Федеральное государственное образовательное бюджетное учреждение высшего образования

«ФИНАНСОВЫЙ УНИВЕРСИТЕТ ПРИ ПРАВИТЕЛЬСТВЕ

РОССИЙСКОЙ ФЕДЕРАЦИИ»

(Финансовый университет)

**Колледж информатики и программирования**

**Отчёт о проделанной работе  
по реферату № 1 по дисциплине**

**МДК.02.02 «Криптографические средства и методы защиты информации»**

На тему: «История развития криптографии»

Студент группы 3ОИБАС-1221

|  |  |
| --- | --- |
| Кован Н. В. | «06» ноября 2023 г. |

Основная профессиональная образовательная программа по специальности

10.02.05 Обеспечение информационной безопасности автоматизированных систем

Форма обучения очная

Проверил: \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ Рой А.В.

Москва

2023

**Введение**

Криптография, искусство обеспечения конфиденциальности и безопасности информации, имеет древнюю и богатую историю. С самых древних времен люди стремились зашифровать свои тайны и обеспечить безопасность своих коммуникаций. История развития криптографии является захватывающим путешествием от простых шифров и кодов до сложных математических алгоритмов, используемых в современных системах шифрования. В этом реферате мы исследуем ключевые этапы этой увлекательной истории, начиная с древности и заканчивая современными методами криптографии, которые обеспечивают безопасность информации в цифровую эпоху.

**Цель работы:** исследовать историю развития криптографии от древности до наших дней. Чтобы достичь этой цели надо решить следующие задачи:

* Провести анализ исторических источников для выявления первых примитивных методов криптографии, используемых в различных культурах и эпохах;
* Исследовать и проанализировать классические методы шифрования, такие как шифр Цезаря, шифр Атбаш и др.;
* Выделить ключевые события в истории криптографии, такие как использование шифров во временах войн, взлом.

Актуальность данной темы несомненна в современном мире информационных технологий и кибербезопасности. Вот почему:

* Понимание исторических контекстов;
* Уроки из прошлого;
* Связь с современными технологиями;
* Кибербезопасность и личная приватность;
* Развитие навыков анализа и исследования.

**Изучении истории развития криптографии**

**Тайнопись древних цивилизаций**

Под заученным термином "криптография" (что буквально означает "тайнопись" по-древнегречески) скрывается вековое стремление человека сохранить важные сведения от посторонних глаз. Начиная с самых ранних времен, письменность сама по себе являлась криптографической системой, поскольку она принадлежала узкому кругу лиц, обеспечивая обмен знаниями, недоступными неграмотным. С распространением письменности возникла потребность в более сложных методах шифрования. Со времен старинных цивилизаций криптография служила нуждам военных, чиновников, купцов и хранителей религиозных секретов.

Одним из самых древних известных примеров использования шифра (приблизительно в 4000 году до н.э.) считается древнеегипетский папирус, на котором перечислены памятники времен фараона Аменемхета II. Автор, оставшийся безымянным, изменил обычные иероглифы, возможно не для того, чтобы скрыть информацию, а скорее для более сильного воздействия на читателя.

Один из известных шифров, древнесемитский атбаш, возник приблизительно в 600 году до н.э. Его простой метод заключался в замене букв алфавита, создавая криптограммы, которые можно найти в тексте Библии.

В Древней Спарте была использована скитала – шифр, представляющий собой цилиндр, обернутый полоской пергамента. Текст писали вдоль пергаментной полосы. После развертывания ленты текст становился шифром, который можно было прочитать только с помощью цилиндра такого же диаметра. Эта спартанская скитала можно назвать одним из первых криптографических устройств.

В IV веке до н.э. автор военных трактатов Эней Тактик создал шифровальный диск, названный его именем. Для записи сообщения нить пропускалась через отверстия диска, каждое из которых было подписано буквой. Для расшифровки текста нужно было просто вытянуть нить в обратной последовательности. Главный недостаток этого устройства заключался в том, что при наличии времени шифр мог быть разгадан кем угодно, обладающим достаточными знаниями. Однако, чтобы быстро удалить информацию с диска Энея, было достаточно вытащить нить или разрушить устройство.

Один из первых задокументированных в истории шифров - шифр Цезаря (приблизительно в 100 году до н.э.). Его принцип был прост: каждая буква в исходном тексте заменялась другой, находящейся в алфавите на определенное число позиций. Если знать это число, можно было разгадать шифр и раскрывать секреты, которые Цезарь передавал своим генералам.

