УДК 654.164 DOI: 10.18698/2541-8009-2019-05-484

ШИФРОВАНИЕ ДАННЫХ В ТЕЛЕКОММУНИКАЦИОННЫХ СЕТЯХ

А.А. Долова n.dlv@yandex.ru
SPIN-код: 9826-0740

А.Ю. Константиниди keepesh97@mail.ru
SPIN-код: 1386-9265

МГТУ им. Н.Э. Баумана, Москва, Российская Федерация

Аннотация

Рассмотрены проблемы взлома и перехвата данных, передаваемых по телекоммуникационным сетям. Обобщены основные подходы к шифрованию данных. Описаны принципы работы простых асинхронных алгоритмов шифрования AES и RSA. Предложена пошаговая практическая методика реализации приведенных алгоритмов на кроссплатформенном языке программирования высокого уровня Java, которая является решением проблемы защиты данных, передаваемых с помощью современных средств связи, основанных на использовании телекоммуникационных технологий. По результатам исследований даны рекомендации по криптографической ценности каждого алгоритма, их достоинств и недостатков, а также приведены примеры предпочтительного использования каждого варианта.

Ключевые слова

Шифрование, телекоммуникации, сети, алгоритм, RSA, AES, данные, защита

Поступила в редакцию 08.04.2019

Введение. Работа посвящена исследованию принципов построения алгоритмов синхронного и асинхронного шифрования и разработке способа их реализации на кроссплатформенном языке программирования.

Объектом исследования являются технологии формирования способов кодирования информации.

Актуальность работы заключается в том, что в век высоких информационных технологий информация является одним из самых ценных ресурсов во всех сферах жизнедеятельности. Изначально люди имели возможность передавать информацию друг другу только вербально — при встрече друг с другом. Позже появились рисунки, а затем и письменность. С того момента как информацию научились облекать в физическую форму, возник вопрос ее защиты. Появились тайные алфавиты, различные шифры, которые со временем становились все сложнее. Однако никогда еще в истории человечества вопрос о защите информации не стоял так остро. В современном мире множество самых разных аспектов жизнедеятельности принимает информационную форму: множество документов хранится в личных государственных кабинетах каждого гражданина, его заработная плата поступает на банковскую карточку, баланс которой он прове-

ряет через мобильные приложения, а личные переписки самого различного характера теперь осуществляются по электронной почте и с помощью мобильных мессенджеров. Огромный объем информации ежедневно передается по телекоммуникационным сетям, а также хранится на их серверах. Для того чтобы обезопасить информацию от получения и обработки третьими лицами, были придуманы алгоритмы шифрования, которые реализуются самими разнообразными методами.

Основными проблемами существующих алгоритмов шифрования являются сложности в совмещении высокой скорости вычисления и обработки информации с достаточным уровнем надежности.

Цель работы — рассмотреть простейшие алгоритмы синхронного и асинхронного шифрования AES и RSA, а также осуществить их реализацию на высокоуровневом языке программирования Java.

Новизна работы заключается в предложенной методике совершенствования функционирования и повышения эффективности применения алгоритмов синхронного и асинхронного шифрования. Эта проблема приобретает особую актуальность в связи с постоянно растущей интеграцией электронных механизмов обработки данных в современную бытовую деятельность человека и необходимостью ее защиты от перехвата сторонними лицами.

Результатом работы являются:

– первичный анализ основных понятий и определений, связанных с методиками шифрования;

– анализ рассматриваемых в данной статье алгоритмов шифрования — AES, RSA;

– анализ операций технологического процесса по операционной диаграмме в нотации IDEF3;

– практическая реализация вышеуказанных алгоритмов на высокоуровневом языке программирования java с приведенным описанием скриптов;

– выводы, приведенные исходя из сравнительного анализа основных характеристических параметров работы алгоритмов синхронного и асинхронного шифрования.

Практическая ценность работы состоит в методике разработки программ на кроссплатформенном языке программирования, реализующих шифрование данных алгоритмами AES, RSA.

Анализ подходов, методов и средств к шифрованию данных в телекоммуникационных сетях. Шифрование — способ защиты данных от неавторизованных пользователей путем обработки и представления данных в искаженном зашифрованном виде. Неавторизованным считается пользователь, у которого нет ключа для расшифровки данных [1].

