УДК 004.056.5

ШИФРОВАНИЕ КАК СПОСОБ ЗАЩИТЫ КОРПОРАТИВНОЙ ИНФОРМАЦИИ

Чеченец В.А.

Учреждение образования «Белорусский государственный университет информатики и радиоэлектроники» филиал Минский радиотехнический колледж
г. Минск, Республика Беларусь

Научный руководитель: Назарова А.И. – преподаватель первой категории, магистр.

Аннотация. Защита корпоративной информации является неотъемлемой составляющей деятельности любой организации, ее утечка может привести к непоправимым последствиям. В статье рассматриваются методы шифрования, как один из способов защиты информации, и реализация программного средства, которое обеспечит возможность шифрования и дешифрования данных на основе использования определенных алгоритмов.

Ключевые слова: криптография, шифрование, дешифрование.

Введение. В современном мире проблема защиты информации вызывает большой интерес. Различные методы шифрования применяются не только для защиты информации от несанкционированного доступа, но и лежат в основе электронных информационных технологий электронного документооборота, электронного голосования и др.

Искусство и наука сокрытия сообщений для обеспечения секретности в информационной безопасности называется криптографией. Слово «криптография» было придумано путем объединения двух греческих слов: «крипто» означает скрытый и «графен» означает письменность.

Искусство криптографии считается рожденным вместе с искусством письма. По мере развития цивилизаций люди организовывали в племена, группы и царства. Это привело к появлению таких идей, как власть, сражения, превосходство и политика. Эти идеи еще больше подпитывали естественную потребность людей тайно общаться с избирательными получателями, что, в свою очередь, также обеспечивало непрерывную эволюцию криптографии.

Корни криптографии находятся в римской и египетской цивилизациях.

Самый древний текст с элементами критографии найден в гробнице древнеегипетского вельможи Хнумхотела II (рисунок 1), наследного князя и номарха города Менат-Хуфу, жившего почти 4000 лет назад. Где-то около 1900 г до н.э. писарь Хнумхотепа описывал жизнь своего господина в его гробнице. Среди иероглифов он использовал несколько необычных символов, которые скрывают прямое значение текста. Такой метод шифрования фактически представляет собой шифр подстановки, когда элементы исходного текста заменяются другими элементами по определённым правилам [1].

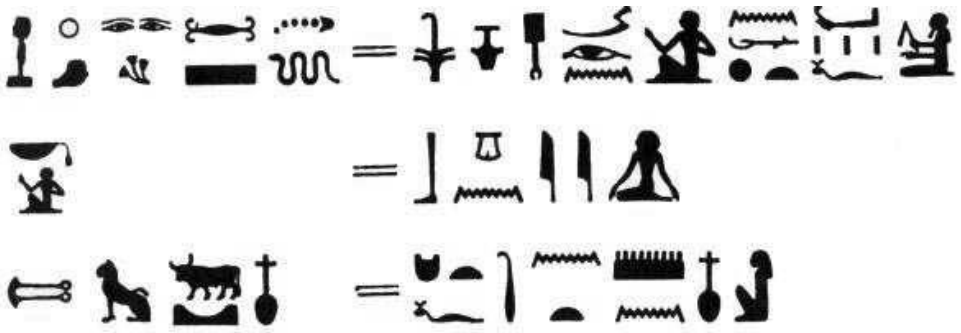

Рисунок 1 –Символы из гробницы Хнумхотепа II и их расшифровка

В современном мире защита информации является одной из наиболее актуальных проблем, а шифрование - одним из способов защиты информации.

Современная криптография решает следующие три основных проблемы:

- обеспечение конфиденциальности (секретности);
- обеспечение аутентификации информации и источника сообщений;
- обеспечение анонимности.

Традиционная криптографическая задача обеспечения секретности информации не утратила своей остроты и в настоящее время. Это связано, главным образом, с тем, что в эпоху массового применения компьютерных технологий задача защиты электронной информации приобрела характер насущной проблемы. При этом к алгоритмам шифрования предъявляются высокие требования как к скорости преобразований данных, так и к стойкости к аналитическим методам анализа. Для технологического применения криптографических средств характерно возрастание требований к шифрам одновременно по стойкости, скорости и простоте реализации.

