УДК 004.056.55

Уфимцева Виктория Борисовна, *канд. техн. наук, доцент каф. ПМиИТ*
Харьковская национальная академия городского хозяйства

АНАЛИЗ УСЛОВИЯ ВЫБОРА МОДУЛЕЙ RSA С УЧЕТОМ ПОРЯДКА ЧИСЕЛ ФИБОНАЧЧИ

Аннотация. В этой статье рассматривается одно из условий, которое необходимо учитывать при выборе модуля $n = p \cdot q$ в криптографической системе с открытым ключом RSA. В противном случае могут быть найдены сомножители числа n. Рассматривается цикловая длина рекурсии $c \leftarrow c^{-1} + 1 \bmod n$, которая является важным условием при использовании чисел Фибоначчи и может быть использована при вычислении безопасных RSA модулей. И анализируется необходимость выполнения условия, что простое число p выбираемое как сомножитель модуля криптографической системы RSA n должно иметь большой индекс u_p, где F_{u_p} − это наименьшее число Фибоначчи, которое содержит p в качестве делителя.

Анотація. В цій статті розглядається одна з умов, яку необхідно враховувати при виборі модуля $n = p \cdot q$ в криптографічній системі з відкритим ключем RSA. В противному випадку можуть бути знайдені співмножники числа n. Розглядається циклова довжина рекурсії $c \leftarrow c^{-1} + 1 \bmod n$, що є важливою умовою при використанні чисел Фібоначчі і може бути використаною при вирахуванні безпечних RSA модулів. Та аналізується необхідність дотримання умови, що просте число p, яке обирається як співмножник модуля криптографічної системи RSA n повинно мати великий індекс u_p, де F_{u_p} − це найменше число Фібоначчі, що вмістить p в якості дільника.

Abstract. In this contribution condition are stated which safe public-key cryptosystem RSA modules $n = p \cdot q$ must fulfill. Otherwise the factors of n can be found. We consider the cycle-lengths of the recursion $c \leftarrow c^{-1} + 1 \bmod n$ which leads to a condition in terms of Fibonacci numbers and may be useful for evaluating the security of cryptosystem RSA modules. Necessity of condition − a prime p selected as factor of an RSA modulus n must have a large index u_p, where F_{u_p} is the smallest Fibonacci number which contains p as a divisor − are analyzed.

Актуальность темы.

Целочисленная проблема факторизации заключается в разложении составного числа n на произведение двух больших простых чисел p и q. Обнаружение больших простых чисел - относительно простая задача, а проблема разложения на множители, произведение двух таких чисел рассматривается в вычислительном отношении труднообрабатываемым [1]. Основываясь на трудности этой задачи Р. Райвест (Ronald Linn Rivest), А. Шамир (Adi Shamir) и Л. Адлеман (Leonard Adleman) из Массачусетского Технологического Института (MIT) в 1977 году предложили криптографический алгоритм с открытым ключом RSA [2].

RSA стал первым алгоритмом такого типа, пригодным и для шифрования и для цифровой подписи. Безопасность алгоритма основана на трудности задачи разложения на множители. RSA использует два ключа — открытый (public) и секретный (private), вместе открытый и соответствующий ему секретный ключи образуют пару ключей (keypair). Открытый ключ не требуется сохранять в тайне, он используется для зашифровывания данных. Если сообщение было зашифровано открытым ключом, то расшифровать его можно только соответствующим секретным ключом.

Основой системы RSA является произведение двух, примерно одинаковых по величине, больших простых чисел p и q:

$$n = p \cdot q, \qquad (1)$$

поэтому стойкость криптосистемы зависит от решения задачи факторизации больших чисел.

На случайные простые числа p и q накладываются ограничения [3]:

- p и q не должны быть слишком близки друг к другу, иначе можно будет их найти, используя метод факторизации Ферма. Однако, если оба простых числа и были сгенерированы независимо, то это ограничение с огромной вероятностью автоматически выполняется.
- Необходимо выбирать «сильные» простые числа, чтобы нельзя было воспользоваться $p-1$ алгоритмом Полларда.

