Анализ современных алгоритмов шифрования данных

А.Д. Москвин, Л.Э. Петросян

Московский государственный университет технологий и управления им. К.Г. Разумовского (Первый казачий университет)

Аннотация: Статья посвящена анализу современных алгоритмов шифрования данных. Введение дает обзор наиболее распространенных алгоритмов шифрования, такие как AES, RSA и SHA. Основная часть статьи включает в себя анализ уязвимостей современных алгоритмов шифрования и рассматривает различные методы атак. В заключение делаются выводы о том, что необходимо использовать комплексные методы защиты данных и периодически обновлять используемые алгоритмы шифрования для предотвращения возможных атак.
Ключевые слова: алгоритм шифрования, безопасность данных, уязвимость, метод атаки, комплексный метод, защита данных.

Шифрование данных – это процесс преобразования исходных данных в зашифрованный вид, который не может быть прочитан без специального ключа. Существует множество алгоритмов шифрования, но не все они обеспечивают достаточную безопасность для защиты конфиденциальной информации.

Среди наиболее распространенных алгоритмов шифрования можно выделить AES, RSA и SHA [1,2]. AES (Advanced Encryption Standard) – это симметричный алгоритм блочного шифрования, используемый для защиты конфиденциальности данных [2]. AES использует блочное шифрование, то есть, он шифрует данные блоками фиксированного размера (обычно 128 бит). RSA (Rivest-Shamir-Adleman) – это асимметричный алгоритм шифрования, используемый для защиты целостности данных и аутентификации. В этом алгоритме для шифрования данных используются математические преобразования [2,3]. SHA (Secure Hash Algorithm) – это криптографическая хеш-функция, которая преобразует входные данные произвольной длины в фиксированный хеш-код фиксированной длины [3,4]. Хеш-функция SHA является односторонней функцией, что означает, что вычисление обратного хеш-кода для заданного хеш-кода является

© Электронный научный журнал «Инженерный вестник Дона», 2007–2023

практически невозможным. Хеш-функцию SHA чаще всего используют для обеспечения целостности данных.

Однако даже эти алгоритмы не являются абсолютно безопасными. Некоторые уязвимости могут быть использованы для атаки на данные, зашифрованные с использованием этих алгоритмов [5].

Так, для расшифровки информации, зашифрованной алгоритмом AES, возможно использовать атаки следующих видов:

Таблица 1

Виды атак для алгоритма AES

№	Название атаки	Описание
1	2	3
1	Метод грубой силы	это метод атаки, при котором злоумышленник перебирает все возможные ключи шифрования, пока не найдет тот, который даст правильный результат дешифровки. Такая атака может быть очень медленной, если длина ключа шифрования достаточно большая, но может быть эффективной, если ключ короткий.

© Электронный научный журнал «Инженерный вестник Дона», 2007–2023

1	2	3
2	Метод анализа времени выполнения	это метод, который использует информацию о времени выполнения шифрования для вычисления ключа шифрования. Такой метод атаки может быть эффективным, если злоумышленник имеет доступ к компьютеру, на котором происходит шифрование.
3	Метод словаря	это метод атаки, при котором злоумышленник использует предварительно подготовленный словарь паролей или ключей для перебора ключа шифрования. Если ключ шифрования является словом или фразой из словаря, то такая атака может быть эффективной.

© Электронный научный журнал «Инженерный вестник Дона», 2007–2023

1	2	3
4	Метод линейного криптоанализа	это метод атаки, при котором злоумышленник использует статистические анализы, чтобы найти зависимости между входными данными, выходными данными и ключом шифрования. Этот метод атаки может быть эффективным, если злоумышленник имеет доступ к большому количеству входных и выходных данных.
5	Метод дифференциального криптоанализа	это метод атаки, при котором злоумышленник ищет различия в двух сообщениях, которые шифруются одним и тем же ключом шифрования. Этот метод атаки может быть эффективным, если злоумышленник имеет доступ к большому количеству пар сообщений и может провести анализ для поиска зависимостей между входными данными, выходными данными и ключом шифрования.

