Оценка защищенности информации при передаче данных между субъектами доступа в клиент-серверной архитектуре

О.В. Куликова[1], *Е.В. Пиневич*[1], *Г.С. Домбаян*[1], *Н.В. Егоров*[1], *А.С. Волохов*[2]

[1] *Донской государственный технический университет, Ростов-на-Дону*
[2]*Ростовский государственный университет путей сообщения*

Аннотация: В статье рассматривается оценка защищенности конфиденциальной информации при передаче данных между пользователями в клиент-серверной архитектуре. В результате работы был разработан алгоритм и реализовано программное средство, которое позволяет обеспечить конфиденциальность информации при взаимодействии между субъектами доступа. Проведено исследование зависимости выбранных параметров эллиптической кривой от времени обработки и передачи шифрованного сообщения. Исследования показали, что с увеличением значений параметров эллиптической кривой увеличивается время обработки конфиденциальной информации в силу недостаточности ресурсов системы.
Ключевые слова: конфиденциальная информация, утечка информации, ассиметричное шифрование, надежность информации, ресурсы системы, канал связи.

Введение

На сегодняшний день, помимо компьютерной безопасности [1], ключевую роль при обеспечении защищенности данных в процессе взаимодействия между несколькими субъектами доступа играет сокрытие содержимого сообщения [2, 3].

Перед компаниями, которые занимаются разработкой подобного рода приложений, преимущественно ставится задача выбора оптимального способа, позволяющего качественно и надежно обеспечить конфиденциальность переписки между пользователями [4].

В руководящих документах [5], принятых Федеральной службой по техническому и экспортному контролю, описаны методы, с использованием которых велика вероятность защиты обрабатываемой информации. Однако, с увеличением вычислительной мощности персональных компьютеров, у злоумышленников возрастает возможность перехвата данных. Следовательно, представляется актуальной разработка оптимального клиент-

серверного приложения, способного обеспечить защищенность информации при взаимодействии между субъектами доступа в соответствии с требованиями по безопасности информации.

1. Алгоритм оценки защищенности данных при передаче по каналу связи между пользователями

Для сокрытия содержимого сообщения используются криптографические методы защиты информации [6], представленные на рисунке 1.

Следует отметить, что ассиметричный алгоритм шифрования является достаточно надежным и устойчивым от различных криптоатак [7] со стороны внешних нарушителей. Однако, скорость шифрования данных низкая в сравнении с симметричным алгоритмом [8].

Важно заметить, что для качественного обеспечения защиты информации стоит использовать ассиметричный метод. Следовательно, в дальнейшем, будем рассматривать криптографический алгоритм шифрования, основанный на эллиптических кривых.

Рис. 1. – Криптографические методы защиты информации

На рисунке 2 продемонстрирована структурная схема контроллера, в которой пошагово описана специфика его работы.

Алгоритм работы контроллера следующий:

– независимо от существования подключенных ранее субъектов доступа, проверяется каждые 30 секунд наличие в очереди новых пользователей;

– при появлении нового пользователя, контроллер добавляет в таблицу маршрутизации значение ip и ожидает следующих соединений [9];

– если количество подключений становится кратным 2, то, по параметрам эллиптической кривой, формируется множество точек;

– выбирается, случайным образом, точка эллиптической кривой;

– по теореме Хассе [10], определяется порядок точки кривой таким образом, чтобы гарантировать пользователям вычисление публичного ключа, полагаясь на то, что полученная в результате точка принадлежит множеству точек кривой [11];

– контроллер, в порядке очереди, выдает пару значений: (P, N).

Опишем алгоритмическое конструирование взаимодействия субъектов доступа, как показано на рисунке 3.

На начальном этапе пользователь отправляет запрос контроллеру для возможности обмениваться данными. Следует отметить, что рассматриваемый процесс является скрытым. Также важно заметить, что на протяжении 30 секунд проверяется наличие пользователей, с которым планируется дальнейшее взаимодействие.

После того, как появляется в сети субъект доступа, которому необходимо скрытно передать конфиденциальную информацию, формируется пара ключей, основанные на ассиметричном алгоритме шифрования Эль – Гамаля [12] затем формируется публичный ключ и производится обмен данными между пользователями.

Рис. 2. – Структурная схема контроллера

Рис. 3. – Структурная схема взаимодействия субъектов доступа

2. Исследование оценки выбранных параметров эллиптической кривой от времени обработки информации

Для оценки скорости обработки данных вносились изменения, касающиеся выбранных параметров эллиптической кривой.

В рамках каждого эксперимента для улучшения наглядности результатов некоторые параметры эллиптической кривой будут постоянными. На рисунке 4 приведен график зависимости фиксированных значений параметров «a» и «b», при некотором изменении значений «p».