По мере использования алгоритма RSA к выбору чисел p и q выдвигались еще дополнительные требования. Так исследования Клауса Хубера (Klaus Huber) показали необходимость учитывать при выборе модуля $n = p \cdot q$ порядка чисел Фибоначчи [4].

Исследования показали: если у выбранного модуля RSA p (или q) индекс u_p наименьшего числа Фибоначчи F_{u_p}, которое содержит p в качестве сомножителя, достаточно мал, то число $n = p \cdot q$ может быть легко разложено на сомножители.

Это может быть сделано путем задания начального значения $c = 1$ и вычисления итерационной формулы:

$$c \leftarrow c^{-1} + 1 \bmod n \quad \text{пока } НОД(c, n) > 1, \tag{2}$$

где c^{-1} обозначает инверсию $c \bmod n$.

Цикловая длина (cycle-lengths) итерационной формулы (2) равняется:

$$L = \begin{cases} 1, \quad для \quad a = \dfrac{1 \pm \sqrt{5}}{2} \\ u_p - 1, \quad для \quad a = -\dfrac{F_j}{F_{j+1}} \\ u_p, \quad в \quad других \quad случаях \end{cases} . \tag{3}$$

Так что при небольшом значении индекса числа Фибоначчи u_p либо рекуррентная формула (2), либо:

$$НОД(n, F_i \bmod n) \; i = 1,2,3,... \tag{4}$$

разложат число n на сомножители за $\min(u_p, u_q)$ шагов.

В связи с этим было выдвинуто условие: Простое число p выбираемое как сомножитель модуля RSA n должно иметь большой индекс u_p, где F_{u_p} – наименьшее число Фибоначчи, которое содержит p в качестве делителя.

Цель и задачи исследования. Целью работы является исследование одной из наиболее распространенных систем с открытым ключом RSA, а именно, анализ и обоснование необходимости учета порядка чисел Фибоначчи при выборе RSA модулей.

Для решения поставленной задачи проанализируем условие выбора простых чисел для модуля RSA с точки зрения вероятности выбора такого числа с небольшим индексом числа Фибоначчи. Вероятность определим как примерную оценку соотношения количества больших простых чисел соответствующей длины, являющихся делителями чисел Фибоначчи с небольшим индексом, к общему количеству таких чисел.

С этой целью была произведена программная генерация чисел Фибоначчи F_i порядка $i = \overline{1,10000}$ с последующим разложением на сомножители.

С точки зрения безопасности число n должно иметь размер не меньше 512 бит (155 десятичных знака), а с 2006г. система шифрования на основе RSA считается надёжной с модулем n размером 1024 бита (315 десятичных знаков) [5]. Так как по условию выбора сомножителей p и q модуля n они должна иметь примерно одинаковую величину, то для n размером 512 бит будем рассматривать числа Фибоначчи, содержащие в сомножителях простые числа длиной 77 и 78 (P_{77} и P_{78}) десятичных знака (табл. 1).

Таблица 1

Числа Фибоначчи с простыми сомножителями длиной 77 и 78 десятичных знака

Числа Фибоначчи F_n	**Факторизация F_n**
F_{401}	13885829·P_{77}
F_{617}	234461·66432482961307571407 37·58574343084466971356308 9·P_{78}
F_{783}	(3,9,27,29,87,261) 360874922114317142260605385 7·P_{78}
F_{793}	(13,61) 30133· 485538041· 3772191484024417· 458500259538957193· 12729787910496663114939916 81 · P_{78}
F_{857}	188114752716182481542615469389235776029 · 481259757493900268926204576196867770018308535752372858446757045 7 · P_{77}
F_{967}	1933.27930829 · 193208122057· 10999042492449833 · 475456324320700873137187391479 7 · 402310645982760211964572510392536242545912271029816655397 · P_{77}
F_{1485}	(3,5,9,11,15,27,33,45,55,99,135,165,297,495) 457381· 76581817484041· 247974902461264902503356994828720347822386074943598290 1 · P_{77}

Для модуля n размером 1024 бита простые сомножители должны быть длиной 155÷158 (P_{155}, P_{156}, P_{157} и P_{158}) десятичных знака (табл. 2).

