УДК 004.056.55

М.Е. Алёхов (5 курс, каф. ПМИ), Н.Е. Губенко(доцент каф. КСМ)

АНАЛИЗ И СРАВНЕНИЕ ЭФФЕКТИВНОСТИ АЛГОРИТМОВ ШИФРОВАНИЯ НА ЭЛЛИПТИЧЕСКИХ КРИВЫХ И RSA

Цель работы – оценка актуальности применения алгоритмов шифрования на эллиптических кривых (ECC), как замены для алгоритма RSA.

На сегодняшний день, защита информации является важной и актуальной проблемой не только для государственных структур или предприятий, но и для обычного пользователя персонального компьютера. В первую очередь, это связано с широким применением различного рода онлайн сервисов, таких как: социальные сети, управление счетами в банках, интернет магазины. Поэтому выдвигаются большие требования к стандартам шифрования, не только с точки зрения надёжности, но и с точки зрения скорости их выполнения на современном оборудовании. Длинна ключей применяемых алгоритмов шифрования постоянно растёт, в связи с этим, снижается их скорость. В такой ситуации становится важно сохранить скорость работы систем защиты, применяя более быстрые алгоритмы с эквивалентной степенью защиты.

Асимметричные алгоритмы построены на том, что существует два типа ключей: открытый и секретный. Не смотря на схожие принципы работы, их реализация сильно различается, поэтому важно определить критерии, на основе которых стоит сравнивать алгоритмы. Основным критерием оценки, при проведении анализа, было время, которое необходимо для шифрования и расшифровки блоков данных равной длинны.

При этом учитывался тот факт, что при равной длине ключа, сравниваемые алгоритмы имеют не одинаковую степень криптостойкости. Была выбрана эквивалентная длина ключа, равная 3072 бита для RSAи 256 бит для шифрования на эллиптической кривой. Такая длинна ключа является оптимальной на сегодняшний день для надёжной долгосрочной защиты информации. В таблице 1 представлены эквивалентные длины ключей для симметричных и асимметричных алгоритмов шифрования [1].

Таблица 1. Сравнение степени защиты для алгоритмов и размеров ключей

Степень защиты	Симметричный алгоритм	Минимальный размер ключа (в битах)	
		RSA	ECC
80	Skipjack	1024	160
112	3DES	2048	224
128	AES-128	3072	256
192	AES-192	7680	384
256	AES-256	15360	512

Ключи для RSAбыли сгенерированы собственной реализацией генератора ключей, публичная экспонента имеет длину 32 бита. В случае эллиптической кривой, использовалась кривая, рекомендуемая стандартом NIST,под названием P-256 [2].

RSAявляется одной из первых, используемых на практике, криптографических систем с открытым ключом. Основным направлением использования является безопасная передача данных, широко применяется взащищенном протоколе SSL. Данный алгоритм основывается на том факте, что разложение натурального числа на произведение простых множителей, является вычислительно сложной задачей, и на сегодняшний день алгоритмов, позволяющих эффективно выполнить такое разложение (факторизацию) нет [3].

Алгоритмы на эллиптических кривых основываются на том факте, что не существует быстрых алгоритмов для решения задачи дискретного логарифмирования в группах их точек. Сегодня известны лишьэкспоненциальные алгоритмы вычисления обратных функций для эллиптических кривых. По сравнению с субэкспоненциальными алгоритмамиразложения числа на простые сомножители (например, RSA), это позволяет уменьшить размер ключа, упростив, таким образом, программную и аппаратную реализацию криптосистем при одинаковом уровне стойкости [4].

В ходе выполнения исследования было реализовано тестовое приложение, позволяющее оценить время выполнения шифрования для сравниваемых алгоритмов. На рисунке 1 представлен график сравнения скорости шифрования блоков данных различной длины (от 16 до 256 байт).

