рис. 5.1): генерация ключей, шифрование и расшифровка. При генерации ключей важно создать как минимум два: открытый и закрытый. С помощью открытого ключа производится шифровка исходного текста, а с помощью закрытого – дешифровка. Таким образом, закрытый ключ должен знать только получатель сообщения. Рис. 5.1

Рассмотрим первый тип. Разложение на простые множители – один из самых часто применяемых способов шифрования с открытым ключом в наши дни. Первой системой, пригодной и для шифрования, и для цифровой подписи (цифровой аналог ручной подписи, использующийся для придания электронному документу юридической силы, которая равна по силе подписанному бумажному аналогу), стала RSA. Аббревиатура образована от первых букв фамилий ее создателей – Rivest, Shamir и Adleman.

Для шифрования с помощью системы RSA нам понадобятся два простых числа. Для примера возьмем a=7 и b=11. На самом деле в таком шифре обычно используются гораздо большие простые числа, но пример может быть рассмотрен и на маленьком. Затем нам понадобится произведение этих чисел n=a\*b=77. Число n называют модулем. После этого нам понадобится вычислить функцию Эйлера от n. Функция Эйлера показывает, сколько есть чисел, которые меньше n и одновременно взаимно простые с ним. Поскольку число n состоит из произведения чисел a и b, то ϕ(n)=ϕ(a)\*ϕ(b). Поскольку a и b – простые числа, ϕ(a)=a-1, а ϕ(b)=b-1, так как все натуральные числа, меньшие простого числа, взаимно просты с ним. Таким образом ϕ(n)=(a-1)(b-1). Тогда в нашем случае ϕ(n)=10\*6=60.

Затем выбирается некое число e. Его называют открытой экспонентой. Оно должно быть взаимно простым со значением ϕ(n), целым, больше единицы, но меньше ϕ(n). Для примера возьмем e=7. Столь малое значение e может потенциально ослабить безопасность схемы RSA, поэтому обычно используются более большие числа. Из числа e мы можем вычислить d – секретную экспоненту. При этом d=e-1 mod ϕ(n), тогда d=43. Пара e и n используется в качестве открытого ключа. В качестве закрытого используется пара d и n.

Предположим, что шифруемый текст – N, а зашифрованный представим, как M. Тогда алгоритм шифрования можно записать, как M=Ne mod n.Дешифровка же будет выглядеть, как N = Md mod n. По формуле все выглядит довольно просто, однако при использовании чисел , занимающих сотни бит, процесс шифровки и дешифровки начинает требовать огромного количества времени.

# 6. Заключение

Походу истории наука криптографии изменялась в зависимости от потребностей того или иного временного отрезка. Чем искуснее становились шифры, тем сложнее становились пути их взлома. Но на каждый раз с появлением нового метода дешифровки появлялись и новые способы кодирования информации. Таким образом, криптография никогда не стояла на месте, совершенствуясь.

Как мы можем заметить, в последние века интерес к шифрованию заметно вырос, а его развитие пошло в разы быстрее. Я считаю, это связано с развитием компьютерных технологий, так как они не могут существовать без шифрования. Тем не менее, на протяжении веков криптография так же занимала немало важную позицию. Она сыграла существенную роль в истории человечества, помогая скрыть информацию от нежелательного прочтения, тем самым сохраняя ее аутентичность и конфиденциальность.

Криптография прошла долгий путь. Начиная с простого шифрования без использования ключей, она прошла долгий путь до криптографии с открытым ключом. Каждый раз тот или иной способ шифрования становился все менее действенным, так как время на его расшифровку сокращалось. Или после раскрытия алгоритма шифрования он становился бесполезным.

Сейчас криптография используется повсеместно в том числе и в обычной жизни. Она составляет огромную часть нашей жизни, которую мы зачастую даже не замечаем, потому что она стала привычной и обыденной, так и оставаясь совершенно непонятной и неизведанной для большинства. Таким образом, не зная, с чем имеем дело, мы не можем добиться максимальной производительности от того, что мы делаем. Поэтому я считаю, что важно знать историю того, что мы ежедневно используем.

# 7. Список литературы

1. Адаменко М. Основы классической криптологии. Секреты шифров и кодов - ДМК-Пресс, 2012

2. Алферов А.П. Основы криптографии - М.: Гелиос АРВ, 2002

3. Бабаш А.В., Шанкин Г.П. Криптография - М.:СОЛОН-ПРЕСС, 2007

4. Бабаш А.В., Шанкин Г.П. История криптографии - Гелиос АРВ, 2002

5. Жельников В. Криптография от папируса до компьютера - М.: Изд-во "ABF", 1996

6. Сингх С. Книга шифров. Тайная история шифров и их расшифровки – Астрель, 2007

7. Шнайер Б. Подстановочные шифры // Прикладная криптография. Протоколы, алгоритмы, исходные тексты на языке Си = AppliedCryptography. Protocols, AlgorithmsandSourceCodein C. — М.: Триумф, 2002.