Таблица 2

Числа Фибоначчи с простыми сомножителями длиной 155÷158 десятичных знака

Числа Фибоначчи F_n	**Факторизация F_n**
F_{1641}	(3,547) 13053350997780544042994125133495 3 · 16728422948644612748416370798750254177288 9 · P_{155}
F_{1713}	(3,571) 23256201901 · 17060780821921 · 55226076015902745973077917 · 364159438267495117175565083136144 1 · P_{156}
F_{1039}	8457461.132846541 · 20616815802035244343789 · 869789684576116767247597 · P_{156}
F_{1899}	(3,9,211,633) 3797 · 11393 · 1331996581 · 111120580793749579397 · 639501603583582129619570941512 1 · 376153138750869771164791654308836091080 57 · P_{156}
F_{1013}	4374133·2341859477·10878282841·14285366521·5728528579532559637 · P_{157}
F_{2415}	(3,5,7,15,21,23,35,69,105,115,161,345,483,805) 588860742541·2667297067452361·8481484594838771930389268119292044741 · P_{157}
F_{2175}	(3,5,15,25,29,75,87,145,435,725) 78301·1774834801·7524303251424572827665924780 1· 298891469007743995372743855942240 1 · P_{158}

В результате исследований выяснилось, что среди сомножителей чисел Фибоначчи с индексом до 10000 всего семь простых чисел имеют длину 77 и 78 десятичных знака, при чем у чисел Фибоначчи F_i порядка $i = \overline{400,1500}$. И семь простых сомножителей длиной 155÷158 десятичных знака у чисел Фибоначчи F_i порядка $i = \overline{1600,2200}$. Так что вероятность встретить такое простое число среди сомножителей чисел Фибоначчи можно определить как малую и равную примерно 0,0007.

Теперь определим, сколько же простых чисел заданной величины существует.

Со времен Эвклида этот вопрос так часто задается, что получил свое обозначение [6]: $\pi(x)$ = количество простых чисел меньших или равных x.

Для небольших значений x количество простых чисел $\pi(x)$ может быть найдено простым подсчетом. Так в 2007г. Т. Оливьера э Сильва (Tomás Oliveira e Silva) было определено $\pi(10^{23}) = 1.925.320.391.606.803.968.923$ [6].

График функции $\pi(x)$ для малых значений x является нерегулярным (рис. 1).

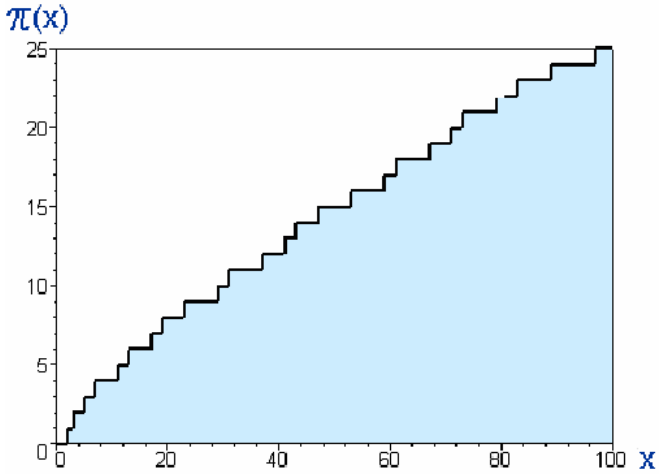

Рис. 1. Количество простых чисел $\pi(x)$ при $x \le 25$

Хотя функция $\pi(x)$ является локально нерегулярной, на графике с большими значениями x (рис. 2) видна определенная зависимость.

Невзирая на то, что распределение простых чисел кажется случайным из-за произвольного расстояния между ними и бесконечного множества простых близнецов, функция $\pi(x)$ неожиданно хорошо себя ведет.

