УДК 004.056.55 **Информационные технологии**

Гузнова Анастасия Дмитриевна, *студентка ФДП и СПО ФГБОУ ВО «Мордовский государственный университет им. Н. П. Огарёва», г. Саранск*
Прокин Александр Александрович, *преподаватель, ФГБОУ ВО «Мордовский государственный университет им. Н. П. Огарёва», г. Саранск*
Венчаков Павел Вячеславович, *преподаватель, ФГБОУ ВО «Мордовский государственный университет им. Н. П. Огарёва», г. Саранск*
e-mail: pvenchakov96@yandex.ru

РАЗРАБОТКА МЕТОДА ШИФРОВАНИЯ ДАННЫХ ДЛЯ ОБЕСПЕЧЕНИЯ ИХ СОХРАННОСТИ

Аннотация: В статье рассказывается о существующих видах и методах шифрования данных. Разработан и описан авторский метод шифрования. Проведено сравнение с существующими методами.

Ключевые слова: HTTPS, протокол, сервер, шифрование, метод, алгоритм, блок-схема.

Annotation: The article describes periodic types and methods of data encryption. The author's blocking method has been developed and described. A comparison with existing methods is made.

Key words: HTTPS, protocol, server, encryption, method, algorithm, block diagram.

В эпоху цифровизации прогресс не стоит на месте, и как следствие, мошенники придумывают более развитые способы вторжения в личную жизнь людей, сбор информации о них. В основном это происходит с целью заработать. Особенно часто они взламывают аккаунты и сервера в интернете, где хранятся личные данные.

Разработчики антивирусного обеспечения ESET установили, что каждый второй пользователь социальных сетей хотя бы раз взламывался, происходила утечка персональных данных и шантаж. Реже встречаются случаи кражи денег с банковских карт. Это связано с тем, что на очень многих сервисах онлайн покупок люди оставляют данные своих карт. Например, 41% опрошенных дают приложениям доступ к геолокации, а 35% – используют основную банковскую карту для покупок в интернете. Треть пользователей позволяют сторонним сайтам и социальным сетям собирать их данные. Встречаются пользователи, которые публикуют фотографии документов или билетов, чеков, пересылают пароли или документы. Если эти данные попадут в руки недоброжелателей, то могут появиться тяжело исправимые последствия. Чтобы не происходила утечка информации необходимо шифровать данные в момент передачи данных между сервером и приложением, а также хранящуюся информацию на сервере [1].

Описываемые проблемы справедливы также для разрабатываемых приложений на смартфон, например, для доставки воды. В мобильном приложении будет страница личного кабинета клиента с данными: почта, номер телефона, адрес проживания, пароль от личного кабинета. Чтобы приложение было безопасным, необходимо шифровать данные на сервере, который будет прикреплен к приложению и данные в момент передачи. Рассмотрим виды и методы шифрования.

Шифрование (от франц. «chiffre –шифр») – ведение секретных записей, сообщений при помощи шифра – условных знаков, букв и цифр. Наука, разрабатывающая математическую теорию и практику шифрования, называется криптографией [2].

Существуют такие виды шифрования как:

− Перестановка – символы текста переставляются по правилу, разработанному в пределах небольшой части этого текста. При сложном алгоритме перестановки можно очень надёжно зашифровать данные;

− Замена (подстановка) – символы текста заменяются буквами алфавита с

определенным сдвигом или того же самого текста;

− Гаммирование – символы текста складываются с символами случайной последовательности. Шифрование этого вида будет более стойким, если длина неповторяющейся части будет как можно больше;

− Шифрование аналитическими преобразованиями – символы текста преобразуются по готовой формуле из математики.

Существует два основных метода шифрования: симметричный и асимметричный.

При симметричных методах шифрования и расшифрования используется один и тот же секретный ключ. Данные передаются и зашифровываются быстро и просто, но ключ должен быть известен отправителю и покупателю, что осложняет процесс распределения ключей. При симметричных алгоритмах не требуются большая скорость интернета и большая мощность компьютера.

Примером такого метода может быть алгоритм Triple DES. При таком алгоритме создается ключ длинной 112 бит. Здесь происходит трехкратное шифрование с двумя ключами.