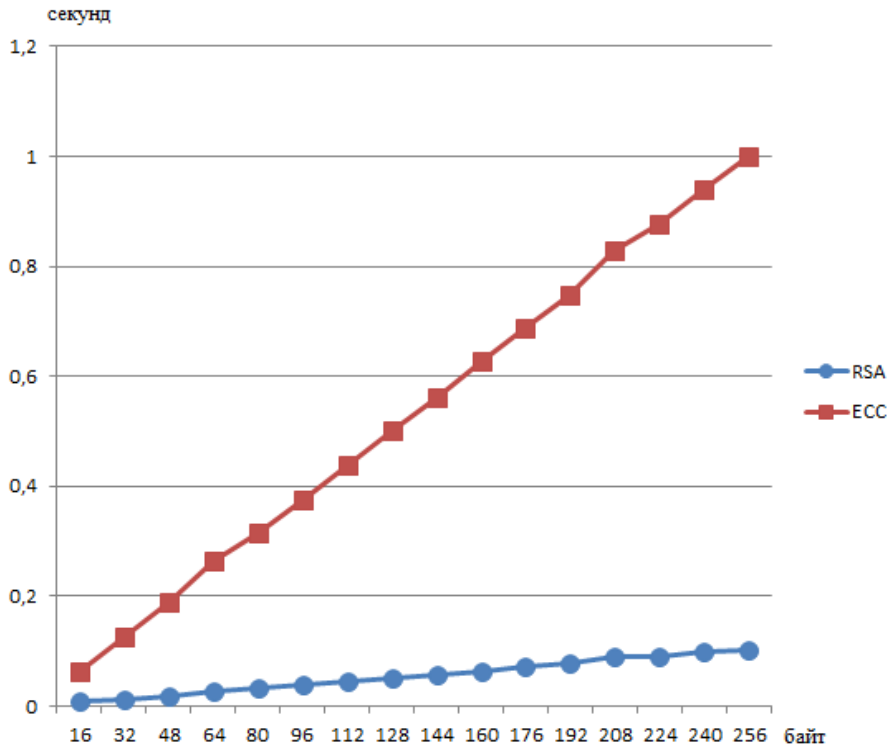

Рис. 1 Сравнение скорости шифрования данных

В результате сравнения скорости шифрования было установлено, что шифрование гораздо быстрее выполняется при использовании алгоритма RSA, для обработки сообщения в 256 байт понадобилось 0,1 секунды. Эллиптические кривые сильно проигрывают в данном случае, для обработки блока той же длины понадобилось 1 секунда, что в 10 раз превышает показатели RSA.

Для шифрования алгоритмом ECCнеобходимо выполнить гораздо большее количество математических операций, чем для RSA. Естественно, при увеличении длины публичной экспоненты скорость шифрования RSAбудет падать, но на практике редко применяют публичные экспоненты длиной более чем 32 бита.

Здесь стоит учитывать, что тестовое приложение, разработанное на языке программирования C# не имеет низкоуровневых оптимизаций для умножения и сложения точек кривой, что значительно понижает скорость шифрования. При использовании более производительных языков можно добиться ускорения в два и больше раз.

После оценки скорости шифрования, была проведена оценка скорости расшифровки блоков данных такого же размера, результат представлен на рисунке 2.

Хорошо виден значительный разрыв в скорости расшифровки, при этом RSA,в данном случае, работает медленнее, чем неоптимизированная реализация ECC. На расшифровку блока данных в 256 байт у RSA ушло 13 секунд, а для эллиптических кривых 1 секунда. В целом, при расшифровке, эллиптические кривые превосходят RSAпо скорости практически в 13 раз.

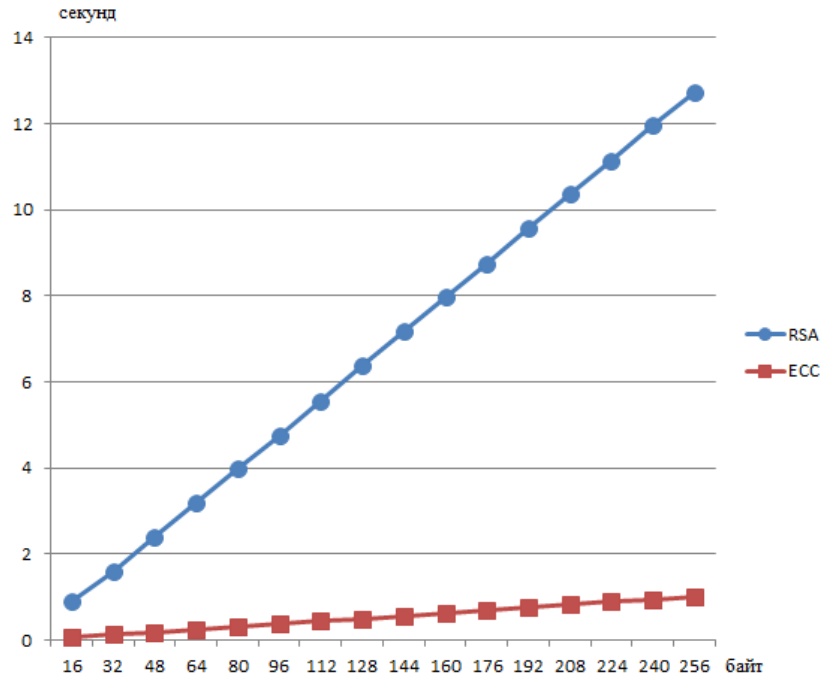

Рис.2 Сравнение скорости расшифровки данных

Результатами проведенного анализа алгоритмов шифрования на эллиптических кривых и RSAявляются данные измерения времени работы алгоритмов при шифровании и расшифровке блоков данных различной длины (от 16 до 256 байт). Исходя из полученных результатов можно сказать, что уже сегодня применение эллиптических кривых является актуальным.

Размеры ключей RSA хоть и увеличиваются пропорционально мощностям оборудования, не могут обеспечить той эффективности, которая достигается при использовании эллиптических кривых. Шифрование RSA 16 байтного блока данных, при использовании 15360 битного ключазаймёт много времени на современном процессоре, в это же время для эллиптической кривой с той же степенью защитыпонадобится ключ длиной всего 512 бит, который может быть обработан быстрее.

ЛИТЕРАТУРА:

1. RSA vs ECC Comparison for Embedded Systems. // Atmel. [Электронный ресурс]. –Режим доступа: http://www.atmel.com/images/atmel-8951-cryptoauth-rsa-ecc-comparison-embedded-systems-whitepaper.pdf
2. Recommended elliptic curves. // National Institute of Standards and Technology. [Электронный ресурс]. – Режим доступа: http://csrc.nist.gov/groups/ST/toolkit/ documents/dss/NISTReCur.pdf
3. RSA. // Материал из Википедии – свободной энциклопедии. [Электронный ресурс]. – Режим доступа: https://ru.wikipedia.org/wiki/RSA
4. Анисимов В.В. Шифрование с открытым ключом. // Информационный ресурс. [Электронный ресурс]. – Режим доступа: https://sites.google.com/site/anisimovkhv/learning/kripto/lecture/tema8#p85