УДК 003.26.09

ИССЛЕДОВАНИЕ МЕТОДОВ КРИПТОАНАЛИЗА АЛГОРИТМА RSA

Стригунов В.В.

к.ф.-м.н., доцент,

Тихоокеанский государственный университет,

Хабаровск, Россия

Щекина А. М.

старший разработчик,

ПАО «Мегафон»,

Санкт-Петербург, Россия

Аннотация

В статье рассматривается изучение реализации пяти методов криптоанализа алгоритма шифрования с открытым ключом RSA, для того чтобы выявить слабые стороны данного алгоритма, обобщить информацию по существующим методам криптоанализа данного алгоритма и провести сравнительный анализ этих методов для определения самого практичного.

Ключевые слова: криптоанализ, алгоритм RSA, факторизация целых чисел, атака Винера, атака Ван-Тилборга, атака Дюжелла, метод факторизации Ферма, алгоритм Гельфонда-Шенкса.

RESEARCH OF RSA ALGORITHM CRYPTO ANALYSIS METHODS

Strigunov V.V.

Ph.D., associate professor,

Pacific State University,

Khabarovsk, Russia

Shchekina A. M.
senior developer,
PJSC Megafon,
Saint-Petersburg, Russia

Annotation
The article discusses the study of the implementation of five methods of cryptanalysis of the RSA public key encryption algorithm in order to identify the weaknesses of this algorithm, summarize information on existing cryptanalysis methods of this algorithm and conduct a comparative analysis of these methods to determine the most practical.

Keywords: cryptanalysis, RSA algorithm, integer factorization, Wiener attack, Van Tilborg attack, Dujell attack, Fermat factorization method, Gelfond-Shanks algorithm.

Введение.

В рамках данной статьи в качестве объекта исследования был выбран алгоритм шифрования с открытым ключом RSA. В криптосистеме с открытым ключом, в отличие от симметричной, используются два ключа: открытый (может быть известен всем) и закрытый (хранится в секрете). Открытый ключ применяется для шифрования сообщений, а закрытый ключ – для их расшифровки. Криптостойкость данного алгоритма основана на сложности разложения больших целых чисел на множители.

Существует множество методов криптоанализа RSA, которые опираются на различные свойства этой криптосистемы [1; 2]. Эти методы достаточно подробно описаны в литературе. Целью данного исследования явилась программная реализация и анализ пяти существующих методов криптоанализа

алгоритма с открытым ключом RSA: атака Винера, атака Ван-Тилборга, атака Дюжелла, метод факторизации Ферма, алгоритм Гельфонда-Шенкса.

Исследование и тестирование методов криптоанализа RSA.

Реализация атак была запрограммирована на языке C++ с использованием библиотеки для арифметики больших чисел MPIR [3]. Данная библиотека была выбрана из-за удобства использования и относительной простоты сборки и подключения. В рамках проведения этапа тестирования реализованных атак выбирались разные значения входных данных, в зависимости от исследуемых свойств конкретного метода.

Для класса атак, основанных на малых значениях секретной экспоненты, очень важно правильно выбрать открытую экспоненту e, так как при ее малых значениях, секретная экспонента d не будет удовлетворять неравенству:

$$d \leq \frac{1}{3} N^{\frac{1}{4}}, \qquad (*)$$

где N – модуль алгоритма RSA.

Для атак Ван-Тилборга и Дюжелла также следует обратить внимание на выбор границы D [4; 5], от данного значения зависит время работы алгоритма, а также максимальное значение секретной экспоненты, которое может быть найдено. В табл. 1 приведены результаты тестирования атаки Винера, атаки Ван-Тилборга и атаки Дюжелла в зависимости от разных значений.

Таблица 1 – Результаты тестирования атак Винера, Ван-Тилборга, Дюжелла

e = 3594320245477, N = 7978886869909, d = 313					
Атака	Атака Винера	Атака Ван-Тилборга		Атака Дюжелла	
		D = 10^4	D = 10^8	D = 10^4	D = 10^8
Время работы, с	0,049	0,72	596,44	0,062	5,405
Значение предела d	560	168*10^5	168*10^9	168*10^5	168*10^9
e = 6792605526025, N = 9449868410449, d = 569					
Атака	Атака Винера	Атака Ван-Тилборга		Атака Дюжелла	
		D = 10^4	D = 10^8	D = 10^4	D = 10^8
Время работы, с	0,011	74,097	615,49	0,019	0,08
Значение предела d	584	175*10^5	175*10^9	175*10^5	175*10^9

e = 4603830998027, N = 7978886869909, d = 5936963					
Атака	Атака Винера	Атака Ван-Тилборга		Атака Дюжелла	
		D = 10^4	D = 10^8	D = 10^4	D = 10^8
Время работы, с	-	357,06	556,87	0,44	15,671
Значение предела d	560	168*10^5	168*10^9	168*10^5	168*10^9

