ИНФОРМАТИКА И ИНФОРМАЦИОННЫЕ ПРОЦЕССЫ / INFORMATICS AND INFORMATION PROCESSES

DOI: https://doi.org/10.23670/IRJ.2024.142.11

РАЗРАБОТКА РАСПРЕДЕЛЕННОЙ СИСТЕМЫ КРИПТОАНАЛИЗА АЛГОРИТМА RSA

Обзор

Калинина Е.С.[1], Манохина Т.В.[2], Подгорная С.О.[3,] *, Ступаков С.А.[4]
[1, 2, 3, 4] Омский государственный университет путей сообщения, Омск, Российская Федерация

* Корреспондирующий автор (ps.light[at]mail.ru)

Аннотация

Одним из важнейших этапов создания современных криптографических алгоритмов является их последующий криптоанализ, который в конечном итоге и определяет возможность применения того или иного алгоритма в определенной сфере защиты информации. В данном контексте требования к криптоанализу, его эффективности и точности значительным образом повышаются. Безопасность RSA зависит от размера и качества ключей, а также от выбора параметров и схем заполнения. Наиболее распространенной атакой на RSA является атака методом перебора, которая пытается факторизовать открытый ключ и найти закрытый ключ. В статье рассмотрены подходы к разработке распределенной системы криптоанализа алгоритма RSA. Представлена модель распределенной компьютерной системы криптоанализа на основе Raspberry Pi, которая реализована в виде кластера на основе восьми мини-компьютеров для организации вычислений по шифрованию/дешифрованию сообщений.

Ключевые слова: криптоанализ, шифрование, алгоритм, распределенная система, информация, защита.

DEVELOPMENT OF A DISTRIBUTED SYSTEM FOR CRYPTANALYSIS OF THE RSA ALGORITHM

Review article

Kalinina Y.S.[1], Manokhina T.V.[2], Podgornaya S.O.[3,] *, Stupakov S.A.[4]
[1, 2, 3, 4] Omsk State University of Railway Engineering, Omsk, Russian Federation

* Corresponding author (ps.light[at]mail.ru)

Abstract

One of the most important stages in the creation of modern cryptographic algorithms is their subsequent cryptanalysis, which ultimately determines the possibility of using a particular algorithm in a specific area of information security. In this context, the requirements for cryptanalysis, its efficiency and accuracy are significantly increased. The security of RSA depends on the size and quality of the keys, as well as the choice of parameters and filling schemes. The most common attack on RSA is the brute-force attack, which attempts to factorize the public key and find the private key. The work discusses an approach to the development of a distributed cryptanalysis system for the RSA algorithm. The model of a distributed computer system of cryptanalysis based on Raspberry Pi is presented, which is implemented as a cluster based on eight mini-computers to organize message encryption/decryption computations.

Keywords: cryptanalysis, encryption, algorithm, distributed system, information, protection.

Введение

Актуальность криптоанализа асимметричных криптоалгоритмов заключается в том, что они используются для защиты каналов передачи данных во многих сферах жизнедеятельности человека: шифрование сеансовых ключей и данных, генерирование цифровых электронных подписей и др. С целью своевременного обнаружения факта, что определенный алгоритм или некоторое множество его ключей являются неустойчивыми для дальнейшего использования, необходимо проводить исследования криптостойкости, т.е. криптоанализ.

Криптоанализ – это искусство и наука оценивания информационных систем с целью изучения их скрытых аспектов [1]. Методы криптоанализа напрямую зависят от криптоалгоритма и информации, которая известна о самой системе, ключах, сообщениях. Особое внимание на сегодняшний день уделяется алгоритму RSA, использование которого позволяет эффективно защитить конфиденциальность и целостность данных в различных приложениях, таких как онлайн-банкинг, электронная коммерция и цифровые подписи. Это один из наиболее распространенных шифров, используемых в протоколе SSL/TLS, позволяющий надежно передавать конфиденциальную информацию через Интернет. Безопасность RSA зависит от размера и качества ключей, а также от выбора параметров и схем заполнения. Наиболее распространенной атакой на RSA является атака методом перебора, которая пытается факторизовать открытый ключ и найти закрытый ключ. Чтобы предотвратить это, ключи RSA должны иметь длину не менее 2048 бит, а лучше 4096 бит или более [2].