На основании проведенного исследования, в рамках курсового проекта разрабатывается программное средство “Секрет фирмы”, которое будет обеспечивать возможность шифрования данных на основе применения шифра Виженера и шифра Цезаря. Для достижения данной цели были поставлены следующие задачи:

- изучение основных принципов шифрования и шифра Виженера, шифра Цезаря;
- обзор и изучение аналогов в сфере шифрования данных;
- разработка программного средства шифрования с использованием алгоритмов шифрования Виженера и Цезаря;
- тестирование и оценка эффективности программного средства;
- практическое применение программного средства в реальных условиях.

По результатам работы и применения программного средства возможно предложить варианты совершенствования существующих алгоритмов шифрования.

Основная часть. Шифрование является одним из самых надежных методов защиты информации, что безусловно важно в современном мире. На данный момент существуют уже тысячи всевозможных кодов и шифров для преобразования информации. В данной статье будут рассмотрены некоторые из них, распространенные и прошедшие испытание временем.

Шифр Цезаря – это классический метод шифрования. Шифр был назван так в честь Юлия Цезаря, который стал первым зафиксированным человеком, использовавшим метод сдвига букв на определенное количество позиций в алфавите для создания шифротекста. Гонцы с секретными военными сообщениями часто перехватывались неприятелем. Цезарь разработал шифр подстановки, в котором заменял одни буквы другими. Только тот, кто знал таблицу подстановки, мог расшифровать секретное сообщение. Теперь, даже если гонец попадёт в руки врага, шифровки не будут рассекречены. Это дало римлянам огромное преимущество в войне.

Шифр Виженера - это метод полиалфавитного шифрования, который использует несколько алфавитов, основанных на ключевом слове. Он был разработан Блезом де Виженером в 16 веке и является одним из самых известных и безопасных методов шифрования. Шифр Виженера построен на методе использования различных шифров Цезаря в различных частях сообщения.

Шифр Виженера был использован во многих исторических событиях, включая Первую мировую войну и Вторую мировую войну, и по-прежнему используется в настоящее время для защиты конфиденциальной информации.

Допустим, необходимо зашифровать слово «ТРАНЗАКЦИЯ», используя слово «ПУХ» в качестве ключа (рисунок 2). Для начала нам нужно сделать длину ключа эквивалентной длине слова для шифрования. Данный процесс представлен на рисунке 2.

Т	Р	А	Н	З	А	К	Ц	И	Я
П	У	Х	П	У	Х	П	У	Х	П

Рисунок 2 – Уравнение длины двух слов

Дальше для шифрования понадобится квадрат Виженера, который представлен на рисунке 3.