По данным, приведенным в таблице, можно сделать следующие выводы:

– атака Винера является самой быстрой атакой, но не всегда находит значения секретной экспоненты даже если значение открытой экспоненты e соразмерно значению модуля N;

– увеличение максимально допустимой границы D, приводит к существенному увеличению времени работы алгоритма, но также расширяет границы поиска d;

– атака Дюжелла работает почти также быстро как атака Винера, но границы ее применения гораздо больше;

– граница применимости атак Ван-Тилборга и Дюжелла одинаковые, но атака Ван-Тилборга в несколько раз медленнее.

С точки зрения зависимости времени работы от размера модуля N тестирование показало, что в случае выбора секретной экспоненты, удовлетворяющей условию (*), взлом алгоритма RSA атакой Винера будет произведен за реальное время. На рис. 1 приведена диаграмма зависимости среднего времени работы атаки Винера от длины модуля N.

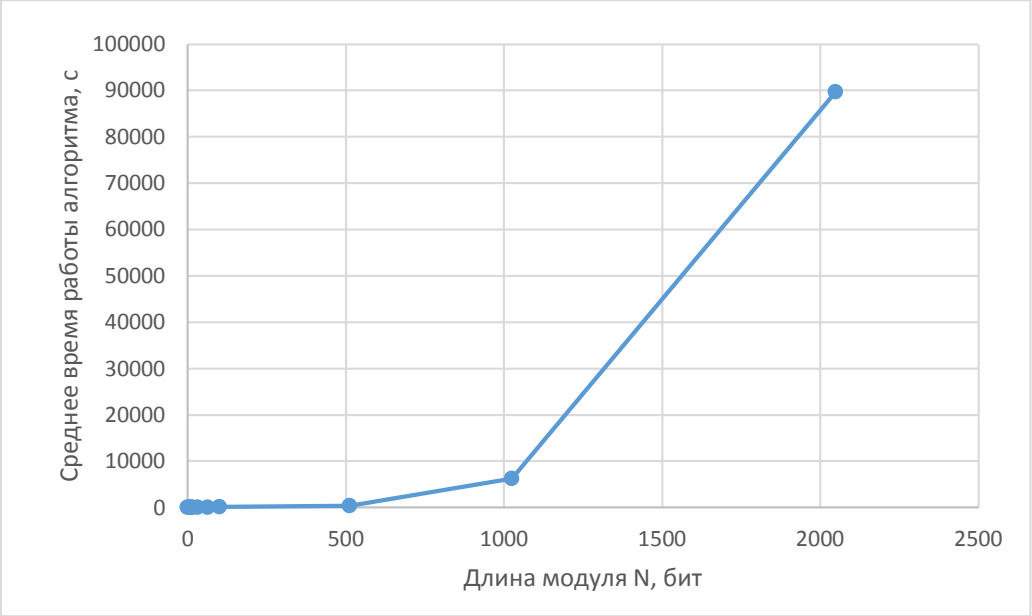

Рис. 1 – График зависимости скорости работы атаки Винера от длины модуля N

Атака Ван-Тилборга показала медленный результат работы даже при использовании модуля длиной тринадцать знаков, поэтому на больших числах данную атаку решено было не испытывать.

Время работы алгоритма Дюжелла также, как и время работы атаки Винера, экспоненциально возрастает при увеличении значения модуля N и для оптимально выбранного D в среднем примерно равно времени выполнения атаки Винера. Но для того, чтобы соотнести реальное время выполнения необходимо рассмотреть, как влияет значение предположительной границы D на продолжительность работы данного алгоритма. В табл. 2 представлены результаты тестирования атаки Дюжелла при разном выборе значения D.

Таблица 2 – Результаты тестирования атаки Дюжелла

D	Длина d, бит	Время, с
10^3	266	2
10^6	276	135
10^7	280	1500
10^8	283	17200

То есть для быстрой работы атаки Дюжелла необходимо сделать верное предположение каким будет значение секретной экспоненты d для корректного выбора значения D.