На сегодняшний день наиболее эффективными по быстродействию и стоимости вычислительных ресурсов для проведения криптоанализа являются распределенные системы. Узлы таких систем могут иметь SMP-, MPP- или PVP-архитектуры, а также создаваться с помощью специализированных FPGA и/или DSP-процессоров [3]. Такие системы с распределенной памятью хорошо масштабируются и могут быть использованы для криптоанализа различных шифров. Условием эффективного использования распределенных систем является оптимальная декомпозиция вычислительной задачи криптоанализа соответствующего шифра относительно учета особенностей процессорных систем, памяти и коммуникационных средств.

Таким образом, особенности создания распределенных систем криптоанализа, а также современные подходы к их построению с учетом специфики шифров представляют на сегодняшний день актуальную научно-техническую задачу.

Авторы многих актуальных работ по этой тематике (например, Петренко А.С. [4], Ясашный О.П. [5], Vijesh Bhagat [6] и др.) приводят ряд аргументов, указывающих на то, что для использования методов криптоанализа на параллельных и распределенных компьютерных системах целесообразно создавать специализированное программное обеспечение. Наряду с этим ведутся разработки в области создания методологии для реализации современных криптоаналитических методов в грид-среде (Ожиганова М.И. [7], Абелян В.З. [8]).

Цель исследования – рассмотрение подходов к разработке распределенной системы криптоанализа алгоритма RSA.

Методы исследования – анализ, синтез, моделирование, систематизация, обобщение, группировка.

Результаты исседования

При разработке алгоритмов программ, положенных в основу распределенной системы криптоанализа алгоритма RSA необходимо учитывать:

1) особенности вычислительных систем, предназначенных для функционирования соответствующего программного обеспечения, в частности: типы и производительность процессорных систем вычислительных узлов; топологии вычислительных сетей; надежность межузловых соединений; скорость передачи данных и латентность коммуникационных интерфейсов; скорость доступа отдельных узлов к централизованным хранилищам данных;

2) особенности алгоритма RSA, в частности: его способность к функциональной декомпозиции и декомпозиции по данным; требования к синхронизации между отдельными частями программы; количество итераций этого метода для повышения достоверности результата.

С точки зрения применимости системы распределенного криптоанализа для RSA можно сформулировать следующие требования к ее компонентам:

1) максимальная универсальность к типам зашифрованных данных;

2) открытые исходные коды и лицензия свободного программного обеспечения;

3) функционирование на различных платформах;

4) вычисления как на центральных, так и на графических процессорах клиентских персональных компьютеров;

5) операционная система Windows на клиентских персональных компьютерах;

6) неограниченное количество клиентов.

Необходимо отметить, что методология разработки программного обеспечения для распределенных сетей существенно отличается от традиционного подхода, поскольку программы работают в распределенной среде с высокой латентностью, а следовательно, задача усложняется проблемами синхронизации подпрограмм, что может быть обусловлено временной недоступностью или занятостью вычислительных ресурсов [9].

Итак, распределенная компьютерная система криптоанализа представляет собой кластерный компьютер и является альтернативой облачной инфраструктуре. В рамках проводимого исследования предлагается в качестве вычислительных ядер использовать мощность восьми серверных ЦП (32 ядра), что позволит запускать и выполнять вычисления с клиентского узла гораздо быстрее, чем клиент может выполнять их самостоятельно. В качестве программного обеспечения управления кластером целесообразно использовать Python 3, что позволит обеспечить возможности запуска соответствующих скриптов для криптоанализа с клиентской станции.

Для того чтобы визуализировать нагрузку на каждый из серверов в кластере, рекомендуется установить светодиодные матрицы Pimoroni Unicorn HAT 8x8 на каждый сервер. Сценарий управления bash на клиентской машине можно использовать для изменения шаблонов на Unicorn HAT [10].

На рис. 1 показана схема организации распределенной компьютерной системы криптоанализа на основе Raspberry PI.