Таким образом, шифрование в телекоммуникационных сетях можно определить как обработку данных, осуществляемую путем выполнения определенных математических действий, называемых алгоритмом шифрования,

предназначенную для перевода данных в формат, недоступный для общего понимания. Перевод информации в исходное состояние осуществляется путем выполнения обратных преобразований, которые именуются расшифровкой. Ключом к шифру называется генерируемый в ходе шифрования набор символов, который является частью математической функции, заложенной в алгоритме шифрования. Именно благодаря ключу авторизованные пользователи, выполняя расшифровку данных, могут получить их в первоначальном виде. Наука, которая описывает способы сокрытия информации методами шифрования, называется криптографией [2, 3].

Благодаря шифрованию обеспечивается три главных аспекта безопасности информации [4]:

– конфиденциальность (полезная информация скрывается от пользователей, не обладающих правами доступа к ней);

– целостность (при передаче и хранении данных полезная информация защищена от редактирования и внесения каких-либо изменений);

– идентифицируемость (источник или отправитель информации может быть аутентифицирован, что исключит возможность отказа отправителя от факта передачи данной информации.

Алгоритмы шифрования делятся на три основных типа: бесключевые, одноключевые и двухключевые [5]. Первые основаны на общей математической функции, не включающей в себя дополнительных параметров. В других методах для усложнения алгоритма шифрования и расшифровки подключается дополнительный параметр — ключ, один или несколько, в зависимости от типа шифрования.

Шифрование методом AES. Алгоритм шифрования AES основан на использования для кодирования и раскодировки информации одного и того же секретного ключа. Таким образом, отправитель шифрует информацию, а получатель, который заведомо владеет секретным ключом, расшифровывает. Алгоритм основан на выполнении определенного порядка простейших математических операций: подстановках, перестановках и линейных преобразованиях. Эти операции выполняются некоторое количество раз, называемое раундами. Данные делятся на блоки по 16 байтов, что позволяет получить ряд преимуществ перед традиционным потоковым шифрованием, поскольку изменение каждого бита в ключе или блоке открытого текста приведет к получению совершенно нового блока зашифрованных данных.

Различают три основных типа AES шифрования [6], определенных по длине ключа:

– AES-128;

– AES-192;

– AES-256.

Длина ключей в данных типах шифрования равно 128, 192 и 256 бит соответственно. Алгоритм AES отличается достаточно высокой скоростью шифро-

вания данных, а также сравнительно высокой степенью надежности. Попытка подбора AES ключа на современных ЭВМ по приблизительным расчетам ученых заняла бы период времени, сравнимый с предполагаемым возрастом Вселенной [7].

Шифрование методом RSA. Алгоритм шифрования RSA относится к ассиметричным системами шифрования, что означает использование для шифрования и расшифровки не одного ключа, а пары ключей: открытого, доступного всем пользователям и не требующего какой-либо защиты, и закрытого [5, 6]. Данные ключи работают в паре. Это означает, что сообщение, зашифрованное одним из ключей, может быть расшифровано только при наличии второго. Алгоритм основан на одной из главных математических проблем: факторизации целого числа.

Данные, которые необходимо зашифровать, рассматриваются как одно большое целое число. В процессе шифрования это число увеличивается до степени ключа и делится с остатком на произведение двух заведомо выбранных простых чисел [8]. Выполняя данный процесс с другим ключом, исходный текст можно получить вновь. Однако на основе описанного алгоритма можно сделать вывод, что данный шифр может быть взломан путем факторизации продукта, используемого при делении. Однако на данный момент времени вычислить необходимые коэффициенты для чисел, код числа которых превышает 768 бит, невозможно [9, 10].

Практическая реализация шифрования AES и RSA. Для того чтобы использовать вышеописанные алгоритмы шифрования для передачи данных по сети, необходимо реализовать их на одном из высокоуровневых языков программирования. В данной работе был выбран объектно-ориентированный язык Java, который на данный момент является одним из самых популярных и широко используемых языков программирования. Одним из главных его преимуществ по праву считается кроссплатформенность, благодаря чему данная реализация шифрования AES и RSA может быть внедрена в любой современный интерфейс, поддерживающий передачу данных по сети [11]. Объявим и выведем строку, которую необходимо зашифровать:

```
String str1 = "nastya_iu4";
System.out.println(str1 + " ");
```

Для реализации вычислительных последовательностей воспользуемся стандартным классом языка JavaCipher, который выполнит математическую последовательность необходимых вычислительных операций.