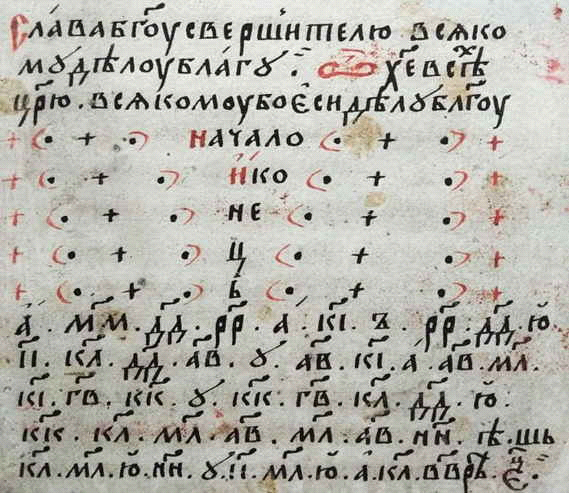
Криптография была распространена среди многих древних народов, но особый прогресс в этой области произошел в наше эпоху благодаря арабским ученым. Их высокий уровень математических знаний и языковых навыков позволил им не только создавать свои собственные шифры, но и расшифровывать чужие. Это стало отправной точкой для развития научных исследований в области криптоанализа - исследования методов дешифровки сообщений без знания ключа. Эпоха "наивной криптографии", когда шифры больше напоминали головоломки, подошла к концу.

**Тарабарщина, цифирь и другие шифры**

Работы арабских ученых способствовали появлению полиалфавитных шифров, более стойких к расшифровке, в которых использовались сразу несколько алфавитов. Однако люди Средневековья продолжали пользоваться простыми шифрами, основанными на замене букв другими буквами или цифрами, неправильном написании букв и т.д. В Средние века в Европе считалось, что криптография была тесно связана с магией и каббалой.

Интересно, что в Древней Руси тоже были свои способы тайнописи, например литорея, которая делилась на простую и мудрую. В мудрой версии шифра некоторые буквы заменялись точками, палками или кругами. В простой литорее, которая еще называлась тарабарской грамотой, все согласные буквы кириллицы располагались в два ряда. Зашифровывали письмо, заменяя буквы одного ряда буквами другого.

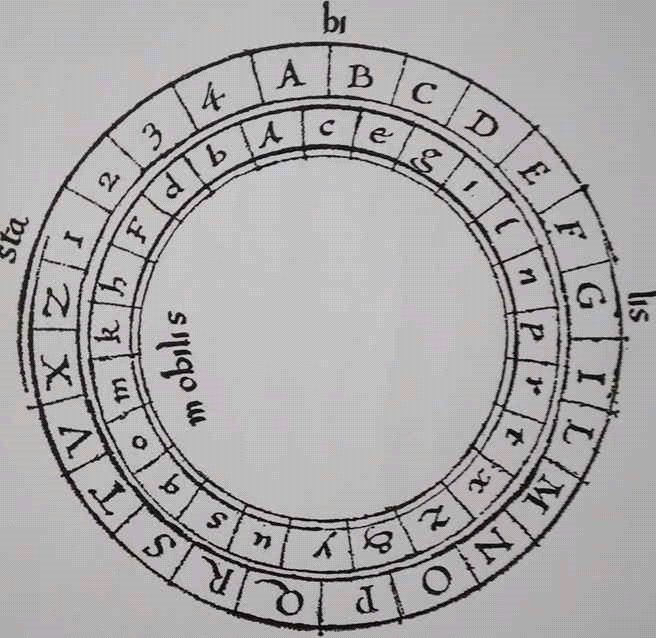
Еще одним известным шифром Древней Руси была цифирь, когда буквы, слоги и слова заменялись цифрами. Иногда для усложнения в шифр добавлялись математические действия, и было непросто разгадать подобную загадку: «Десятерица сугубая и пятерица четверицею, единица четверицею сугубо и десятерица дващи».



**Рисунок 1.**Тайнопись XVI века.

В период Возрождения криптография переживает свой расцвет. Это время характеризуется развитием формальной криптографии и появлением более структурированных и надежных шифров. Ученые эпохи Ренессанса сталкивались с загадками, которые криптографы в последующие столетия пытались разгадать.