Существует алгоритм шифрования IDEA, который более безопасный, чем предыдущий алгоритм. В нем используют ключ длинной 128 бит, а внутренняя структура более устойчива к криптоанализу.

При асимметричных методах для шифрования используется уже два ключа: первый ключ – открытый, он используется для шифровки; второй – закрытый, для расшифровки. Тот, кто владеет закрытым ключом – знает и открытый, и его передает тому, кто будет шифровать данные. Недостатком такого метода является то, что ключи могут создаваться очень медленно.

На данный момент RSA считается самым надежным асимметричным методом шифрования. Для шифрования текста используются математические вычисления, которые трудно восстановить, не зная последовательности.

Также очень известен сейчас алгоритм Эль Гамаля. Шифрование происходит по возведению в степень по модулю большого простого числа. Чем больше число, тем более надежная будет система шифрования.

Существует ряд требований для криптографической защиты информации:

- простота процедур шифрования и расшифрования;
- незначительная избыточность кода;
- надежность шифрования данных.

Чтобы была возможность передавать данные между приложениями и сервером существует протокол HTTP. Приложение формирует запрос и отправляет его на сервер. В момент передачи информации как раз и работает протокол HTTP. С помощью него происходит обработка запроса, т.е. определяется, куда надо отослать информацию и что вернуть обратно, формирование ответа, отправка необходимых данных обратно. Чтобы информация при передаче была защищена, используется протокол HTTPS. Это слияние протоколов HTTP и SSL или HTTP и TLS. TLS и SSL – криптографические протоколы. Сайту выдается SSL/TLS-сертификат, который подтверждает, что соединение защищено. Данные перед отправкой шифруются, а на сервере расшифровываются [3]. TLS использует алгоритм симметричного шифрования AES, который формирует ключи длинной 128, 192 или 256 бит (чем длиннее ключ, тем больше защищенность). С помощью AES шифруются различные интернет-файлы, Wi-Fi, VPN, мобильные приложения. Также TLS может использовать гибридное шифрование [4].

TLS и SSL используют асимметричное шифрование для аутентификации, регистрации, а симметричное шифрование для конфиденциальности.

Авторами предлагается следующий метод шифрования:

Есть два ключа. Первый состоит из определённого количества чисел. Второй состоит из определенного количества математических знаков + и * (плюс и умножить). Ключи по размеру должны совпадать.

Принцип шифрования: берём первую букву из слова, определяем ее порядковый номер и берём это число. Берём первую цифру из первого ключа. И берём первый знак из второго ключа. Складываем или умножаем числа, в зависимости от математического знака. Получившееся число – новый номер буквы из алфавита. Таким образом, получаем новую букву. Алгоритм показан в

виде блок-схемы на рисунке 1. По аналогии шифруем все остальные буквы. Регистр букв не имеет значения, знаки препинания и пробелы остаются такими как были.