Таким, образом, атака Винера и атака Дюжелла показали приемлемый результат взлома алгоритма RSA при оптимальном выборе показателей, влияющих на их работу.

Для проведения тестирования атаки с помощью метода факторизации Ферма было выбрано фиксированное значение e = 65537, так как этот параметр не влияет на работу алгоритма. Затем выбирались различные значения модуля N, который зависит от значений его множителей p и q. В табл. 3 приведены результаты тестирования данной атаки в зависимости от разных значений p и q.

Таблица 3 – Результаты тестирования метода Ферма

p	q	$\lvert p-q\rvert$	N	$\sqrt{N}$	время, с
3559	3571	12	12709189	3565	0,003
317	115249	114932	36533933	6044	0,02
115249	270343	155094	31156760407	176512	0,012
3571	270343	266772	965394853	31070	0,057
15485867	32452867	16967000	502560782130689	22417867	0,695
452930459	433024253	19906206	196129873669422127	442865525	0,045
982451653	961748927	20702726	944871823102126331	972045175	0,025
1109	49979687	49978578	55427472883	235430	8,318
115249	179424673	179309424	20678514138577	4547363	29,312
270343	961748927	961478584	260002090171961	16124580	159,52

По данным, приведенным в табл. 3, можно сделать вывод, что время выполнения алгоритма действительно зависит от того насколько близки значения p и q и насколько значение одного из множителей близко к значению квадратного корня из N.

Также по результатам тестирования можно заметить, что алгоритм очень быстро работает для небольших чисел N, но для разложения больших чисел на множители он совершенно не приемлем. К примеру, разложение числа с пятнадцатью знаками выполняется за секунды, а разложение сороказначного

числа занимает более часа. На рис. 2 приведена диаграмма зависимости среднего времени работы алгоритма от длины модуля N.

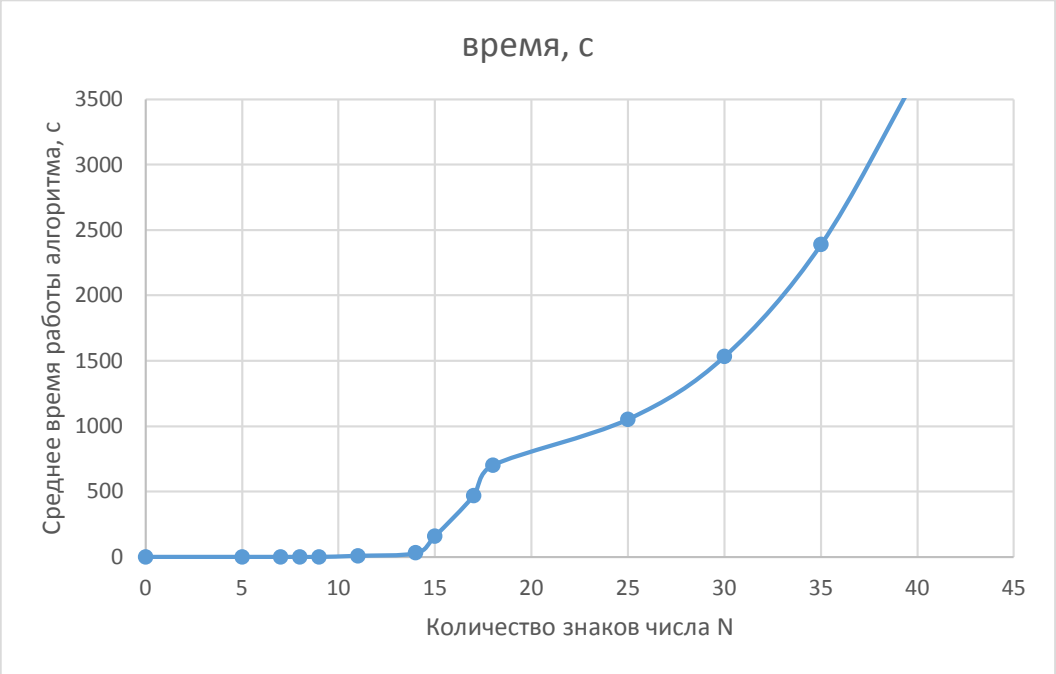

Рис. 2 – График зависимости скорости работы метода Ферма от длины модуля N

Для тестирования алгоритма с использованием метода Гельфонда-Шенкса также было выбрано фиксированное значение e = 65537, так как оно участвует только в шифровании выбранного исходного текста и на работу алгоритма в целом не влияет. Затем выбирались значения модуля N различной длины. В ходе тестирования было увидено, что от длины модуля N зависит только среднее время работы алгоритма. А в рамках тестирования чисел одной длины, например, для числа длиной 10 знаков, секретная экспонента была найдена в одном случае за секунду, а в другом за 382 секунды.

