89. АЛГОРИТМ RSA: МАТЕМАТИЧЕСКИЕ ОСНОВЫ, РЕАЛИЗАЦИЯ И КРИПТОСТОЙКОСТЬ

Лагутинова О.А.

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

Русина Н. В. – ст. преп. каф. ЭИ

Работа посвящена криптографической системе RSA. Рассмотрены исторические предпосылки, математические основы, процесс генерации ключей с практическим примером и анализ уязвимостей, таких как атака Винера и повторное использование модуля. Обсуждаются современные угрозы, связанные с квантовыми вычислениями и методами факторизации, а также даны рекомендации по повышению безопасности.

Асимметричный шифр RSA – один из первых криптографических алгоритмов. Он был изобретён в 1977 году тремя учёными из Массачусетского технологического института (MIT): Рональдом Ривестом, Ади Шамиром и Леонардом Адлеманом (Rivest–Shamir–Adleman) и до сих пор занимает лидирующую позицию среди криптографических систем.

До появления RSA в криптографии использовались только симметричные шифры, что создавало проблему безопасного обмена ключами. В 1976 году Уитфилд Диффи и Мартин Хеллман предложили концепцию криптографии с открытым ключом, включающую протокол обмена ключами, однако их идея не содержала конкретного алгоритма для шифрования данных. В 1977 году Ривест, Шамир и Адлеман произвели фурор в мире криптографии, представив алгоритм RSA. Его основа зиждется на двух

ключевых математических принципах: использовании функции Эйлера и теореме Эйлера, а также на свойствах модульной арифметики.

Все операции выполняются по модулю n, где n=p*q, а p и q — большие простые числа. Это создает простоту и безопасность использования, а именно: само число n взять легко, однако простые множители найти достаточно сложно. На этом чудеса математики не заканчиваются. Еще одной важной составляющие являются теорема и функция великого математика Эйлера. Функция Эйлера (рисунок 1) используется для нахождения количества чисел взаимно простых с n

$$\varphi(n) = n \cdot \sum_{\alpha|n} \frac{\mu(\alpha)}{\alpha}$$

и используется для генерации ключей. То есть данная формула в нашем контексте будет выглядеть так: $\phi(n)=(p-1)(q-1)$.

Но на этом помощь Эйлера не заканчивается: в ход идет его Теорема. Она гласит: если

Если *a* и *n* взаимно просты, то(рис.2):

$$a^{\varphi(m)} \equiv 1 \pmod{m}$$

Где φ- уже известная функция Эйлера. Это свойство является основой в корректности шифрования.

Как же происходит генерация ключей. Возьмем один из самых известных примеров: p=7, *q*=11

Тогда n=p*q=77. Далее находим функцию Эйлера: $\phi(n)= (7-1) (11-1)=60$.

Дальше появляются дополнительные переменные: открытая экспонента (e) и закрытая экспонента (d).Где e взаимно простое с $\phi(n)$.Чаще всего берут 65537, по причине того, что оно большое, простое и удобно для вычисления .В нашем примере возьмем e=17 так как НОД (17,60) =1. И так мы нашли ключ для шифрования нашего сообщения(e,n). Теперь найдем ключ для его дешифровки Для нахождения d используется расширенный алгоритм Евклида, решающий уравнение:

17d ≡ 1 (mod 60).

В результате получаем d = 53, так как 17×53 = 901 и 901 (mod 60) = 1. Теперь у нас есть ключи для расшифровки (d, n).

Криптографическая значимость RSA.

Несмотря на высокую надежность алгоритма RSA, он подвержен ряду атак. Одна из таких угроз — атака Винера, которая использует уязвимость при малых зна чениях закрытой экспоненты d. Если d слишком мало, злоумышленник может восстановить его, анализируя отношение открытой экспоненты e и модуля n с помощью непрерывных дробей. Этот метод оказывается эффективным, если e приближается к значению функции Эйлера φ(n). Для предотвращения атаки рекомендуется выбирать d ≥ 2n и избегать чрезмерно больших значений e, придерживаясь стандартных параметров, например, e = 65537.

Другой распространенной угрозой является атака повторного использования модуля. Она возникает, когда один и тот же модуль n применяется разными пользователями с различными открытыми экспонентами e_1 и e_2. Если эти экспоненты взаимно просты, злоумышленник может воспользоваться двумя шифротекстами c_1 = m^{e_1} mod n и c_2 = m^{e_2} mod n для восстановления исходного сообщения m с помощью расширенного алгоритма Евклида. Чтобы минимизировать риск, необходимо использовать уникальные модули n для каждого пользователя и применять вероятностные схемы дополнения, например, OAEP, гарантирующие уникальность каждого шифротекста.

Алгоритм RSA также широко применяется в Microsoft Authenticode для цифровой подписи исполняемых файлов, таких как .exe и .dll, обеспечивая их аутентичность и целостность. Процесс включает генерацию пары ключей RSA, где приватный ключ используется для шифрования хеша файла, например, SHA-256, создавая цифровую подпись. Эта подпись затем встраивается в файл вместе с сертификатом, выданным доверенным центром сертификации. При запуске Windows проверяет подпись, расшифровывая ее публичным ключом из сертификата, и сравнивает хеш для подтверждения неизменности содержимого. Если подпись недействительна или отсутствует, система предупреждает пользователя сообщением «Неизвестный издатель», предотвращая подделку программного обеспечения и внедрение вредоносного кода.

На протяжении многих лет RSA был универсальным, простым в использовании и довольно надёжным. Однако с развитием квантовых вычислений (например, с появлением алгоритма Шора) и совершенствованием классических методов факторизации (таких как GNFS) стойкость RSA снижается. Поэтому в современных системах рекомендуется использовать ключи длиной не менее 2048 бит.

Список использованных источников:

1.Menezes, A. J., van Oorschot, P. C., & Vanstone, S. A. СПРАВОЧНИК ПРИМЕНИМОЙ КРИПТОГРАФИИ / Menezes, A. J., van Oorschot, P. C., Vanstone, S. A. // CRC Press, 1996. – С. 1–805.

2.Rivest, R. L., Shamir, A., & Adleman, L. МЕТОД ПОЛУЧЕНИЯ ЦИФРОВЫХ ПОДПИСЕЙ И КРИПТОСИСТЕМ С ОТКРЫТЫМ КЛЮЧОМ / Rivest, R. L., Shamir, A., Adleman, L. // Communications of the ACM, 1978. – Vol. 21. №2. – doi: 10.1145/359340.359342.

3.RFC 8017: PKCS #1: СПЕЦИФИКАЦИИ RSA-КРИПТОГРАФИИ // RFC Editor, 2016. – С. 1–64.

4.Stallings, W. Криптография и сетевая безопасность / Stallings, W. – Pearson Education, 2017. – С. 1–857.