102. РОЛЬ ПРОСТЫХ ЧИСЕЛ В КРИПТОГРАФИЧЕСКОМ АЛГОРИТМЕ RSA

Щуцкая В.В, Павлюткина М.С, студенты гр.473901

Белорусский государственный университет информатики и радиоэлектроники
г. Минск, Республика Беларусь

Русина Н.В. – ст. преп., каф. ЭИ

Аннотация. В статье рассматривается роль простых чисел в алгоритме RSA — фундаментальной асимметричной криптосистеме. Описаны этапы генерации ключей, методы шифрования и расшифровки. Особое внимание уделено криптографическим требованиям к простым числам, способам их генерации и влиянию на устойчивость алгоритма. Также приведены типичные уязвимости, возникающие при использовании слабых или предсказуемых простых чисел. Подчёркивается важность правильного выбора простых чисел для обеспечения безопасности RSA на фоне современных угроз, включая развитие квантовых вычислений.

Ключевые слова. RSA, криптография, асимметричное шифрование, простые числа, факторизация, генерация ключей, криптостойкость, тест Миллера–Рабина, атаки на RSA, квантовые вычисления.

Алгоритм RSA, разработанный Ривестом, Шамиром и Адлеманом в 1978 году, является фундаментальной асимметричной криптосистемой, применяемой для защиты данных, цифровых подписей и безопасного обмена ключами. Его надежность базируется на вычислительной сложности разложения на множители больших целых чисел, в частности — произведения двух крупных простых чисел. В данной работе исследуется значение простых чисел в RSA, критерии их выбора и влияние на криптографическую устойчивость алгоритма.

Принцип работы алгоритма RSA

RSA относится к классу асимметричных алгоритмов шифрования, использующих пару ключей: открытый (публичный) и закрытый (приватный). Процесс работы RSA можно разделить на три основных этапа:

1. Формирование ключевой пары
2. Процедура шифрования данных
3. Процедура расшифровки данных

Генерация ключевой пары

1. Выбираются два различных больших простых числа p и q.
2. Вычисляется их произведение:

$$n = p \times q \tag{1}$$

Число n называется модулем и является частью открытого и закрытого ключей.

3. Вычисляется функция Эйлера:

$$\phi(n) = (p-1) \times (q-1) \tag{2}$$

Выбирается целое число e (открытая экспонента), такое что:

$$1 < e < \phi(n) \text{ и } \text{НОД}(e, \phi(n)) = 1 \tag{3}$$

4. Вычисляется число d (закрытая экспонента) — мультипликативно обратное к e по модулю ϕ(n):

$$d = e^{-1} \times \text{mod}(\phi(\text{n})) \tag{4}$$

Открытый ключ: (e, n)
Закрытый ключ: (d, n)

Шифрование и дешифрование

• Шифрование: сообщение m (в виде числа) шифруется как:

$$\text{c}=\text{m}^{e} \times \text{mod}(\text{n}) \tag{5}$$

• Дешифрование: зашифрованное сообщение c расшифровывается как:

$$m = c^{d} \times mod(n) \tag{6}$$

Роль простых чисел в RSA

Криптостойкость и проблема факторизации

Устойчивость RSA к взлому основывается на вычислительной сложности факторизации — задачи разложения модуля n на исходные простые множители p и q. Несмотря на существование эффективных алгоритмов (например, метода квадратичного решета или общего решета числового поля), факторизация чисел длиной более 1024 бит остается практически неосуществимой при современных вычислительных мощностях.

Выбор простых чисел

Для обеспечения безопасности:

• p и q должны быть большими (не менее 512 бит каждый для стойкости в 1024 бита).

• Они не должны быть близкими друг к другу, иначе n можно быстро факторизовать методом Ферма.

• (p − 1) и (q − 1) должны иметь большие простые делители, чтобы противостоять атаке Полларда.

• Простые числа должны быть сильными (strong primes), то есть удовлетворять дополнительным условиям криптостойкости.

Методы генерации простых чисел

Поскольку проверка простоты больших чисел является ресурсоемкой задачей, на практике применяются вероятностные тесты:

- Тест Миллера–Рабина (наиболее распространен благодаря высокой эффективности)
- Тест Соловея–Штрассена

Детерминированные методы (например, решето Эратосфена) не используются из-за их вычислительной неэффективности для больших чисел.

Атаки на RSA, связанные с простыми числами

1. Факторизация n – если злоумышленник найдет p и q, он сможет вычислить d.
2. Атака на слабые простые числа – если p или q малы или имеют предсказуемую структуру, их можно подобрать перебором.
3. Атака по времени – анализ времени выполнения операций может раскрыть ключи.

Современные вызовы и применение RSA

С появлением квантовых вычислений криптостойкость RSA может оказаться под угрозой. Алгоритм Шора, предназначенный для квантовых компьютеров, способен эффективно выполнять факторизацию больших чисел, что напрямую угрожает безопасности RSA. Это стало стимулом для развития постквантовой криптографии — криптосистем, устойчивых к атакам с использованием квантовых технологий.

Несмотря на потенциальные угрозы, RSA по-прежнему широко используется в реальных приложениях. Примеры включают:

– Протокол HTTPS (в связке с TLS) для защиты веб-трафика;

– Цифровые подписи в электронной почте (например, с использованием PGP/GPG);

– Защита программного обеспечения от подделки (электронные лицензии, верификация подписи кода);

– Аутентификация в VPN-системах и защищённых каналах связи.

Благодаря простоте реализации и высоким стандартам безопасности RSA остаётся ключевым элементом в арсенале современной криптографии.

Заключение

Простые числа служат основой криптографической стойкости алгоритма RSA. Их корректный подбор и генерация напрямую влияют на безопасность всей системы. Современные стандарты шифрования требуют использования достаточно больших и случайных простых чисел, устойчивых к известным методам факторизации. В условиях стремительного развития технологий особенно актуален вопрос регулярного обновления криптографических протоколов. Поэтому понимание роли простых чисел в RSA становится не только теоретически значимым, но и практически необходимым для специалистов в области информационной безопасности. Однако с развитием квантовых вычислений и появлением алгоритма Шора традиционные реализации RSA могут потребовать модификации или замены на постквантовые криптосистемы. Тем не менее, на сегодняшний день RSA остается одним из самых надежных и широко применяемых алгоритмов асимметричного шифрования.

Список литературы

1.Rivest, R., Shamir, A., Adleman, L. (1978). A Method for Obtaining Digital Signatures and Public-Key Cryptosystems.
2.Menezes, A., van Oorschot, P., Vanstone, S. (1996). Handbook of Applied Cryptography.
3.Boneh, D. (1999). Twenty Years of Attacks on the RSA Cryptosystem.