Создадим объект класса Cipher и инициализируем его по алгоритму шифрования:

```
Cipher cipher = Cipher.getInstance("AES");
```

Сгенерируем секретный ключ для алгоритма шифрования данных, определив его как случайную последовательность символов длиной в 128 бит:

```
KeyGenerator random = KeyGenerator.getInstance("AES");
random.init( keysize: 128);
SecretKey key = random.generateKey();
```

Определим операцию шифрования созданным ключом, создадим массив, в который запишем зашифрованные данные, и реализуем вывод результата в консоль:

```
cipher.init(Cipher.ENCRYPT_MODE, key);
byte[] secret = cipher.doFinal(str1.getBytes());
for(int i = 0; i < secret.length; i++){
    byte b = secret[i];
    System.out.print(b);
}
```

Определим функцию расшифровки данных и пропишем вывод результата:

```
Cipher decoder = Cipher.getInstance("AES");
decoder.init(Cipher.DECRYPT_MODE, key);
byte[] decoded_secret = decoder.doFinal(secret);
for(int i = 0; i < decoded_secret.length; i++){
    byte b = decoded_secret[i];
    System.out.print((char) b);
}
```

Таким образом, после компиляции получили последовательность из начального блока данных, зашифрованное сообщение и декодированное сообщение, которое полностью совпало с изначальным блоком данных:

```
nastya_iu4
17-17266910-1419-341-1199472-5-15-10147
nastya_iu4
Process finished with exit code 0
```

Аналогичным образом реализуется алгоритм шифрования RSA, за тем исключением, что для данного метода нам необходимо инициализировать и сгенерировать два ключа: публичный и приватный:

```
nastya_iu4_another_method
10926-122-57529958-107138696-69-8620-43-3012212620-25-69781074639-7565747-538028
nastya_iu4_another_method
Process finished with exit code 0
```

Метод реализации данных операций представлен на полном листинге программного кода. Создание пар ключей вынесено отдельным блоком кода, где идет реализация открытого ключа OpenSource и закрытого ключа PrivateSource, которыми в последствии будет происходить шифрование и расшифровка данных соответственно.

Листинг кода шифрования алгоритмом RSA

```
import javax.crypto.*;
import javax.security.auth.login.LoginException;
import java.security.*;

public class RSA {
public static void main(String[] args) throws LoginException, NoSuchAlgorithmException
        , NoSuchPaddingException, InvalidKeyException, BadPaddingException, IllegalBlockSizeException {

      String str1 = "nastya_iu4_another_method";
System.out.println(str1 + " ");

      Cipher cipher = Cipher.getInstance("RSA");

KeyPairGenerator MakeNewPair = KeyPairGenerator.getInstance("RSA");
KeyPair NewPair = MakeNewPair.generateKeyPair();
      Key OpenSource = NewPair.getPublic();
      Key PrivateSource = NewPair.getPrivate();


cipher.init(Cipher.ENCRYPT_MODE, OpenSource);
byte[] secret = cipher.doFinal(str1.getBytes());
for(int i = 0; i<secret.length; i++){
byte b = secret[i];
System.out.print(b);
      }
System.out.println(' ');
      Cipher decoder = Cipher.getInstance("RSA");
decoder.init(Cipher.DECRYPT_MODE, PrivateSource);
byte[] decoded_secret = decoder.doFinal(secret);
for(int i = 0; i<decoded_secret.length; i++){
byte b = decoded_secret[i];
System.out.print((char) b);
      }
   }
}
```

Согласно представленным результатам видно, что оба алгоритма полностью удовлетворяют главной задаче сокрытия смысла исходного блока данных. В результате компиляции было выявлено, что на обработку одной и той же строки (для эксперимента была взята строка первого метода “nastya_iu4”), было потрачено в первом случае 993 мс, а во втором случае — 2 с 779 мс, что говорит о явном преимуществе алгоритма AES по скорости вычисления.

При решении комплекса задач, связанных с аудитом информационной безопасности программного обеспечения вычислительных систем, возникает необходимость анализа данных различного рода. При проведении аудита информационной безопасности в случае отсутствия технической документации появляется необходимость анализа данных в условиях неосведомленности об архитек-

туре вычислительной системы [12–14]. Применяя шифрование в телекоммуникационных сетях можно обеспечить требуемый уровень качества сложных программных систем [15].

Заключение. Криптография является одним из главных методов защиты информации, передаваемой по телекоммуникационным сетям. Каждый тип шифрования обладает своими преимуществами и недостатками. Разобранные алгоритмы симметричной и асимметричной криптографии отличаются по вычислительной сложности и степени надежности, именно поэтому лучше не отдавать предпочтение какому-либо одному типу шифрования, а использовать их в симбиозе. Так, извлекая все преимущества скорости вычисления алгоритма AES, целесообразно шифровать весь основной пакет данных именно этим методом, а ключ к шифру дополнительно кодировать алгоритмом RSA, пользуясь его высокой надежностью. Данный метод безопасной передачи данных можно реализовать на любом устройстве в сети, поскольку выбранный для реализации язык программирования Java поддерживает кроссплатформенность.

