УДК 003.26.09

ИСТОРИЯ КРИПТОГРАФИИ

Ушкова А. С., студент 2 курса факультета информационные системы и технологии
Научный руководитель – Горбоконенко В. Д., доцент
ФГБОУ ВО УлГТУ

Ключевые слова: *История, криптография, шифрование, тайнопись, шифр.*

Данная работа посвящена изучению истории криптографии. Были выявлены виды древних шифров и определено, как применяется криптография в наше время.

За понятием «криптография», что с древнегреческого означает «тайнопись», скрывается желание человека спрятать информацию от других людей. Сама письменность изначально была криптографической системой, так как принадлежала узкому кругу грамотных людей. С помощью нее они могли обмениваться знаниями, которые не были доступны неграмотным. С распространением письма возникла потребность в сложной системе шифрования. С древних времен криптография служила чиновникам, военным, купцам и хранителям религиозных знаний.

Первым шифром (около 4000 лет до н.э.) ученые считают древнеегипетский папирус времен правления фараона Аменемхета II. Неизвестный автор изменил знаменитые иероглифы, но, скорее всего, для сильного воздействия на читателя, а не для сокрытия информации.

Еще один известный древний шифр – это древнесемитский атбаш (где-то 600 г. до н.э.). Информацию скрывали простым способом: подменой букв алфавита. Такой вид шифра встречается в Библии.

В Древней Спарте использовали скиталу. Скитала – это цилиндр определенного диаметра, вокруг которого обматывали полоску пергамента. Текст писали на пергаменте в строку, после чего его разматывали, и сообщение становилось нечитаемым. Послание можно было прочитать только с помощью

цилиндра такого же диаметра. Спартанская скитала является первым криптографическим устройством.

В IV веке до н.э. автор военных трактатов Эней Тактик придумал шифровальный диск. Впоследствии устройство было названо его именем. Диск состоял из отверстий и написанных рядом букв. Для записи послания необходимо было последовательно продевать нить в отверстия. Чтобы прочитать текст, нужно было всего лишь вытянуть нить в обратном направлении. В этом и заключается минус этого устройства: разгадать шифр мог любой грамотный человек. Но зато уничтожить послание было очень легко. Для этого необходимо вытащить нить и разбить устройство.

Шифр Цезаря является первым задокументированным шифром (примерно 100 г. до н.э.). Его принцип был очень прост: каждая буква алфавита исходного текста заменялась на другую, отстоящую от нее по алфавиту на определенное число позиций. Разгадать данный шифр можно только зная данное число.

В Древней Руси тоже были свои способы тайнописи. Например, литорея, которая делилась на простую и мудрую. В простой версии шифра, ее еще называли тарабарская грамота, согласные буквы кириллицы располагались в два ряда. Зашифровывали послание, заменяя буквы одного ряда буквами другого. А в мудрой литорее буквы заменялись точками, палочками или кругами.

Цифирь так же является известным шифром Древней Руси. Здесь буквы, слоги и даже целые слова заменялись цифрами. Для усложнения в шифр добавлялись математические выражения. Такую загадку было не так просто разгадать.

Примерно в 1466 году итальянский ученый Леон Альберти изобретает шифровальный диск, состоящий из двух частей: внутренней и внешней. На внешнем неподвижном диске были написаны цифры и буквы. Внутренний подвижный диск тоже содержал буквы и цифры, но в другой последовательности и являлся ключом к разгадке. Для шифрования необходимо было найти нужную букву текста на верхней части и заменить ее на букву на внутренней, которая находится под ней. После внутренний диск смещается, и новая буква зашифровывается уже с новой позиции. Шифр

Альберти стал одним из первых шифров многоалфавитной замены, которые основаны на принципе комбинаторики.

Промышленная революция оказала большое влияние на криптографию. В 1790 году Томас Джефферсон создал дисковой шифр, названный в дальнейшем цилиндром Джефферсона. Это устройство основано на роторной системе. Оно позволило автоматизировать процесс шифрования и стало первым криптоустройством Нового времени.

Во Второй мировой войне противники использовали мобильные электромеханические шифраторы, шифры которых считались нераскрываемыми. Устройства были роторными или на цевочных дисках. К первым относилась знаменитая немецкая машина «Энигма», ко вторым – машина М-209, которой пользовались американцы.

«Энигма» работала следующим образом: при нажатии на клавишу с буквой в движение приходили один или несколько роторов. Буква заменялась несколько раз по принципу шифра Цезаря, и в окошке выдавался результат. Данные шифры считались самыми стойкими для взлома, так как количество их комбинаций достигало 15 квадриллионов. Однако шифр «Энигмы» все же был взломан, сначала польскими криптографами в 1932 году, а после английским ученым Аланом Тьюрингом, который создал специальную машину «Бомба» для расшифровки сообщений «Энигмы». Комплекс состоял из 210 таких машин и позволял расшифровать до 3 тыс. сообщений нацистов в сутки. Данное устройство внесло большой вклад в победу союзников.

О советских шифровальных машинах известно мало, так как до нашего времени информация о них была засекречена. Известно, что до 1990-х годов в СССР использовалась роторная шифровальная машина «Фиалка». В отличии от других устройств, в ней использовалось 10 роторов, а результат выводился на бумажную ленту.

С появлением компьютеров криптография выходит на новый уровень. Мощности новых устройств позволяют создавать более сложные шифры. Код или шифр становится языком общения между компьютерами, а криптография становится гражданской отраслью.

Распространение интернета невозможно представить без криптографии. С появлением социальных сетей, онлайн-магазинов и сайтов государственных услуг передача персональных данных происходит ежедневно

в огромных количествах. С шифрованием мы встречаемся постоянно: когда смотрим статус покупки, вводим пароль, или делаем денежный перевод. Криптография прошла огромный путь от простых шифров древности к сложным криптосистемам. Будущее этой науки творится на наших глазах. Очередная революция в шифровании произойдет с появлением квантовых суперкомпьютеров, разработка которых уже ведется.

Библиографический список:

1. Криптография: история шифровального дела [Электронный ресурс] // сайт «Ростех». – Режим доступа: https://rostec.ru/news/kriptografiya-istoriya-shifrovalnogo-dela/ (дата обращения 09.04.2021).

2. Как шифровали секретные письма на Руси [Электронный ресурс] // сайт «Кириллица». – Режим доступа: https://cyrillitsa.ru/history/51049-kak-shifrovali-sekretnye-pisma-na-rus.html (дата обращения 17.04.2021).

HISTORY OF CRYPTOGRAPHY

Ushkova A. S.

Key words: *History, cryptography, encryption, cipher.*

This work is devoted to the study of the history of cryptography. The types of ancient ciphers were identified and it was determined how cryptography is used in our time.