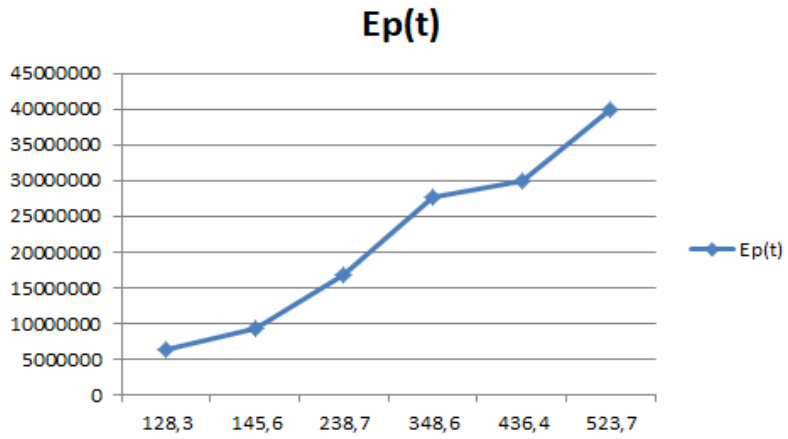

Рис. 4. – График зависимости изменения «p» от времени обработки информации

Можно сделать вывод о том, что при увеличении значения поля также увеличивается время для обработки информации. Это время включает в себя: процессы генерирования точек эллиптической кривой; формирование пар значений (общая точка, порядок точки); генерирование ключей шифрования.

Далее исследование проводилось с внесением изменений параметра «a» при условии, что параметры «b» и «p» будут фиксированными. Результаты эксперимента представлены на рисунке 5. Следует отметить, что при увеличении параметра «a», время, которое затрачивается на сокрытие данных от нарушителей, также увеличивается.

Аналогичные исследования проводились и с внесением изменений параметра «b». Результаты эксперимента представлены на рисунке 6. Важно

отметить, что при увеличении параметра «b», время, которое затрачивается на сокрытие данных от нарушителей, также увеличивается.

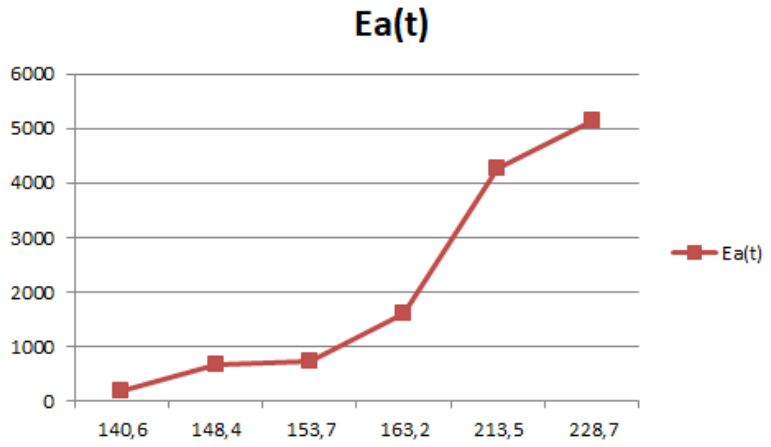

Рис. 5. – График зависимости изменения параметра «a» от времени обработки информации

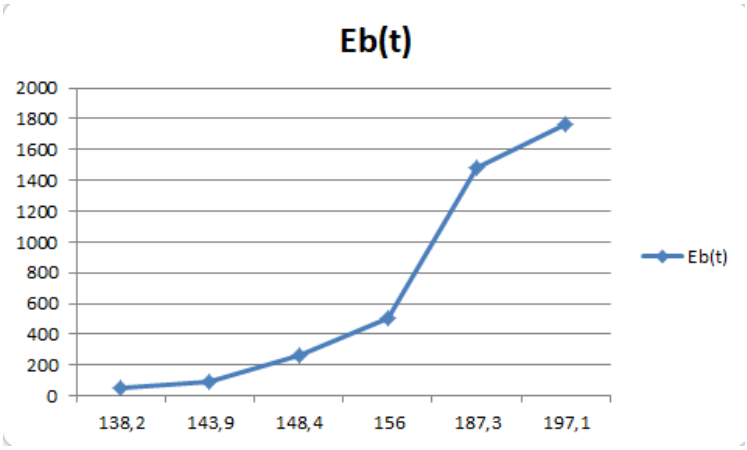

Рис. 6. – График зависимости изменения параметра «b» от времени обработки информации

Заключение

Таким образом, в результате работы разработан алгоритм обеспечения защищенности информации при передаче данных между субъектами доступа в клиент-серверной архитектуре. Также проведено исследование зависимостей при изменении параметров эллиптической кривой от времени

обработки информации, которое демонстрирует поведение работы разработанного программного средства.

Литература

1. Ганжур М.А., Ганжур А.П., Борисенко И.М. Обеспечение компьютерной безопасности с использованием метода «безопасность через неясность» // Инженерный вестник Дона, 2019, №1. URL: ivdon.ru/ru/magazine/archive/n1y2019/5755 (дата обращения 15.11.2020 г.).

2. Маро Е.А. Алгебраический анализ стойкости криптографических систем защиты информации// Инженерный вестник Дона, 2013, №4. URL: ivdon.ru/ru/magazine/archive/n4y2013/1996 (дата обращения 15.11.2020 г.).