© Электронный научный журнал «Инженерный вестник Дона», 2007–2023

1	2	3
6	Метод снижения размерности	это метод атаки, который использует математические методы для снижения размерности задачи расшифровки данных, что делает ее более простой для решения. Этот метод атаки может быть эффективным, если злоумышленник имеет достаточно большое количество данных.
7	Метод корреляционной статистики	это метод атаки, который использует корреляционные анализы для выявления зависимостей между входными данными, выходными данными и ключом шифрования. Этот метод атаки может быть эффективным, если злоумышленник имеет достаточно большое количество входных и выходных данных.

Важно отметить, что большинство из этих методов атак являются сложными и требуют значительных вычислительных ресурсов [6,7]. Кроме того, использование сильных ключей шифрования, а также правильная реализация алгоритма шифрования могут существенно уменьшить вероятность успешной атаки на систему.

© Электронный научный журнал «Инженерный вестник Дона», 2007–2023

Для расшифровки информации зашифрованной алгоритмом RSA возможно использовать атаки следующих видов:

Таблица 2

Виды атак для алгоритма RSA

№	Название атаки	Описание
1	2	3
1	Метод факторизации	RSA основывается на том, что факторизация больших чисел является трудной задачей. Однако, если злоумышленник сможет разложить на множители число N, используемое при шифровании сообщения, то он сможет получить секретный ключ и расшифровать сообщение. Для этого используются алгоритмы факторизации, такие как метод факторизации Ферма и метод решета чисел.
2	Метод выборки текста	если злоумышленник может получить несколько закодированных сообщений, которые содержат одну и ту же информацию, он может использовать их для расшифровки других сообщений, которые были зашифрованы с использованием того же открытого ключа.

© Электронный научный журнал «Инженерный вестник Дона», 2007–2023

1	2	3
3	Метод повторного использования	если злоумышленник перехватит зашифрованное сообщение, он может повторно отправить его на сервер, который будет использовать тот же открытый ключ для расшифровки сообщения. Злоумышленник может использовать полученное расшифрованное сообщение для получения секретного ключа.
4	Метод подбора открытого ключа	если злоумышленник знает, что сообщение было зашифровано с использованием RSA, он может попробовать подобрать открытый ключ, используя общеизвестные значения для p и q. Эта атака называется атакой методом Боннигтона.
5	Метод грубой силы	если злоумышленник может перехватить зашифрованное сообщение и знает, что это сообщение имеет низкую энтропию (т.е. оно содержит мало случайности), он может использовать атаку методом грубой силы для перебора всех возможных комбинаций для расшифровки сообщения.

© Электронный научный журнал «Инженерный вестник Дона», 2007–2023

1	2	3
6	Метод времени	если злоумышленник может измерить время, которое требуется для расшифровки зашифрованного сообщения, он может использовать эту информацию для получения секретного ключа. Для этого злоумышленник может отправить много зашифрованных сообщений на сервер, измерить время, которое требуется на расшифровку каждого из них, и сравнить время, необходимое для каждого расшифрованного сообщения. Если время расшифровки сообщения зависит от секретного ключа, злоумышленник может использовать эту информацию для определения значений секретного ключа.
7	Метод ошибок	если злоумышленник может перехватить несколько зашифрованных сообщений, он может использовать атаку методом ошибок для определения значения секретного ключа. Эта атака основывается на том, что при дешифровании сообщения может возникнуть ошибка, если значения ключа неверны. Злоумышленник может использовать эту информацию для определения правильных значений ключа.

© Электронный научный журнал «Инженерный вестник Дона», 2007–2023

1	2	3
8	Метод подделки	если злоумышленник может влиять на сообщения, которые зашифрованы с использованием RSA, он может использовать атаку методом подделки, чтобы создать свои собственные сообщения, которые будут расшифровываться так, как злоумышленник хочет.

