Мустафаева Нармин Имрановна,
студент III курса факультета дизайна,
Московский государственный университет технологий и управления
имени К.Г. Разумовского (Первый казачий университет)

Куприяненко Анастасия Алексеевна,
студент III курса факультета дизайна,
Московский государственный университет технологий и управления
имени К.Г. Разумовского (Первый казачий университет)

Научный руководитель:
Василенко Елена Владимировна, кандидат педагогических наук,
Московский государственный университет технологий и управления
имени К.Г. Разумовского (Первый казачий университет)

ИСТОРИЯ РАЗВИТИЯ КРИПТОГРАФИИ

Аннотация: в статье рассказывается об истории науки криптография, а также про ее влияние на жизнь современного человека.

Ключевые слова: криптография, шифрование, сцитала, литорея, шифр Цезаря, диск Энея, решетка Кардано, шифр Вижинера, Enigma, машина Тьюринга, DES, RSA, блокчейн.

Информация играет ключевую роль в развитии человечества. С древних времен она передавалась из поколения в поколение. Но со временем у людей возникла потребность передавать знания тайно. И теперь трудно представить нашу жизнь без безопасной передачи информации.

Криптография – это наука о том, как защитить информацию от посторонних лиц при соблюдении ряда принципов: конфиденциальность, сохранение целостности информации при ее передаче и подтверждение авторства. Ключевым методом криптографии является шифрование. В его основе – использование секретного ключа, чтобы зашифровать текст и скрыть ценные сведения. Как только человек понял, что может передавать свои мысли в виде графических символов, он начал искать способы делать это тайно. Так появились тайнопись и криптография. Условно историю можно поделить на три периода: домашинная, машинная и современная криптография. К домашинной криптографии можно отнести время, когда информация передавалась письменно. Самые древние ее следы встречаются еще в античности. Например, древние греки и спартанцы использовали шифр – сцитала. Его применяли со времен войны Спарты против Афин в V веке до н. э. Он состоит из цилиндра, вокруг которой обматывалась по спирали полоска пергамента с написанным сообщением. Получатель разматывал ленту и мог прочитать зашифрованное послание.

Похожий шифр был использован и в Древней Руси – литорея. Ее суть заключается в замене одних букв алфавита другими, поставив согласные буквы по порядку в 2 ряда. Самый древний документ, зашифрованный литореей, принадлежал митрополиту Киприану. Его переписка с Сергием Радонежским и Феодором Симоновским датируется 1229 годом.

Криптография развивалась также в Древнем Египте и Древнем Риме. Если египтяне использовали простейшие методы замены символов, то римляне шифровали текст. Например, шифр Цезаря – самый известный шифр античности. Согласно труду «Жизнь двенадцати цезарей», Цезарь вел секретную переписку, используя алфавит. Суть шифра в том, что каждая буква была смещена на три позиции вправо. То есть вместо A – D, B – E, C – F и т. д. Шифр Цезаря стал отсчетом для создания более сложных шифров.

Еще одним значимым изобретением в истории криптографии является диск Энея, диаметром около 15 см и с проделанными в нем отверстиями. Их количество равнялось числу букв в алфавите. Чтобы зашифровать послание, нужно поочерёдно протягивать свободный конец нити через отверстия, получая последовательность букв. Но получатель таким образом должен был прочитать сообщение наоборот. Это устройство стало прародителем других криптографических инструментов.

В эпоху Средних веков и Ренессанса шифрование сообщений стало предметом изучения и совершенствования для многих государств. Эпоха Возрождения стала временем не только всемирных открытий, но и великих тайн. Кто знал чужие секреты, тот вершил судьбы мира.

В 1550 году итальянский математик Джероламо Кардано опубликовал книгу «О тонкостях», в которой был описан способ шифрования. Сейчас мы называем называем это «решеткой Кардано». Решетка представляет собой лист твёрдого материала с вырезанными «окнами», которые могут быть повернуты на 90 градусов. При использовании всех окон, решетка поворачивается, и буквы открытого текста вписываются в окна повернутой решётки. Этот способ шифрования называется перестановкой.

После Ришелье усовершенствовал решётку Кардано, вырезав прямоугольник из плотного материала с окнами. Секретный текст вписывался в окна, затем решётка снималась, и оставшиеся клетки заполнялись, чтобы получить невинное сообщение.

Большинство исторических шифров, представленных в художественной литературе и кино, относятся к моноалфавитным шифрам. Их главной слабостью считается возможность взлома путем анализа частоты использования символов. Так в XVI веке появился шифр Виженера, который должен был решить эту проблему. Интересно, что название «шифр Виженера» появилось почти три столетия спустя, и французский дипломат Блез Виженер не имел отношения к его созданию. Он только порекомендовал Генриху III использовать этот шифр, благодаря чему он стал широко известен среди шифровальщиков. В XVII веке были выдвинуты главные требования к шифрам: они не должны поддаваться дешифрованию и возбуждать подозрений, а также требовать много времени для написания и чтения. Эти же требования сохраняются и сегодня.

Машинная криптография возникает в XIX веке с появлением телеграфа и последующим развитием электричества. Тогда криптография начала играть ключевую роль в военной, политической и коммерческой безопасности.

В этот период американец Эдвард Хеберн изобрел первую роторную машину. В криптографии роторная машина представляет собой устройство, в котором электрические схемы соединены с механическими частями печатной машины в целях шифрования и дешифрования сообщений. Это стало самым современным криптографическим оборудованием XX века. В 1918 году криптограф Артур Шербиус разработал легендарную роторную машину Enigma, которая стала мощным инструментом для немцев во время Второй мировой войны. Немецкий флот использовал ее для передачи секретных схем маршрутов. Несмотря на внешнюю простоту устройства, шифры долго оставались неразгаданными.

С появлением первых ЭВМ и всемирной сети Интернет, методы шифрования стали более сложными и конфиденциальными. В 1975 году бюро IBM разработали стандарт шифрования данных DES. Этот шифр был создан для применения в государственных учреждениях и быстро получил свое распространение. DES – это сложный блочный алгоритм, при выполнении шифрования которого текст переводится в двоичный код, при этом разбивается на отдельно зашифрованные блоки. Сегодня DES как один из самых распространенных алгоритмов, используется для коммерческой информации. Важным открытием в мире криптографии стала технология блокчейна. Это такая база данных, которая хранится на множестве компьютеров, но объединена единой сетью. Блокчейн состоит из

цепочки взаимосвязанных блоков, в каждом из которых хранится соответствующая информация. Каждый следующий блок содержит ссылку на предыдущий. Благодаря этому можно проследить историю изменения любой информации, которая содержится в блокчейне.

История криптографии – это история противостояния между защитой данных и попытками их прочесть. Вместе с развитием технологий криптографы стараются сделать шифрование всё более сложным и запутанным.

Список литературы:

1. Алгоритм шифрования DES URL: https://spravochnick.ru/informatika/algoritm_shifrovaniya_des/ (08.12.2023).
2. Литорея URL: https://ru.wikipedia.org/wiki/Литорея (21.11.2023).
3. Как взломали немецкий код Enigma во время Второй Мировой войны URL: https://www.iphones.ru/iNotes/vzlom-koda-enigma-kak-bomba-tyuringa-izmenila-hod-vtoroy-mirovoy-voyny-06-10-2019 (дата обращения: 16.07.2019)