3. Баранова Е.К., Бабан А.В. Информационная безопасность и защита информации: Учебное пособие / Москва: изд-во РИОР, 2018. 336 с.

4. Шаньгин В.Ф., Соколов А.В. Защита информации в распределенных корпоративных сетях и системах. ДМК, 2002, серия "Администрирование и защита", 656 с.

5. Методика определения угроз безопасности информации в информационных системах. – // Методический документ ФСТЭК России. – 2015. – URL: mindstep.ru/ wiki/index.php/Методика_определения_угроз_безопасности_информации_в_информационных_системах (дата обращения 26.11.2020 г.).

6. Венбо, Мао Современная криптография: теория и практика: пер. с англ, Москва: Издательский дом «Вильямс», 2015. 768 с.

7. Саломаа А. Криптография с открытым ключом. Москва: Мир, 1995. 318 с.

8. Панасенко С.П. Алгоритмы шифрования. Специальный справочник. БХВ-Петербург, 2009. 576 с.

9. Жданов О. Н. Чалкин В.А. Эллиптические кривые. Основы теории и криптографические приложения – СГАУ им. М. Ф. Решетникова. – Москва: URSS ЛИБРОКОМ, 2012. 193 с.

10. Washington, Lawrence C. Elliptic Curves. Number Theory and Cryptography, 2nd Ed, Discrete Mathematics and its Applications, Boca Raton: Chapman & Hall/CRC Press. 2008. P.536.

11. Болотов А. А., Гашков С. Б., Фролов А. Б., Часовских А. А. Элементарное введение в эллиптическую криптографию. Алгебраические и алгоритмические основы, Москва: Учебное пособие, 2019. 376 с.

12. Elgamal T. A Public-Key Cryptosystem and a Signature Scheme Based on Discrete Logarithms // IEEE Trans. Inf. Theory /F.Kschischang — IEEE, 1985, Vol. 31, Iss. 4. Pp. 469 -472.

References

1. Ganzhur M.A., Ganzhur A.P., Borisenko I.M. Inzhenernyj vestnik Dona 2019, №1. URL: ivdon.ru/ru/magazine/archive/n1y2019/5755 (data obrashhenija 15.11.2020 g.).

2. Maro E.A. Inzhenernyj vestnik Dona 2013, №4. URL: ivdon.ru/ru/magazine/archive/n4y2013/1996 (data obrashhenija 15.11.2020 g.).

3. Baranova E.K., Baban A.V. Informacionnaja bezopasnost' i zashhita informacii: Uchebnoe posobie [Information Security and Information Protection: A Study Guide], Moskva: izd-vo RIOR, 2018. P. 336.

4. Shan'gin V.F., Sokolov A.V. Zashhita informacii v raspredelennyh korporativnyh setjah i sistemah [Information protection in distributed corporate networks and systems]. DMK, 2002, cerija "Administrirovanie i zashhita", P. 656.

5. Metodika opredelenija ugroz bezopasnosti informacii v informacionnyh sistemah. [Methodology for determining threats to information security in information systems]. Jelektronnyj Metodicheskij dokument FSTJeK Rossii,

2015. URL: mindstep.ru/wiki/index.php/Metodika_opredelenija_ugroz_bezopasnosti_informacii_v_informacionnyh_sistemah (data obrashhenija 26.11.2020 g.).

6. Venbo, Mao Sovremennaja kriptografija: teorija i praktika: Per. s angl. [Modern cryptography: theory and practice], Moskva: Izdatel'skij dom «Vil'jams», 2015.P. 768.

7. Salomaa A. Kriptografija s otkrytym kljuchom [Public key cryptography]. Moskva: Mir, 1995. P. 318.

8. Panasenko S.P. Algoritmy shifrovanija. Special'nyj spravochnik [Encryption algorithms. Special reference]. BHV-Peterburg, 2009. P. 576.

9. Zhdanov, O. N. Jellipticheskie krivye. Osnovy teorii i kriptograficheskie prilozhenija [Elliptic curves. Fundamentals of Theory and Cryptographic Applications], SGAU im. M. F. Reshetnikova, Moskva: URSS LIBROKOM, 2012. P. 193.

10. Washington, Lawrence C. Elliptic Curves. Number Theory and Cryptography, 2nd Ed, Discrete Mathematics and its Applications, Boca Raton: Chapman & Hall, CRC Press. 2008. P. 536.

11. Bolotov A. A., Gashkov S. B., Frolov A. B., Chasovskih A. A. Jelementarnoe vvedenie v jellipticheskuju kriptografiju. Algebraicheskie i algoritmicheskie osnovy [An elementary introduction to elliptic cryptography. Algebraic and algorithmic foundations], Moskva: Uchebnoe posobie, 2019. P. 376.

12. Elgamal T. A Public-Key Cryptosystem and a Signature Scheme Based on Discrete Logarithms (angl.) IEEE, 1985, Vol. 31, Iss. 4. Pp. 469 -472.