Примерно в 1466 году итальянский ученый Леон Альберти придумал шифровальный диск, состоящий из двух частей: внешней и внутренней. На неподвижном внешнем диске были расположены буквы алфавита и цифры. Внутренний подвижный диск также содержал буквы и цифры, но в другом порядке и служил ключом к шифру. Для шифрования нужно было найти букву текста на внешнем диске и заменить ее на букву с внутреннего диска, находящуюся под ней. После этого внутренний диск смещался, и новая буква шифровалась уже с новой позиции. Таким образом, шифр Альберти стал одним из первых многоалфавитных шифров, основанных на комбинаторном принципе. Кроме того, Леон Альберти написал одну из первых научных работ по криптографии - "Трактат о шифрах".



**Рисунок 2.** Шифровальный диск Леона Альберти.

Важно отметить стеганографию, на которую также обратил внимание Леон Альберти в своей работе. В отличие от шифров, стеганография не просто скрывает смысл информации, но и позволяет утаить сам факт передачи или хранения данных. Используя этот метод, текст можно спрятать под видом картинки, кулинарного рецепта, списка покупок или, например, кроссворда. Или вовсе сделать его невидимым, написав молоком, лимонным соком или специальными чернилами. Часто в одном сообщении использовались и методы стеганографии, и криптографии.

Прорывом в области криптографии стала книга «Полиграфия» аббата Иоганеса Тритемия, выпущенная в 1518 году. Эта книга рассказывала о различных шифрах, включая те, что использовали полиалфавитную замену. Следует упомянуть Блеза де Виженера, французского дипломата и алхимика XVI века, который считается одним из самых известных шифровальщиков своего времени. Он разработал устойчивый шифр, включающий 26 алфавитов, а порядок их использования зависел от знания пароля. Шифр Виженера можно охарактеризовать как комбинацию нескольких упомянутых ранее методов Цезаря.

**Эпоха шифровальных машин**

Промышленная революция также затронула область криптографии. В приближенные к 1790 году времена один из основателей США, Томас Джефферсон, разработал дисковый шифр, который позже был назван цилиндром Джефферсона. Этот устройство, использующее роторную систему, автоматизировало процесс шифрования и являлось первым криптографическим устройством Нового времени.

Изобретение телеграфа оказало значительное воздействие на область шифрования. Первоначальные методы шифрования стали устаревать, особенно в свете нарастающей потребности в надежном шифровании в период военных конфликтов XIX-XX веков. В этот период основной толчок для развития криптографии пришел именно из военной сферы. С 1854 года британские военные начали использовать шифр Плейфера, основанный на шифровании пар символов (биграмм). Этот метод шифрования был в употреблении до начала Второй мировой войны.

Во время Второй мировой войны противники начали применять передовые мобильные электромеханические шифраторы, чьи шифры казались нераскрываемыми. Эти устройства основывались на роторных или цевочных дисках. К роторным машинам относилась знаменитая «Энигма», используемая нацистами, а к цевочным – американская машина M-209.

Принцип работы «Энигмы» заключался в следующем: каждое нажатие клавиши с буквой вызывало движение одного или нескольких роторов. Буква заменялась несколько раз в соответствии с методом шифра Цезаря, и результат отображался в окошке. Шифры, созданные с использованием «Энигмы», считались очень надежными из-за огромного количества их возможных комбинаций, которое достигало 15 квадриллионов. Однако код «Энигмы» был расшифрован – сначала польскими криптографами в 1932 году, а затем британским ученым Аланом Тьюрингом, который создал специальное устройство для расшифровки сообщений «Энигмы» под названием «Бомба». Этот комплекс из 210 машин позволял англичанам расшифровывать до 3 тысяч военных сообщений нацистов в день и сыграл ключевую роль в победе союзников.

Мало было известно о советских шифровальных машинах из-за их строгой засекреченности до недавнего времени. Например, в СССР и союзных странах до 1990-х годов применялась роторная шифровальная машина «Фиалка». В отличие от «Энигмы» и других подобных устройств, в «Фиалке» было использовано 10 роторов, а вывод информации осуществлялся на бумажную ленту.

**Криптография для всех**

В 1949 году Клод Шеннон написал работу «Теория связи в секретных системах», что привело к тому, что криптография окончательно стала частью математики. К концу 1960-х годов роторные шифровальные системы были заменены более совершенными блочными, требующими использования цифровых электронных устройств. В 1967 году Дэвид Кан опубликовал популярную книгу «Взломщики кодов», что привлекло большой интерес к криптографии.