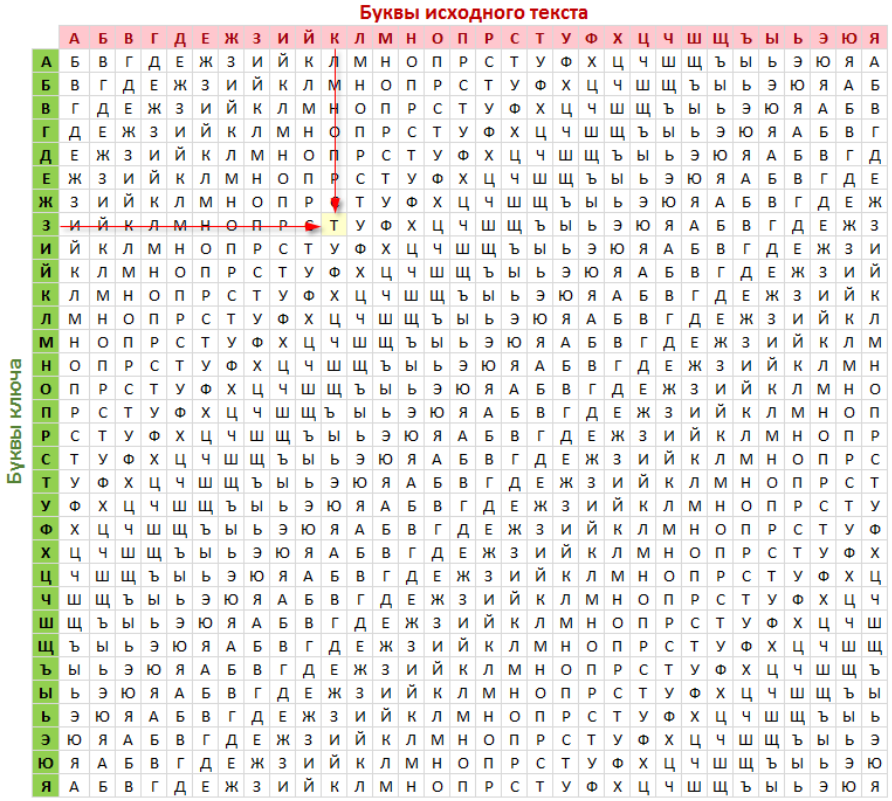

Рисунок 3 – Квадрат Виженера

Выбираются буквы на пересечении. Например, первая буква слова “Т”, буква под ней “П”, на их пересечении “В”. Соответственно, первая буква слова в зашифрованном виде – “В”.

Повторяя эти действия, получается результат, представленный на рисунке 4. Для дешифрования действия будут аналогичными.

Т	Р	А	Н	З	А	К	Ц	И	Я
П	У	Х	П	У	Х	П	У	Х	П
В	Д	Ц	Э	Ы	Ц	Ъ	К	Ю	П

Рисунок 4 – Слово, получившееся в результате сдвига

Во времена Первой мировой войны большой популярностью пользовался шифр Playfair. Его суть заключалась в том, что буквы латинского алфавита записывались в квадрат 5x5, после чего буквы исходного алфавита разбивались по парам. Далее, используя квадрат в качестве ключа, эти биграммы заменяли на другие по определенному алгоритму. Преимущество данного шифра было в том, что он не требовал дополнительных устройств, и, как правило, к тому моменту, когда сообщение расшифровывали, оно уже теряло актуальность. Еще одним способом тайнописи был шифратор Джефферсона.

В 1920 году голландский изобретатель Александр Кох изобрел первую роторную шифровальную машинку. Затем, на нее получили патент немецкие изобретатели, которые усовершенствовали ее и выпустили в производство, под названием «Enigma» (от греч. – загадка). Таким образом, эта машинка приобреталась многими фирмами, которые желали сохранить в тайне свои переписки. В этом и состояла вся гениальность Энигмы – все знали алгоритм шифрования, но никто не мог подобрать нужный ключ, так как число возможных комбинаций превосходило 15 квадриллионов [3].

Чтобы работать с Энигмой нужно для начала настроить машины на начальном положении, которое называется “ключ”. Далее нужно ввести сообщения для зашифровки на клавиатуре машины, повернуть роторы шифрующего механизма на определенное количество шагов, используя установленный ключ. Когда сообщение проходит через роторы, машина меняет его по пути, используя сложные математические алгоритмы.

Метод шифрования ROT1 очень прост. Каждая буква шифра заменяется на следующую за ней в алфавите [4].

Шифр Гронсфельда – это модификация шифра Цезаря. Данный способ является значительно более стойким к взлому и заключается в том, что каждый символ кодируемой информации шифруется при помощи одного из разных алфавитов, которые циклически повторяются. Можно сказать, что это многомерное применение простейшего шифра замены.

Принцип метода шифрования публичным ключом состоит в наличии двух ключей, один из которых передается публично, а второй является секретным (приватным). Открытый ключ используется для шифровки сообщения, а секретный – для дешифровки. В роли открытого ключа чаще всего выступает очень большое число, у которого существует только два делителя, не считая единицы и самого числа. Вместе эти два делителя образуют секретный ключ. Процесс шифрования данным методом представлен на рисунке 5.