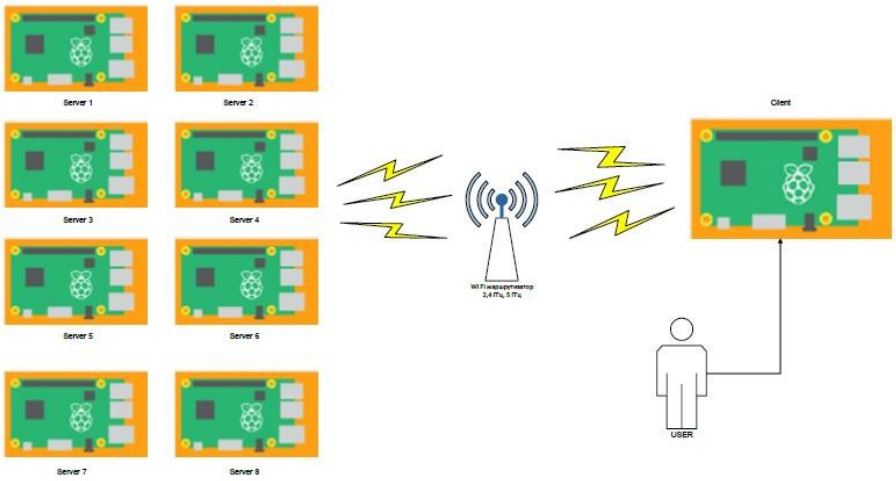

Рисунок 1 - Схема организации распределенной компьютерной системы криптоанализа на основе Raspberry PI

DOI: https://doi.org/10.23670/IRJ.2024.142.11.1

Примечание: составлено автором

Для взаимодействия с распределенной системой криптоаналитик/группа исследователей, которые по отношению к сети являются виртуальной организацией, могут воспользоваться одним из двух подходов. Первый – предполагает использование некоторых утилит с графическим интерфейсом или интерфейсом командной строки, которые позволяют взаимодействовать с промежуточным программным обеспечением для запуска необходимых задач и загрузки файлов в хранилища данных для дальнейшего исследования. Второй подход предусматривает работу с веб-интерфейсом, который, в свою очередь, взаимодействует с промежуточным программным обеспечением, что позволяет выполнять функции по координации работы членов соответствующей виртуальной организации. В рассматриваемом случае актуальным для виртуальной организации является создание криптоаналитического грид-портала с необходимым функционалом.

В качестве примера использования распараллеливания на практике можно рассмотреть XSL-атаку. Она распараллеливается на нескольких этапах (рис. 2): на первом этапе – по входным данным – это множество шифротекстов, подмножества которых могут быть использованы отдельными кластерными системами, на пятом этапе – решение системы линейных алгебраических уравнений для отдельного шифротекста может выполнять целая кластерная система или отдельный ее GPU-узел (вложенная декомпозиция).