На рис. 3 приведена диаграмма зависимости среднего времени работы алгоритма от длины модуля N.

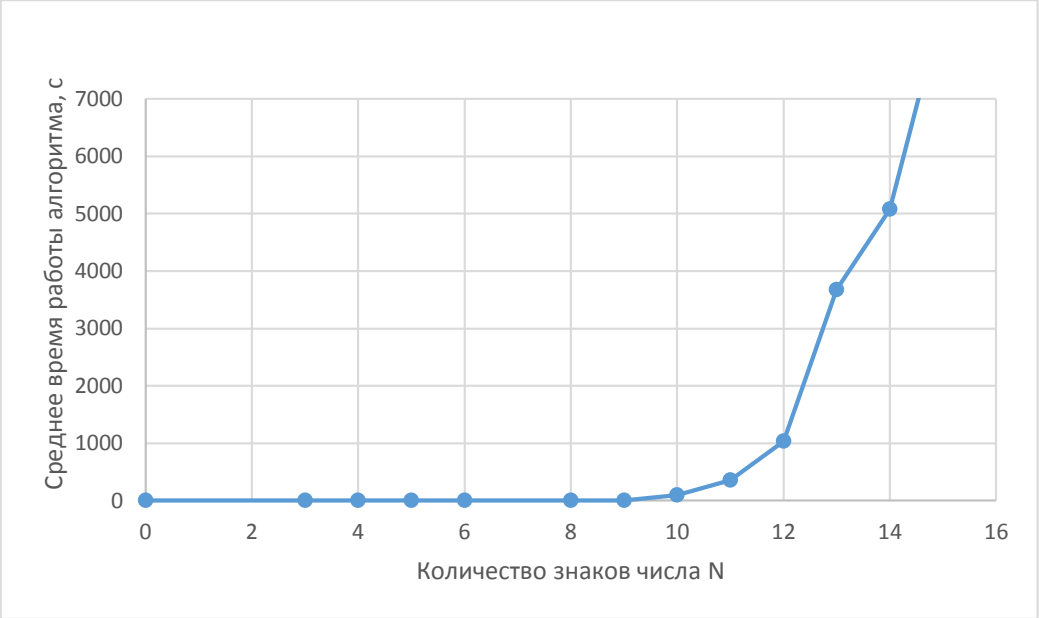

Рис. 3 – График зависимости скорости работы метода Гельфонда-Шенкса от длины модуля N

По результатам тестирования можно заметить, что алгоритм очень быстро работает для небольших чисел N, но для вычисления дискретного логарифма большого числа, данный метод в среднем работает даже медленнее чем метод факторизации Ферма.

Сравнительный анализ методов криптоанализа RSA.

Рассмотрим положительные и отрицательные стороны реализованных алгоритмов, выявленные в результате тестирования, соотнесем теоретические и практические данные и оценим практичность использования каждого из изученных методов.

В табл. 5 приведена сводная теоретическая информация, касающаяся максимально допустимого значения секретной экспоненты d и теоретического времени работы реализованных алгоритмов. Также для наглядности в данной таблице указаны практические данные, полученные при тестировании реализованных алгоритмов с входными данными: e = 6792605526025, N = 9449868410449.

Таблица 5 – Сравнение реализованных алгоритмов

Методы	Максимально допустимое значение d	Теоретическое время работы алгоритма	Практическое время работы алгоритма, с
Атака Винера	$d \leq (N\text{^}0.25)/3$	$O(lnN)$	0,011
Атака Ван-Тилборга	$d \leq DN\text{^}0.25$	$O(D^2A^2)$	74,097
Атака Дюжелла	$d \leq DN\text{^}0.25$	$O(D^2\,log\,A)$	0,019
Метод Ферма	d не ограничено	$O(N)$	0,47
Метод Гельфонда-Шенска	d не ограничено	$O(\sqrt{N})$	3767,5

Длина реального модуля алгоритма RSA на сегодняшний день составляет не менее 309 знаков (1024 бита) и время работы реализованных атак в разы больше времени, указанного в данной таблице. Также необходимо заметить, что в реальных системах шифрования RSA в большинстве случаев используются достаточно малые значения открытых экспонент, и, следовательно, большие значения секретных экспонент. То есть в общем случае ни одна из реализованных атак не сможет получить значения секретной экспоненты реального алгоритма RSA, что говорит о его криптостойкости.