С распространением компьютеров криптография перешла на новый уровень. Мощности новых устройств позволили создавать намного более сложные шифры. Шифрование стало языком общения между компьютерами, а сама криптография стала важной отраслью. В 1978 году был разработан стандарт шифрования DES, который послужил основой для многих современных криптографических алгоритмов.

Сфера применения криптографии расширяется, и в это время власти разных стран пытаются сохранить контроль над использованием шифров. Разработки криптографов подвергаются секретности, производителей шифровальных устройств обязывают внедрять "задние двери" для доступа спецслужб.

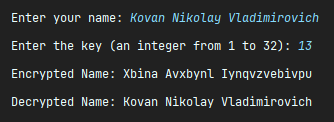
В то время как независимые криптоаналитики параллельно разрабатывали методы шифрования, доступные для всех – так называемую открытую криптографию, эта область стала особенно важной с распространением интернета. С внедрением сети возникла острая необходимость в защите конфиденциальности данных. Первым алгоритмом с открытым ключом стал RSA, разработанный в 1977 году, и названный по первым буквам фамилий его создателей – Риверста, Шамира и Адельмана. Американский программист Филипп Циммерман создал в 1991 году популярный пакет PGP с открытым исходным кодом для шифрования электронной почты.

С развитием доступного интернета по всему миру криптография стала неотъемлемой частью нашей повседневной жизни. С появлением мессенджеров, социальных сетей, онлайн-магазинов и государственных сайтов, передача персональной информации в сети происходит непрерывно и в огромных объемах. Каждый день мы сталкиваемся с криптографией, вводя пароли, отслеживая статусы покупок онлайн или совершая денежные транзакции через банковские приложения. Криптография прошла долгий путь от простых шифров древности к сложным криптосистемам. Будущее этой науки развивается перед нашими глазами – следующий виток в развитии шифрования наступит с появлением квантовых суперкомпьютеров, разработка которых уже активно ведется.

**Создание программы для зашифрования и расшифрования ФИО**

С помощью любого компилятора напиши создайте возможность зашифрования и расшифрования своих ФИО с с помощью шифра Цезаря и произвольным ключом 0 < n < 33.

#include <iostream>  
#include <string>  
  
std::string encrypt(*const* std::string& text, *int* n) {  
 std::string encrypted\_text = "";  
 *for* (*char* character : text) {  
 *if* (std::isalpha(character)) {  
 *int* shift = (std::isupper(character)) ? 65 : 97;  
 *char* encrypted\_char = *static\_cast*<*char*>((*static\_cast*<*int*>(character) - shift + n) % 26 + shift);  
 encrypted\_text += encrypted\_char;  
 } *else* {  
 encrypted\_text += character;  
 }  
 }  
 *return* encrypted\_text;  
}  
  
std::string decrypt(*const* std::string& encrypted\_text, *int* n) {  
 std::string decrypted\_text = "";  
 *for* (*char* character : encrypted\_text) {  
 *if* (std::isalpha(character)) {  
 *int* shift = (std::isupper(character)) ? 65 : 97;  
 *char* decrypted\_char = *static\_cast*<*char*>((*static\_cast*<*int*>(character) - shift - n + 26) % 26 + shift);  
 decrypted\_text += decrypted\_char;  
 } *else* {  
 decrypted\_text += character;  
 }  
 }  
 *return* decrypted\_text;  
}  
  
*int* main() {  
 std::string name;  
 *int* key;  
  
 std::cout << "Enter your name: ";  
 std::getline(std::cin, name);  
  
 std::cout << "Enter the key (an integer from 1 to 32): ";  
 std::cin >> key;  
  
 std::string encrypted\_name = encrypt(name, key);  
 std::cout << "Encrypted Name: " << encrypted\_name << std::endl;  
  
 std::string decrypted\_name = decrypt(encrypted\_name, key);  
 std::cout << "Decrypted Name: " << decrypted\_name << std::endl;  
  
 *return* 0;  
}



**Заключение**

В ходе данной работы были выполнены следующие задачи:

* Проведен анализ исторических источников для выявления первых примитивных методов криптографии;
* Исследовал и проанализировал классические методы шифрования, такие как шифр Цезаря, шифр Атбаш и др.;
* Выделил ключевые события в истории криптографии.

Таким образом, изучение истории криптографии подчеркивает важность этой науки в современном мире, где конфиденциальность и безопасность данных становятся все более критическими аспектами нашей цифровой жизни. Несмотря на ее древние корни, криптография продолжает развиваться и адаптироваться к новым вызовам, играя ключевую роль в обеспечении информационной безопасности и конфиденциальности в наше время.