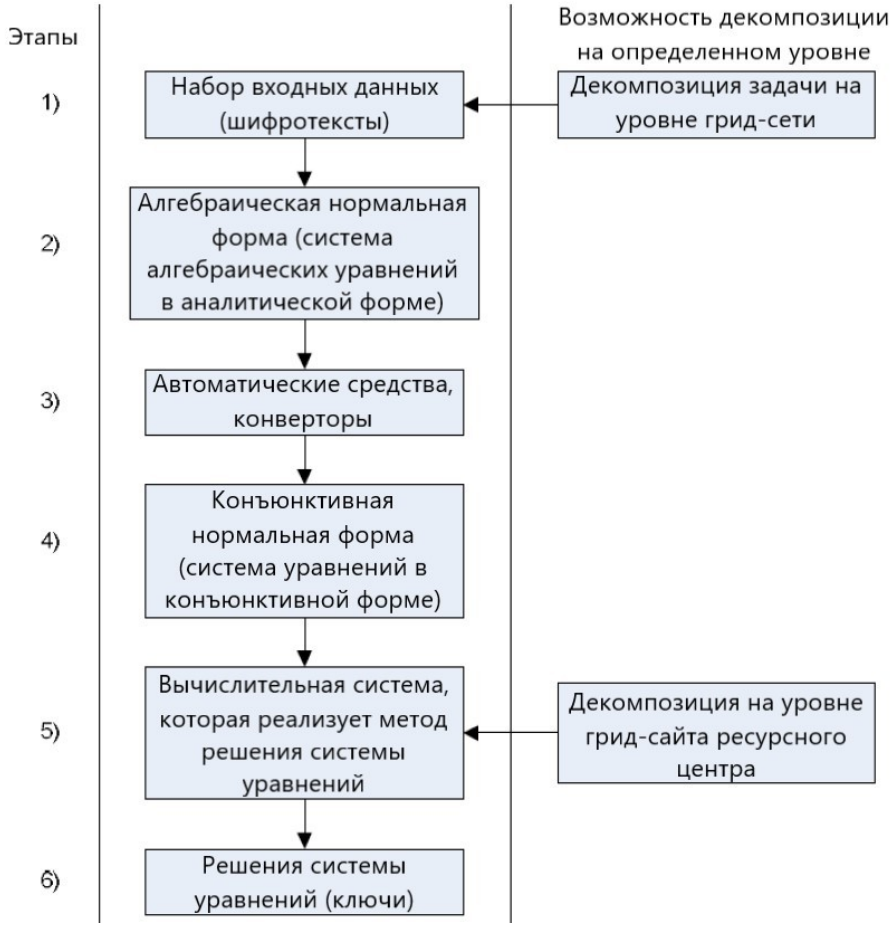

Рисунок 2 - Схема алгебрического криптоанализа и подходы к декомпозиции задачи
DOI: https://doi.org/10.23670/IRJ.2024.142.11.2

Примечание: составлено автором

Заключение

Современные требования к безопасности данных требуют постоянного развития криптографии, а вместе с ней и криптоанализа. Для проверки безопасности и эффективности алгоритмов шифрования разрабатываются новые техники и инструменты. В настоящее время квантовые вычисления, машинное обучение и облачные вычисления являются одними из тенденций и вызовов в криптоанализе RSA.

В данном контексте особого внимания заслуживают распределенные системы криптоанализа. В процессе исследования формализована система на базе вычислительных кластеров для реализации современных криптоаналитических алгоритмов в распределенной среде. В частности, представлена модель распределенной компьютерной системы криптоанализа на основе Raspberry Pi, которая реализована в виде кластера на основе восьми мини-компьютеров для организации вычислений по шифрованию/дешифрованию сообщений.

Конфликт интересов

Не указан.

Рецензия

Сообщество рецензентов Международного научно-исследовательского журнала
DOI: https://doi.org/10.23670/IRJ.2024.142.11.3

Conflict of Interest

None declared.

Review

International Research Journal Reviewers Community
DOI: https://doi.org/10.23670/IRJ.2024.142.11.3

Список литературы / References

1. Стригунов В.В. Исследование методов криптоанализа алгоритма RSA / В.В. Стригунов // Дневник науки. — 2020. — № 5 (41). — С. 34.
2. Reza F. Securing Wireless Sensor Networks Against Denial-of-Sleep Attacks Using RSA Cryptography Algorithm and Interlock Protocol / F. Reza // International Journal of Communication Systems. — 2019. — Vol. 33. — Iss. 4. — P. 34-39.
3. Malik Z. Cryptanalysis and improvement of blind signcryption scheme based on elliptic curve / Z. Malik // Electronics Letters. — 2019. — Vol. 55. — Iss. 8. — P. 113-119.
4. Петренко А.С. Метод оценивания квантовой устойчивости блокчейн-платформ / А.С. Петренко // Вопросы кибербезопасности. — 2022. — № 3 (49). — С. 2-22.
5. Ясашный О.П. Программная реализация генетического алгоритма на основе модели Голдберга с анализом его применения в криптографии / О.П. Ясашный // Молодой исследователь Дона. — 2022. — № 6 (39). — С. 79-83.
6. Vijesh B. Lightweight cryptographic algorithms based on different model architectures: A systematic review and futuristic applications / B. Vijesh // Concurrency and Computation: Practice and Experience. — 2022. — Vol. 35. — Iss. 1. — P. 156-164.
7. Ожиганова М.И. Оценка возможностей квантовых алгоритмов криптоанализа / М.И. Ожиганова // Защита информации. Инсайд. — 2021. — № 6 (102). — С. 70-82.
8. Абелян В.З. Криптографический алгоритм RSA / В.З. Абелян // International Journal of Advanced Studies in Computer Engineering. — 2020. — № 1. — С. 4-10.
9. Abdullah A. Cloud computing platform: Performance analysis of prominent cryptographic algorithms / A. Abdullah // Concurrency and Computation: Practice and Experience. — 2022. — Vol. 34. — Iss. 15. — P. 56-59.
10. Кочкаров Э.Р. Описание современных методов криптоанализа для взлома криптографического алгоритма с открытым ключом RSA / Э.Р. Кочкаров // Развитие и актуальные вопросы современной науки. — 2018. — № 5 (12). — С. 30-34.