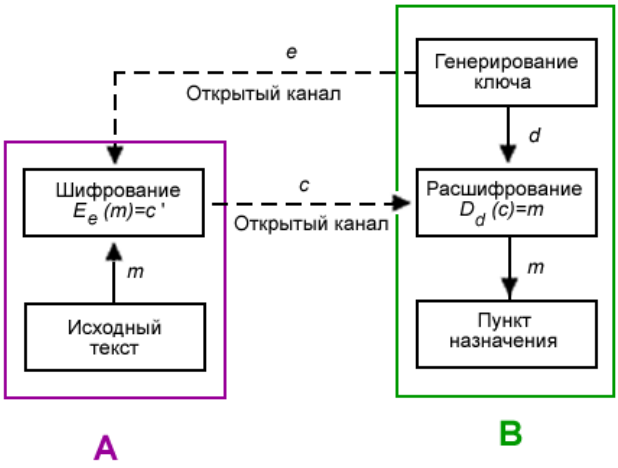

Рисунок 5 – Шифрование публичным ключом

Защита корпоративной информации является одним из важных аспектов бизнеса. Корпоративная информация может включать в себя такие данные, как финансовые отчеты, планы развития, интеллектуальную собственность, клиентскую базу и многое другое. Утечка корпоративной информации может происходить при использовании электронных писем, при копировании файлов сотрудниками и при несанкционированных внедрениях злоумышленников в систему. Этого можно избежать при помощи шифрования данных.

Рассмотрим преимущества и недостатки применения методов шифрования данных в компаниях. К числу преимуществ можно отнести следующие [1]:

– охрана базы данных от несанкционированного доступа;

– защита информации от копирования и обнародования;

– повышение уровня корпоративной этики за счет обеспечения безопасности обмена личными сообщениями;

– аутентификация – криптографические методы, такие как MAC и цифровые подписи, могут защитить информацию от подделки.

В числе недостатков можно выделить следующие:

– высокая стоимость с точки зрения времени и денег;

– сложно зашифрованная, аутентичная и имеющая цифровую подпись информация может быть труднодоступной даже для законного пользователя;

– избирательное управление доступом;

– криптография не может полностью защитить от уязвимостей и угроз, возникающий из-за плохого проектирования систем, протоколов и процедур.

В рамках курсового проекта разрабатывается программное средство «Секрет фирмы» предназначенное для защиты данных компании путем шифрования на основе использования алгоритмов Цезаря и Виженера. Данные методы шифрования широко известны, а также позволяют получить базовые понятия о принципах работы криптографии. Оба метода используются для замены символов в исходном тексте на другие символы из алфавита, что делает исходный текст невозможным для прочтения без специального ключа. Однако, необходимо учитывать, что защита текста от расшифровки может быть нарушена при использовании простых ключей.

Заключение. За века своего существования человечество придумало множество способов хранения тайн. Развитие криптографии и криптоанализа неразрывно связано с очень высоким уровнем развития вычислительной техники.

Принимая во внимание эти факты, современная криптография будет вынуждена искать более сложные в вычислительном отношении проблемы или разрабатывать совершенно новые методы архивирования целей, которые в настоящее время используются современной криптографией.

Современные компании все чаще прибегают к профессиональной помощи специалистов по безопасности. Специалист строит и внедряет систему защиты в ИТ-инфраструктуру компании или организации, предотвращает и блокирует попытки проникнуть в нее извне.

Список литературы

1. *Криптография и защищенная связь: история первых шифров // Habr [Электронный ресурс]. – 2017. Режим доступа: https://habr.com/ru/post/321338/ – Дата доступа: 21.03.2023*

2. *Преимущества и недостатки криптографии // CoderLessons [Электронный ресурс]. – 2018. Режим доступа: https://coderlessons.com/tutorials/akademicheskii/izuchite-kriptografiiu/preimushchestva-i-nedostatki-kriptografii – Дата доступа: 20.03.2023*

3. *Алгоритм Энигмы // Habr [Электронный ресурс]. – 2014. Режим доступа: https://habr.com/ru/post/217331/ – Дата доступа: 22.03.2023*

4. *Популярные коды и шифры // IT-BLACK [Электронный ресурс]. – 2019. Режим доступа: https://it-black.ru/populjarnye-kody-i-shifry/ – Дата доступа: 23.03.2023*

UDC 004.056.5

ENCRYPTION AS A WAY TO PROTECT CORPORATE INFORMATION

Chechenech V.A.

Educational institution "Belarusian State University of Informatics and Radioelectronics"
branch "Minsk Radio Engineering College", Minsk, Republic of Belarus

Scientific supervisor: Nazarova A.I. – teacher of the first category, master.

Annotation. Protection corporate information is the significant part of business. Information leak leads to irreparable consequences. There are methods of encryption as the way to protect information and realization software that provides opportunity of encryption and decryption data based on the use of certain algorithms in the article.

Keywords: cryptography, encryption, decryption.