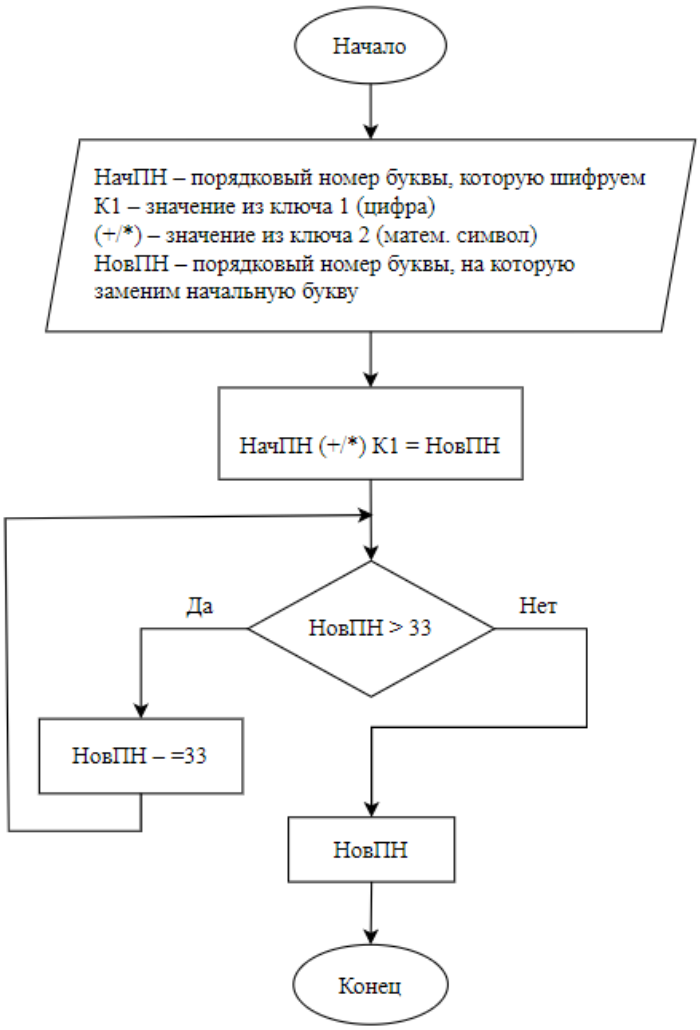

Рисунок 1 – Блок-схема принципа шифрования

Если произведение или сумма получается двузначным числом, которое больше 33, то мы вычитаем из него 33 до тех пор, пока число не станет меньше 33. Таким образом получаем порядковый номер. Если число трехзначное, то так же вычитаем 33, пока число не станет меньше 33.

Пример шифрования:

Зашифруем слово: АЛФАВИТ

Ключ 1: 768954036784 Ключ 2(секретный): +*++**+*+++*

1. Первая буква в слове А – она первая в алфавите, получается порядковый номер 1

Берем в ключе1 (далее К1) первую цифру – 7, в ключе2 (далее К2) первый символ – +

Складываем 1+7 = 8

Получается буква А превратится в восьмую букву алфавита: Ж

2. Вторая буква Л – порядковый номер 13

К1 – 6 К2 – *

Умножаем 13*6 = 78

78 > 32

Вычитаем: 78 - 33 = 45

45 - 33 = 12

Получается снова буква К

3. Ф – 22, К1 – 8, К2 – +, 22 + 8 = 30, Получается Э

4. И т.д. (первые 3 буквы зашифровались как ЖКЭ…)

Когда закончатся оба ключа, а фраза еще не закончилась, берем данные с начала ключа.

С помощью этого алгоритма можно шифровать и цифры. Например:

Зашифруем число 22. Ключи будем использовать те, что написаны в примере выше.

Шифруем – 22. Из ключа1 и ключа2 возьмем первые символы: К1 – 7, К2 – +. Складываем 22 и 7, получаем 29. Таким образом, мы зашифруем число 22 числом 29.

Разработанный метод относится к симметричным методам шифрования с заменой. Его можно использовать в разрабатываемом приложении, о котором говорилось ранее, а также в подобных архитектурах и моделях «клиент-сервер».

Описанные выше алгоритмы, безусловно, надежные, они проверены временем, их тяжело взломать, они сейчас активно используются и справляются со своим назначением. Если рассматривать асимметричные методы, то они все работают недостаточно быстро. Предложенный алгоритм имеет легкий принцип работы, также устойчивость к атакам, но присутствует

много операций, два ключа, что делает его медленным. Описанный метод будет дорабатываться, усовершенствоваться в процессе написания приложения и тестирования.

Библиографический список:

1 ТАСС: исследование: каждого второго пользователя хоть раз взламывали в социальных сетях: сайт. – URL: https://tass-ru.turbopages.org/tass.ru/s/obschestvo/11006151 (дата обращения: 30.01.2023). – Режим доступа: свободный. – Текст: электронный.

2 Райзберг Б. А. Современный экономический словарь / Райзберг Б. А., Лозовский Л. Ш., Стародубцева Е. Б. – 2-е изд., испр. М.: ИНФРА-М, 1999. – 479 с. – Текст: электронный.

3 Skillbox: Что такое HTTP и зачем он нужен: сайт. – URL: https://skillbox.ru/media/code/chto-takoe-http-i-zachem-on-nuzhen/ (дата обращения: 04.01.2023). – Режим доступа: свободный. – Текст: электронный.

4 Skillbox: как интернет защищает информацию: сайт. – URL: https://skillbox.ru/media/code/kak-internet-zashchishchaet-informatsiyu-i-pochemu-etu-zashchitu-skoro-razrushat-kvantovye-kompyuter/ (дата обращения: 10.01.2023). – Режим доступа: свободный. – Текст: электронный.