Список литературы на английском языке / References in English

1. Strigunov V.V. Issledovanie metodov kriptoanaliza algoritma RSA [Research of methods of cryptanalysis of the RSA algorithm] / V.V. Strigunov // Dnevnik nauki [Diary of Science]. — 2020. — № 5 (41). — P. 34. [in Russian]
2. Reza F. Securing Wireless Sensor Networks Against Denial-of-Sleep Attacks Using RSA Cryptography Algorithm and Interlock Protocol / F. Reza // International Journal of Communication Systems. — 2019. — Vol. 33. — Iss. 4. — P. 34-39.
3. Malik Z. Cryptanalysis and improvement of blind signcryption scheme based on elliptic curve / Z. Malik // Electronics Letters. — 2019. — Vol. 55. — Iss. 8. — P. 113-119.
4. Petrenko A.S. Metod ocenivanija kvantovoj ustojchivosti blokchejn-platform [Method for assessing the quantum stability of blockchain platforms] / A.S. Petrenko // Voprosy kiberbezopasnosti [Issues of cybersecurity]. — 2022. — № 3 (49). — P. 2-22. [in Russian]
5. Jasashnyj O.P. Programmnaja realizacija geneticheskogo algoritma na osnove modeli Goldberga s analizom ego primenenija v kriptografii [Software implementation of a genetic algorithm based on the Goldberg model with an analysis of its application in cryptography] / O.P. Jasashnyj // Molodoj issledovatel' Dona [Young Don Researcher]. — 2022. — № 6 (39). — P. 79-83. [in Russian]
6. Vijesh B. Lightweight cryptographic algorithms based on different model architectures: A systematic review and futuristic applications / B. Vijesh // Concurrency and Computation: Practice and Experience. — 2022. — Vol. 35. — Iss. 1. — P. 156-164.
7. Petrenko A.S. Ocenka vozmozhnostej kvantovyh algoritmov kriptoanaliza [Assessing the capabilities of quantum cryptanalysis algorithms] / A.S. Petrenko // Zashhita informacii. Insajd [Information Protection. Insider] — 2021. — № 6 (102). — P. 70-82. [in Russian]
8. Abeljan V.Z. Kriptograficheskij algoritm RSA [RSA cryptographic algorithm] / V.Z. Abeljan // International Journal of Advanced Studies in Computer Engineering. — 2020. — № 1. — P. 4-10. [in Russian]
9. Abdullah A. Cloud computing platform: Performance analysis of prominent cryptographic algorithms / A. Abdullah // Concurrency and Computation: Practice and Experience. — 2022. — Vol. 34. — Iss. 15. — P. 56-59.

10. Kochkarov Je.R. Opisanie sovremennyh metodov kriptoanaliza dlja vzloma kriptograficheskogo algoritma c otkrytym kljuchom RSA [Description of modern cryptanalysis methods for breaking the RSA public key cryptographic algorithm] / Je.R. Kochkarov // Razvitie i aktual'nye voprosy sovremennoj nauki [Development and current issues of modern science]. — 2018. — № 5 (12). — P. 30-34. [in Russian]