В целом, для того чтобы защитить информацию, зашифрованную методом RSA, следует принимать следующие меры [8]:

1. Генерировать ключи с помощью достаточно больших простых чисел p и q, чтобы избежать возможных атак на основе факторизации.
2. Использовать достаточно длинные ключи для защиты от атак методом перебора.
3. Хранить приватный ключ в надежном месте, чтобы предотвратить несанкционированный доступ.
4. Использовать защищенный протокол передачи данных при передаче зашифрованной информации, чтобы защитить ее от перехвата и расшифровки злоумышленниками.
5. Регулярно обновлять ключи, чтобы избежать возможных уязвимостей в системе.
6. Использовать дополнительные меры защиты, например, добавление цифровой подписи для подтверждения подлинности сообщений или

© Электронный научный журнал «Инженерный вестник Дона», 2007–2023

использование двухфакторной аутентификации для защиты от несанкционированного доступа к приватному ключу.

Для расшифровки информации зашифрованной алгоритмом SHA возможно использовать атаки следующих видов:

Таблица 3

Виды атак для алгоритма SHA

№	Название атаки	Описание
1	2	3
1	На дневной свет	это метод, при котором злоумышленник вычисляет хеш-функцию для большого количества случайных входных данных и сохраняет хеш-коды в базу данных. Затем злоумышленник ищет коллизии в хеш-кодах, которые могут использоваться для расшифровки информации.
2	С помощью библиотек	это метод, при котором злоумышленник может использовать ошибки в реализации библиотек хеш-функций, которые могут привести к возможности расшифровки хеш-кода. Такие ошибки могут возникнуть, например, из-за недостаточной проверки входных данных, дополнительной логики или неожиданного поведения при определенных входных данных.

© Электронный научный журнал «Инженерный вестник Дона», 2007–2023

1	2	3
3	Метод перебора	это метод, при котором злоумышленник генерирует случайные входные данные, вычисляет их хеш-коды и сравнивает их с целевым хеш-кодом, пока не найдет соответствующий. Однако, SHA имеет большую длину хеш-кода, что делает такой подход практически невозможным.
4	Метод рассматривания	это метод, при котором злоумышленник может искать уязвимости в реализации алгоритма хеширования SHA и использовать эти уязвимости для обхода хеширования. Такие уязвимости могут включать в себя ошибки в реализации алгоритма или обнаружение слабых мест в алгоритме, которые могут быть использованы для расшифровки информации.

После рассмотрения различных методов атак можно сделать вывод что даже эти алгоритмы шифрования не являются абсолютно безопасными.

Рекомендации пользователю, которые могут помочь улучшить безопасность данных:

1. Для повышения уровня безопасности данных необходимо использовать комплексные методы защиты [9-11]. Один из таких методов – это использование нескольких алгоритмов шифрования последовательно. Данный подход позволяет существенно повысить уровень защиты данных, так как

© Электронный научный журнал «Инженерный вестник Дона», 2007–2023

атакующий должен расшифровать данные с использованием нескольких различных алгоритмов.

2. Необходимо периодически обновлять используемые алгоритмы шифрования для предотвращения возможных атак [9]. Многие алгоритмы шифрования имеют ограниченный срок жизни, так как уязвимости могут быть обнаружены со временем.

В данной статье был проведен анализ современных алгоритмов шифрования данных. Были рассмотрены наиболее распространенные алгоритмы шифрования, такие как AES, RSA и SHA. Также были рассмотрены уязвимости данных алгоритмов и различные методы атак. Для повышения уровня безопасности данных необходимо использовать комплексные методы защиты и периодически обновлять используемые алгоритмы шифрования.

Литература

1. Бабенко Л.К., Ищукова Е.А. Современные алгоритмы блочного шифрования и методы их анализа. - М.: Гелиос АРВ, 2015. - 376 с.

2. Мао В. Современная криптография: теория и практика. - М.: Вильямс, 2005. - 768 с.