Тем не менее, можно утверждать, что атака Винера является самой быстрой из рассматриваемых атак. Однако, данный метод найдет значение секретной экспоненты только в случае, если d будет удовлетворять неравенству (*). То есть, если реальное значение модуля RSA – 1024 бита, то значение d должно быть не превышать 256 бит.

Атака Ван-Тилборга и атака Дюжелла – это модификации атаки Винера, которые расширяют границы поиска секретной экспоненты. В общем случае использование атаки Ван-Тилборга занимает очень длительное время, в то время как атака Дюжелла осуществляет взлом алгоритма RSA за реальное время. Эти алгоритмы зависят от выбора максимально допустимого значения границы D, то есть при неправильном выборе этого значения секретная экспонента может быть не найдена или время работы алгоритма станет не приемлемым. Таким образом

данные модификации как расширяют границы применения атаки Винера, так и накладывают на него дополнительные ограничения.

Атака с помощью метода факторизации Ферма показала хорошую эффективность только при малых значениях модуля N. В настоящее время минимально допустимая длина модуля N для алгоритма RSA равна 1024 бита, а проблема выбора близких значений p и q давно известна и учитывается при формировании значения $N = p \cdot q$. Из плюсов данного алгоритма можно отметить то, что он обязательно выполнит разложение модуля N на множители, только в случае больших чисел, произойдет это за не приемлемый для взлома алгоритма RSA промежуток времени.

Атака с применением алгоритма Гельфонда-Шенкса с теоретической точки зрения должна быстрее находить секретную экспоненту, чем атака при помощи метода Ферма. В некоторых удачных случаях это подтверждается на практике, но для средних значений модуля N, алгоритм оказался еще более медленным. Также следует заметить, что эта атака требует выделения большого объема памяти размерности квадратный корень из N, что накладывает дополнительные ограничения. Данный метод, как и метод Ферма ищет любые значения секретной экспоненты, но делает это за очень длительный промежуток времени. Таким образом, можно сделать вывод, что алгоритм Гельфонда-Шенкса также не приемлем для взлома алгоритма RSA.

Таким образом, самым практичным из реализованных методов является атака Дюжелла, так как она обладает приемлемым временем выполнения и способна находить значения секретной экспоненты в большем диапазоне, чем атака Винера.

Библиографический список:

1. Шнайер Б. Прикладная криптография / Б. Шнайер. — Триумф, 2002. — 816 с.

2. Лекция 4: Методы криптоанализа [Электронный ресурс] : информационный сайт. – Режим доступа : http://www.intuit.ru/studies/courses/600/456/lecture/10198 (дата обращения 15.05.2020).

3. MPIR: Multiple Precision Integers and Rationals [Электронный ресурс] : информационный сайт. – Режим доступа: http://mpir.org/ (дата обращения 15.05.2020).

4. Атака Дюжелла на криптосистему RSA [Электронный ресурс] : информационный сайт. – Режим доступа: http://cryptowiki.net/ index.php?title=Атака_Дюжелла_на_криптосистему_RSA (дата обращения 15.05.2020).

5. Song Y. Yan Cryptanalytic Attacks on RSA / Y. Yan Song. – Springer Science + Business Media, LLC, 2008. – 255 p.

6. Wiener M. J. Cryptanalysis of short RSA secret exponents / M. J. Wiener // IEEE Trans. Inform. Theory. – 1990. – Vol. 36. – P. 553–558.

7. Verheul E. R. Cryptanalysis of ‘less short’ RSA secret exponents / E. R Verheul, H.C.A. van Tilborg // Appl. Algebra Eng. Comm. Computing. – 1997. – V. 8. – P. 425-435.

8. Dujella A. A variant of Wiener’s attack on RSA / A. Dujella // Computing. – 2009. – Vol. 85. – P. 77 – 83.

Оригинальность 94%