Юсупов Александр Олегович
студент
Бачонаев Абдулло Дилдорович
студент
Научный руководитель
Сергеев Александр Эдуардович
канд. физ.-мат. наук, доцент

ФГБОУ ВО «Кубанский государственный аграрный университет им. И.Т. Трубилина»
г. Краснодар, Краснодарский край

ПРОСТЫЕ ЧИСЛА КАК СТРАЖИ ИНТЕРНЕТА: МАТЕМАТИЧЕСКИЕ ОСНОВЫ RSA-ШИФРОВАНИЯ

Аннотация: *в статье исследуются вопросы математических основ криптографического алгоритма RSA, базирующегося на свойствах простых чисел, функции Эйлера и модульной арифметики. Рассматривается формальная корректность алгоритма, вычислительная сложность лежащих в его основе задач, а также приводится детальный числовой пример и анализ современных требований к практической реализации. Особое внимание уделяется теоретическим аспектам, определяющим криптостойкость RSA, и инженерным решениям, обеспечивающие его надежность в реальных системах.*

Ключевые слова: *криптография, RSA, простые числа, теория чисел, функция Эйлера, модульная арифметика, асимметричное шифрование, криптостойкость, стандарты шифрования.*

Развитие информационных технологий привело к необходимости надежной защиты данных, передаваемых по открытым каналам связи. Криптография, опирающаяся на строгие математические методы, стала ключевым инструментом обеспе-

чения конфиденциальности и целостности информации. Одним из наиболее значимых достижений в данной области является алгоритм RSA, предложенный в конце XX века и до настоящего времени сохраняющий практическую актуальность.

До появления криптосистем с открытым ключом основой защиты информации являлись симметричные шифры, требующие предварительного обмена секретным ключом. С увеличением масштабов сетевого взаимодействия такая модель стала трудно реализуемой. Идея асимметричного шифрования позволила устранить данное ограничение за счет использования математических задач с выраженной вычислительной асимметрией.

Алгоритм RSA основан на фундаментальных результатах теории чисел. В частности, ключевую роль играют простые числа и свойства взаимной простоты. Простыми называются натуральные числа, имеющие ровно два различных делителя: единицу и само число. Именно их уникальные арифметические свойства делают возможным построение криптографически стойких систем. Эта «уникальность» кажется достаточно очевидной, однако именно на ней строится стойкость RSA: легко умножить два больших простых числа, но крайней трудно разложить их произведение обратно на множители. Данная задача является факторизацией, и она считается вычислительно сложной для современных компьютеров, если числа достаточно велики.

Для генерации ключей выбираются два больших простых числа p и q. На их основе вычисляется составное число $n = p \cdot q$, которое используется в качестве модуля для всех дальнейших операций. При этом знание n не позволяет эффективно восстановить значения p и q, что связано с вычислительной сложностью задачи факторизации.

Следующим шагом является вычисление функции Эйлера $\varphi(n)$. Для произведения двух простых чисел она имеет вид $\varphi(n) = (p - 1)(q - 1)$. Данная функция определяет количество чисел, взаимно простых с n, поэтому играет центральную роль в доказательстве корректности RSA.

Теорема Эйлера утверждает, что для любого целого числа a, взаимно простого с n, выполняется сравнение $a^{\varphi(n)} \equiv 1 \pmod{n}$. Эта теорема является

обобщением малой теоремы Ферма и служит теоретическим фундаментом алгоритма RSA.

Открытая экспонента e выбирается таким образом, чтобы gcd(e, φ(n)) = 1. Секретная экспонента d определяется из условия ed ≡ 1 (mod φ(n)). Существование такого числа d гарантируется тем, что e и φ(n) взаимно просты, а его нахождение осуществляется с помощью расширенного алгоритма Евклида.

Корректность алгоритма RSA заключается в том, что операция дешифрования является обратной операции шифрования. Пусть исходное сообщение представлено числом m. Тогда шифртекст имеет вид c ≡ m^e (mod n), а результат дешифрования вычисляется как m' ≡ c^d (mod n).

С учетом равенства ed = 1 + kφ(n) для некоторого целого k получаем m' ≡ m^{1+kφ(n)} ≡ m·(m^{φ(n)})^k (mod n). Согласно теореме Эйлера, при взаимной простоте m и n выполняется m^{φ(n)} ≡ 1 (mod n), что приводит к равенству m' ≡ m (mod n).

Криптостойкость RSA основана на вычислительной сложности задачи факторизации больших чисел. Современные алгоритмы разложения, включая решето числового поля, имеют субэкспоненциальную сложность, что делает факторизацию чисел длиной в несколько тысяч бит практически невыполнимой.

Следует отметить, что операции модульного возведения в степень, используемые в RSA, могут быть эффективно реализованы с помощью алгоритмов быстрого возведения в степень, что обеспечивает приемлемую производительность даже при больших размерах ключей.

Развитие квантовых вычислений ставит под вопрос долгосрочную безопасность RSA. Алгоритм Шора теоретически позволяет факторизовать большие числа за полиномиальное время. Тем не менее на сегодняшний день практическая реализация квантовых компьютеров достаточной мощности остается недостижимой.

В заключение отметим, что RSA является наглядным примером успешного применения абстрактных математических теорий в прикладных задачах. Простые числа и модульная арифметика, изучаемые в рамках классической теории

чисел, легли в основу одной из наиболее важных технологий современной информационной безопасности.

Список литературы

1. Rivest R.L. A Method for Obtaining Digital Signatures and Public-Key Cryptosystems / R.L. Rivest, A. Shamir, L. Adleman // Communications of the ACM. – 1978. – Vol. 21. No. 2. – P. 120–126.

2. Menezes A.J. Handbook of Applied Cryptography / A.J. Menezes, P.C. van Oorschot, S.A. Vanstone. – Boca Raton: CRC Press, 1996. EDN JWJYHB

3. Khan Academy. Modular arithmetic and RSA cryptography [Electronic resource]. – Access mode: https://www.khanacademy.org/computing/computer-science/cryptography/modern-crypt/v/rsa-encryption-part-1 (date of application: 28.01.2026).

4. Шнайер Б. Прикладная криптография: протоколы, алгоритмы и исходные тексты / Б. Шнайер. – М.: Диалектика, 2003.

5. Stallings W. Cryptography and Network Security: Principles and Practice / W. Stallings. – 7th ed. – Harlow: Pearson Education, 2017.

6. Rosen K.H. Elementary Number Theory and Its Applications / K.H. Rosen. – Boston: Pearson, 2011.