Литература

[1] Асосков А.В., Иванов М.А., Мирский А.А. и др. Поточные шифры. М., Кудиц-образ, 2003.

[2] Рябко Б.Я., Фионов А.Н. Криптографические методы защиты информации. М., Горячая линия – Телеком, 2005.

[3] Архангельская А.В., Запечников С.В. Характеристики области эффективного применения методов поточного шифрования для защиты трафика в телекоммуникационных системах. *Информационное противодействие угрозам терроризма*, 2005, № 4, с. 183–186.

[4] Шнайер Б. Прикладная криптография. Протоколы, алгоритмы, исходные тексты на языке Си. М., Триумф, 2002.

[5] Бабенко Л.К, Ищукова Е.А. Дифференциальный крипто анализ поточных шифров. *Известия ЮФУ. Технические науки*, 2009, № 11, с. 232–238.

[6] Баженов Р.И. Информационная безопасность и защита информации. Биробиджан, ДГСГА, 2011.

[7] Бикмаева Е.В., Баженов Р.И. Об оптимальном выборе системы защиты информации от несанкционированного доступа. *APRIORI. Серия: Естественные и технические науки*, 2014, № 6. URL: http://www.apriori-journal.ru/index.php/journal-estesvennie-nauki/id/414

[8] Коноваленко Д.А., Баженов Р.И. Разработка лабораторно–практических работ по стеганографическим и криптографическим методам защиты информации в курсе «Информационная безопасность». *Современная педагогика,* 2014, № 11(24), с. 27–33.

[9] Ирзаев Г.Х. Экспертный метод аудита информационных систем. *Вестник Дагестанского государственного технического университета. Технические науки*, 2011, т. 1, № 20, с. 11–15.

[10] Абакарова О.Г., Ирзаев Г.Х. Метод интегральной оценки качества информационных систем правоохранительных органов. *Научное обозрение*, 2014, № 2, с. 180–184.

[11] Демин А.А., Карпунин А.А., Ганев Ю.М. Методы верификации и валидации сложных программных систем. *Программные продукты и системы*, 2014, № 4, с. 229–233.

[12] Сельвесюк Н.И., Островский А.С., Гладких А.А. и др. Объектно–ориентированное проектирование нейронной сети для автоматизации определения архитектуры вычислительной системы в задачах обеспечения информационной безопасности. *Научный вестник НГТУ*, 2016, № 1(62), с. 133–145.

[13] Власов А.И., Колосков С.В., Пакилев А.Е. Нейросетевые методы и средства обнаружения атак на сетевом уровне. *Нейроинформатика-2000. 2-я Всеросс. науч.- тех. конф. Сб. науч. тр. Ч. 1*. М., Изд-во МИФИ, 2000, с. 30–40.

[14] Пугачев Е.К., Лапина Н.А. Подход к проектированию механизма обновления баз правил системы обнаружения атак. *Технологии инженерных и информационных систем*, 2018, № 3, с. 110–114.

[15] Карпунин А.А., Ганев Ю.М., Чернов М.М. Методы обеспечения качества при проектировании сложных программных систем. *Надежность и качество сложных систем*, 2015, № 2(10), с. 78–84.

Долова Анастасия Андреевна — бакалавр кафедры «Проектирование и технология производства электронной аппаратуры», МГТУ им. Н.Э. Баумана, Москва, Российская Федерация.

Константиниди Анастас Юрьевич — бакалавр кафедры «Проектирование и технология производства электронной аппаратуры», МГТУ им. Н.Э. Баумана, Москва, Российская Федерация.

DATA ENCRYPTION IN TELECOMMUNICATION NETWORKS

A.A. Dolova n.dlv@yandex.ru
SPIN-code: 9826-0740

A.Yu. Konstantinidi keepesh97@mail.ru
SPIN-code: 1386-9265

Bauman Moscow State Technical University, Moscow, Russian Federation

Abstract

This article reviews the problems of hacking and interception of data transmitted over telecommunications networks. The main approaches to data encryption are summarized. The principles of operation of simple asynchronous encryption algorithms AES and RSA are described. A step-by-step practical technique for implementing the above algorithms in a high-level cross-platform programming language Java is proposed, which is a solution to the problem of protecting data transmitted using modern communication tools based on the use of telecommunication technologies. According to the research results, recommendations on the cryptographic value of each algorithm are given, their advantages and disadvantages and examples of the preferred use of each option are described.