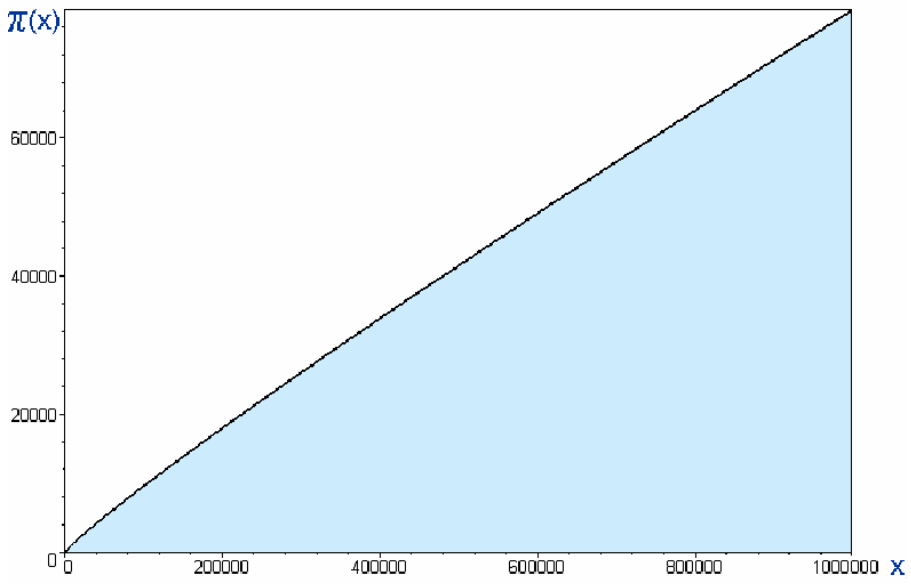

Рис. 2. Количество простых чисел $\pi(x)$ при $x \le 10^6$

Теорема о распределении простых чисел [7]: Количество простых чисел не достигающих x асимптотически приближается к $x/\log x$ или $\pi(x) \sim x/\log x$. Т.е. $x/\log x$ является хорошей аппроксимацией для $\pi(x)$.

Используя вышесказанное, определяем, что количество простых чисел длиной 77 и 78 десятичных знаков $\pi(10^{78}) - \pi(10^{76})$ примерно равно $18 \cdot 10^{75}$, а длиной 155÷158 десятичных знаков $\pi(10^{158}) - \pi(10^{154}) \sim 16 \cdot 10^{155}$.

Вывод. Таким образом, так как количество больших простое чисел заданного размера среди сомножителей чисел Фибоначчи невелико, а общее количество простых чисел такого размера несоизмеримо большое, то при выборе модулей RSA условием учета порядка числа Фибоначчи можно пренебречь. В системах с повышенным требованием к безопасности можно выдержать это условие, создав таблицы простых чисел нужного размера с небольшим порядком числа Фибоначчи воизбежание их выбора в качестве модулей RSA.

1. *Венбо Мао. Современная криптография: теория и практика. – М.: «Вильямс», 2005. — 768с.*
2. *R. Rivest, A. Shamir, L. Adleman. A Method for Obtaining Digital Signatures and Public-Key Cryptosystems // Communications of the ACM, Vol. 21 (2), 1978, pp.120–126.*
3. *Нильс Фергюсон, Брюс Шнайер. Практическая криптография. – М.: «Диалектика», 2004. – 432с.*
4. *Klaus Huber. Some Considerations concerning the Selection of RSA Moduli // Advances in Cryptology - Eurocrypt '91. – Brighton, UK: Springer, 1991, P. 294-301. – www.springerlink.com/content/tbhv7184jc56mynb/fulltext.pdf*
5. *Введение в криптографию /Под общ. ред.В.В.Ященко – М., МЦНМО, 2008. – http://nature.web.ru*
6. *Chris K. Caldwell. How Many Primes Are There? http://primes.utm.edu/howmany.shtml*
7. *G. H. Hardy and E. M. Wright. An introduction to the theory of numbers.* – Clarendon, Oxford, 1938, 419 pp.