3. Paar C., Pelzl J. Understanding Cryptography: A Textbook for Students and Practitioners. Springer, 2009. - 372 с.

4. Панасенко С.П. Алгоритмы шифрования. Специальный справочник.. - СПб.: БХВ-Петербург, 2009. - 576 с.

5. Шаньгин В.Ф. Информационная безопасность и защита информации. - М.: ДМК Пресс, 2014. - 702 с.

6. Жданов О. Н. Методика выбора ключевой информации для алгоритма блочного шифрования. - М.: ИНФРА-М, 2015. - 869 с.

© Электронный научный журнал «Инженерный вестник Дона», 2007–2023

7. Плёнкин А.П. Симметричное шифрование квантовыми ключами // Инженерный вестник Дона. 2016. №3. URL: ivdon.ru/ru/magazine/archive/n1y2016/3705.

8. Мациборко В.В., Будко А.Ю., Береснев А.Л., Мациборко М.А. Исследование устройств регистрации ионного тока в камере сгорания // Инженерный вестник Дона, 2014, №4. URL: ivdon.ru/ru/magazine/archive/n4y2014/2611/.

9. Лось А. Б., Нестеренко А. Ю., Рожков М. И. Криптографические методы защиты информации. - 2-е изд. - М.: Юрайт, 2016. - 474 с.

10. Ferguson N., Schneier B., Kohno T. Cryptography Engineering: Design Principles and Practical Applications. Wiley, 2011. - 558 с.

11. Горев А. И., Симаков А. А. Обеспечение Информационной Безопасности. - М.: Звезда Петербурга, 2005. - 446 с.

References

1. Babenko L.K., Ishchukova E.A. Sovremennye algoritmy blochnogo shifrovaniya i metody ikh analiza [Modern block cipher algorithms and methods of their analysis]. M.: Gelios ARV, 2015. 376 p.

2. Mao V. Sovremennaya kriptografiya: teoriya i praktika [Modern Cryptography: Theory and Practice]. M.: Vil'yams, 2005. 768 p.

3. Paar C., Pelzl J. Understanding Cryptography: A Textbook for Students and Practitioners. Springer, 2009. 372 p.

4. Panasenko S.P. Algoritmy shifrovaniya. Spetsial'nyy spravochnik. [Encryption algorithms. Special Reference Guide.]. SPb.: BKhV-Peterburg, 2009. 576 p.

5. Shan'gin V.F. Informacionnaja bezopasnost' i zashhita informacii [Information security and information protection]. M.: DMK Press, 2014. 702 p.

© Электронный научный журнал «Инженерный вестник Дона», 2007–2023

6. Zhdanov O. N. Metodika vybora kljuchevoj informacii dlja algoritma blochnogo shifrovanija [Methodology for selecting key information for a block cipher algorithm]. M.: INFRA-M, 2015. 869 p.

7. Pljonkin A.P. Inzhenernyj vestnik Dona, 2016, №3. URL: ivdon.ru/ru/magazine/archive/n1y2016/3705.

8. Matsiborko V.V., Budko A.Yu, Beresnev A.L., Matsiborko M.A. Inzhenernyj vestnik Dona, 2014, №4, URL: ivdon.ru/ru/magazine/archive/n4y2014/2611/.

9. Los' A. B., Nesterenko A. Ju., Rozhkov M. I. Kriptograficheskie metody zashhity informacii [Cryptographic methods of information protection]. 2-e izd. M.: Jurajt, 2016. 474 p.

10. Ferguson N., Schneier B., Kohno T. Cryptography Engineering: Design Principles and Practical Applications. Wiley, 2011. 558 p.

11. Gorev A. I., Simakov A. A. Obespechenie Informacionnoj Bezopasnosti [Ensuring Information Security]. M.: Zvezda Peterburga, 2005. 446 p.

© Электронный научный журнал «Инженерный вестник Дона», 2007–2023