Keywords

Encryption, telecommunications, networks, algorithm, RSA, AES, data, protection

Received 08.04.2019

References

[1] Asoskov A.V., Ivanov M.A., Mirskiy A.A., et al. Potochnye shifry [Stream ciphers]. Moscow, Kudits-obraz Publ., 2003 (in Russ.).

[2] Ryabko B.Ya., Fionov A.N. Kriptograficheskie metody zashchity informatsii [Cryptographic methods of information protection]. Moscow, Goryachaya liniya –Telekom Publ., 2005 (in Russ.).

[3] Arkhangel'skaya A.V., Zapechnikov S.V. Properties of effective application area of stream encryption methods for traffic protection in telecommunication systems. *Informatsionnoe protivodeystvie ugrozam terrorizma*, 2005, no. 4, pp. 183–186 (in Russ.).

[4] Shnayer B. Prikladnaya kriptografiya. Protokoly, algoritmy, iskhodnye teksty na yazyke Si [Applied cryptography. Protocols, algorithms, source codes in C language]. Moscow, Triumf Publ., 2002 (in Russ.).

[5] Babenko L.K, Ishchukova E.A. Differential cryptanalysis of stream ciphers. *Izvestiya YuFU. Tekhnicheskie nauki* [Izvestiya SFedU. Engineering Sciences], 2009, no. 11, pp. 232–238 (in Russ.).

[6] Bazhenov R.I. Informatsionnaya bezopasnost' i zashchita informatsii [Information safety and information protection]. Birobidzhan, DGSGA Publ., 2011 (in Russ.).

[7] Bikmaeva E.V., Bazhenov R.I. The optimal choice of the system to protect information from unauthorized access. *APRIORI. Seriya: Estestvennye i tekhnicheskie nauki*, 2014, no. 6. URL: http://www.apriori-journal.ru/index.php/journal-estesvennie-nauki/id/414 (in Russ.).

[8] Konovalenko D.A., Bazhenov R.I. Development of laboratory practical works on steganography and cryptography methods to protect the information in the subject "Information security". *Sovremennaya pedagogika* [Modern pedagogy], 2014, no. 11(24), pp. 27–33 (in Russ.).
[9] Irzaev G.Kh. The expert method of safety audit of the information systems. *Vestnik Dagestanskogo gosudarstvennogo tekhnicheskogo universiteta. Tekhnicheskie nauki* [Herald of Daghestan State Technical University. Technical Sciences], 2011, vol. 1, no. 20, pp. 11–15 (in Russ.).
[10] Abakarova O.G., Irzaev G.Kh. Method of integral assessment of the quality of information systems of law enforcement agencies. *Nauchnoe obozrenie* [Science Review], 2014, no. 2, pp. 180–184 (in Russ.).
[11] Demin A.A., Karpunin A.A., Ganev Yu.M. Verification and validation methods for complex software systems. *Programmnye produkty i sistemy* [Software & Systems], 2014, no. 4, pp. 229–233 (in Russ.).
[12] Sel'vesyuk N.I., Ostrovskiy A.S., Gladkikh A.A., et al. Object-oriented design of a neural network to automate the process of computer architecture determination in the information security problems. *Nauchnyy vestnik NGTU* [Scientific Bulletin of NSTU], 2016, no. 1(62), pp. 133–145 (in Russ.).
[13] Vlasov A.I., Koloskov S.V., Pakilev A.E. [Neural network methods and attack detecting equipment at network level]. *Neyroinformatika-2000. 2-ya Vseross. nauch.- tekh. konf. Sb. nauch. tr. Ch. 1* [Neuroinformatics-2000. Proc. 2nd Russ. Sci.-Tech. Conf. Vol. 1]. Moscow, MEPhI Publ., 2000, pp. 30–40 (in Russ.).
[14] Pugachev E.K., Lapina N.A. Engineering approach to renovation mechanism of rule database for attack detection system. *Tekhnologii inzhenernykh i informatsionnykh system* [Technologies of Engineering and Information Systems], 2018, no. 3, pp. 110–114 (in Russ.).
[15] Karpunin A.A., Ganev Yu.M., Chernov M.M. Quality assurance methods in complex program systems design. *Nadezhnost' i kachestvo slozhnykh system* [Reliability & Quality of Complex Systems], 2015, no. 2(10), pp. 78–84 (in Russ.).

Dolova A.A. — Bachelor's Degree Student, Department of Electronic Equipment Design and Technology, Bauman Moscow State Technical University, Moscow, Russian Federation.

Konstantinidi A.Yu. — Bachelor's Degree Student, Department of Electronic Equipment Design and Technology, Bauman Moscow State Technical University, Moscow, Russian Federation.