Алгоритм асимметричного шифрования RSA с использованием функции бинарного возведения в степень по модулю

Розенберг Алексей Светославович
9 класс, МАОУ «Лицей №38» Советского района г. Нижнего Новгорода
Научный руководитель: Куликова Светлана Юрьевна,
учитель математики высшей квалификационной категории, ОАНО «Школа «Летово», г.Москва

В работе была выдвинута гипотеза о прямо пропорциональной зависимости скорости работы шифровального алгоритма RSA от длины ключа. Для исследования зависимости от различных параметров была написана имплементация алгоритма с использованием функции бинарного возведения в степень по модулю, с помощью которой была проведена серия тестирований подсчета времени выполнения алгоритма от количества бит ключей. По полученным данным был составлен график зависимости времени работы криптосистемы от размера ключа, подтвердивший предположение.

В наше время шифрование, а в особенности асимметричное, может быть крайне полезно в области компьютерных технологий. Сейчас все крупные корпорации пользуются теми или иными методами шифрования данных для защиты своего продукта от взлома. Криптосистема RSA используется в таких протоколах, как PGP, S/MIME, TLS/SSL, IPSEC/IKE и других [1].

В своей работе я хотел изучить данную криптосистему, скорость ее работы и сложность реализации для возможного дальнейшего использования другими программистами. Поэтому я разработал свою имплементацию улучшенной версии алгоритма RSA с использованием функции бинарного возведения в степень, а также попытался найти от чего зависит скорость работы алгоритма. Цель моей работы – разработать программу шифрования и дешифрования на основе алгоритма RSA и функции бинарного возведения в степень и проверка с помощью данной программы выдвинутой в работе гипотезы.

Криптосистема RSA основана на вычислительной сложности задачи факторизации больших целых чисел. Ее уникальность также заключается в том, что это асимметричный криптографический алгоритм. Моя гипотеза заключается в том, что скорость шифрования сообщения линейна по количеству бит открытого ключа. Аналогично, скорость шифрования RSA линейна по длине открытого. Это объясняется тем, что при шифровании и дешифровании сообщения используется функция возведения в степень, в которой ключи выполняют роль показателей этих степеней. [2]

Принцип работы данной криптосистемы следующий [3]: выбираются два случайных простых числа p и q с большим количеством цифр. Затем эти числа перемножаются; полученное число n оставляется, а простые числа «прячутся» от посторонних лиц. Далее при помощи функции Эйлера, которая зависит от знания факторизации числа n, вычисляем ее результат по формуле:

$$\varphi(p,q) = (p-1)(q-1)$$

Затем подбираются открытый и закрытый ключи. Открытый ключ e должен быть взаимно простым с φ. Затем выбирается закрытый ключ d. Для этого используется теорема Эйлера, которая в данном примере будет выглядеть как

$$m^{\varphi(n)} \equiv 1 \ (mod\ n)$$ [4]

Из нее следует, что $e * d = \varphi(n) + 1$, из которого выражается d.

Для шифрования и дешифрования сообщения используется односторонняя функция возведения числа в степень по модулю. При зашифровке сообщения оно возводится в степень e по модулю n, тогда как при расшифровке получившееся зашифрованное письмо возводится в степень d по модулю n.

Моя версия RSA отличается от изначальной наличием в ней функции быстрого, или бинарного, возведения в степень по модулю. Ее суть заключается в разбиении на множители показателя степени. Так возведение происходит гораздо быстрее, так как количество операций умножения уменьшается. Данный алгоритм позволяет сократить время шифрования и дешифрования сообщения. Ускорять процесс вычисления ключей не имеет смысла, так как они он выполняется один раз в начале работы программы, в то время как кодирование и декодирование сообщения может проводиться многократно. Алгоритм описывается формулой:

$$a^n = \left(a^{\frac{n}{2}}\right)^2 = a^{\frac{n}{2}} * a^{\frac{n}{2}}$$

В результате серии тестирований я вывел следующие графики зависимости времени работы программы от количества бит ключа для кодирования и декодирования сообщения:

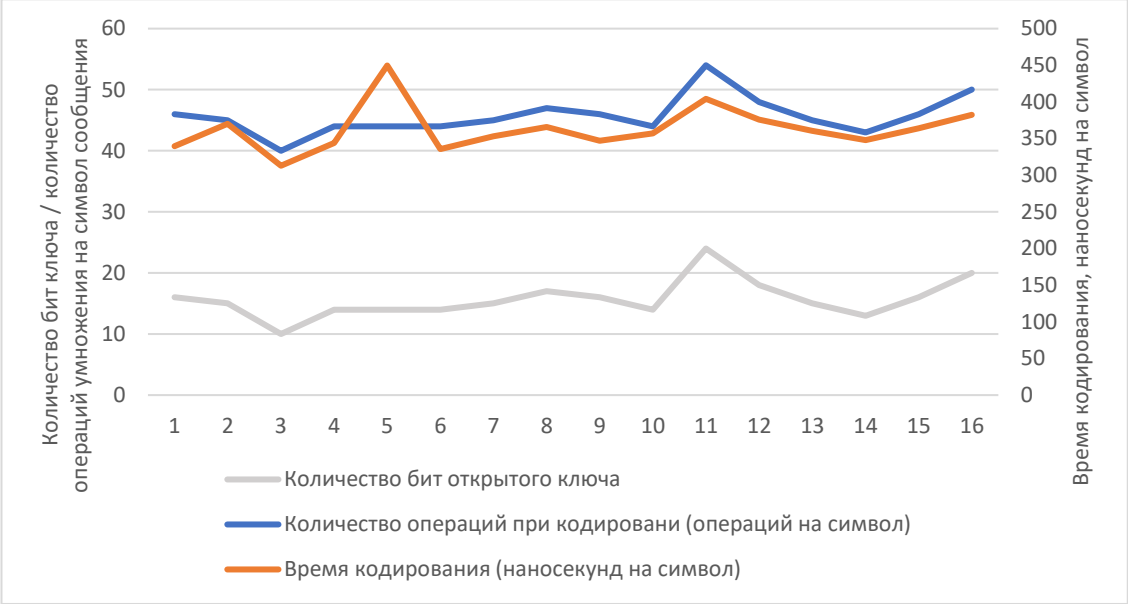

Рис. 1. Кодирование сообщения

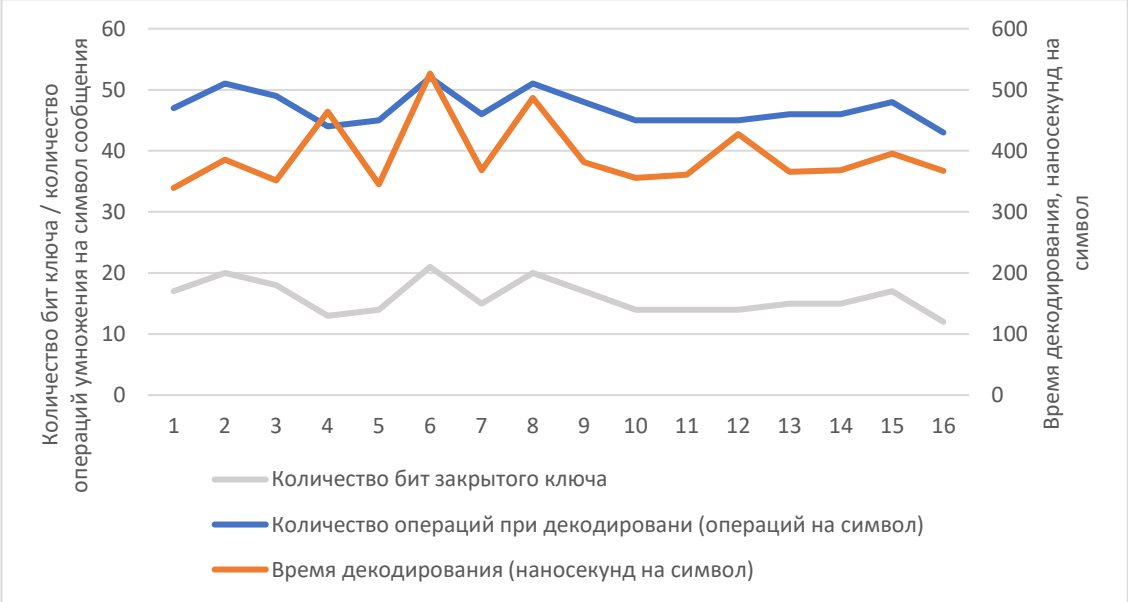

Рис. 2. Декодирование сообщения

Также построив графики зависимости количества операций от количества бит ключа можно увидеть прямо пропорциональную зависимость, значит можно утверждать, что гипотеза подтвердилась:

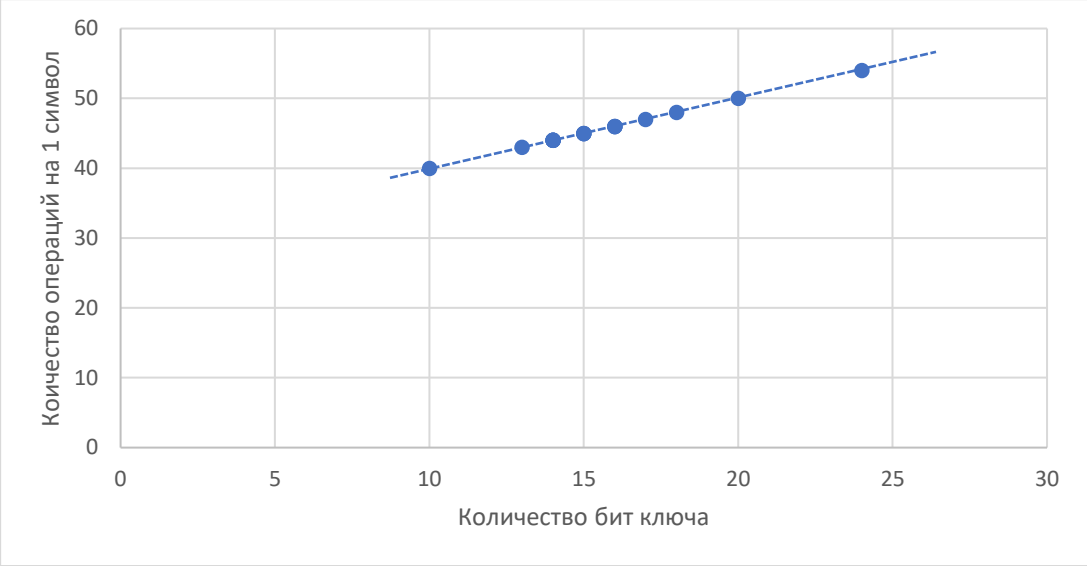

Рис. 3. Зависимость количества операций при кодировании от количества бит открытого ключа

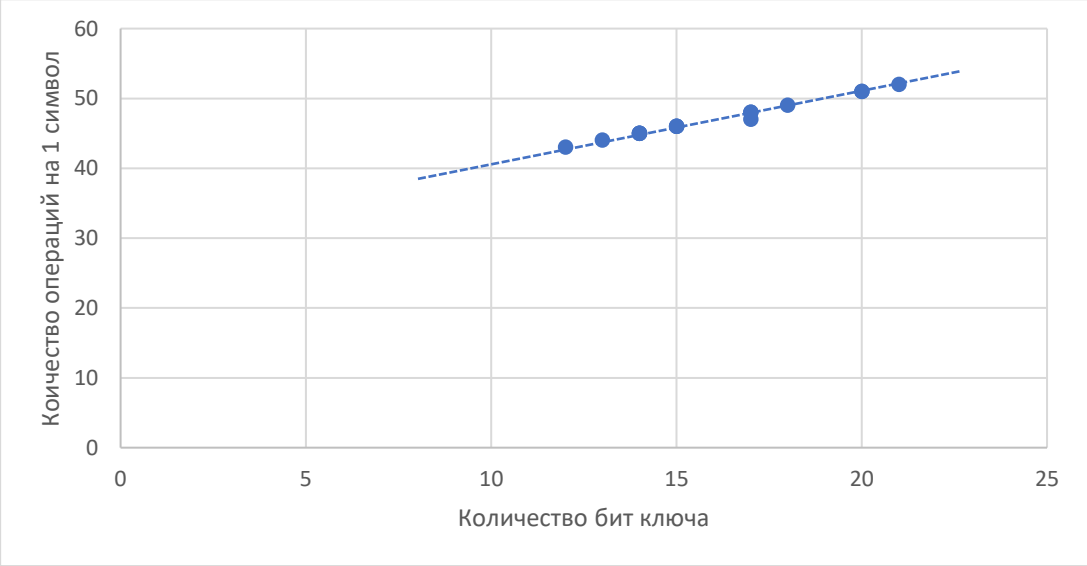

Рис. 4. Зависимость количества операций при декодировании от количества бит закрытого ключа

По итогам исследований, была найдена зависимость скорости работы программы от определенных параметров с помощью собственной имплементации алгоритма RSA с использованием функции бинарного возведения в степень по модулю.

Литература:

1. Bakhtiari M., Maarof M. A. Serious Security Weakness in RSA Cryptosystem // IJCSI — 2012. — Vol. 9, Iss. 1, No 3. — P. 175—178.
2. Rivest R., Shamir A., Adleman L. A method for obtaining digital signatures and public-key cryptosystems // Commun. ACM — NYC, USA: ACM, 1978. — Vol. 21, Iss. 2. — P. 120—126.
3. Menezes A. J., Oorschot P. v., Vanstone S. A. Handbook of Applied Cryptography — CRC Press, 1996. — 816 p.
4. Introduction to Modern Cryptography — CRC Press, 2015. — P. 411. — 583 p.