УДК 681.3.06: 519.248.681

И. Д. ГОРБЕНКО, д-р техн. наук, П. В. КОЛЕСНИКОВ

ОЦЕНКА СТОЙКОСТИ RSA СИСТЕМ, В КОТОРЫХ ОТКРЫТЫЕ КЛЮЧИ ИЛИ ПАРАМЕТРЫ ЯВЛЯЮТСЯ ЛИЧНЫМИ

Введение

В 90-е годы широкое распространение получили криптографические системы, базирующиеся на преобразованиях с использованием математического аппарата колец, полей, групп, включая эллиптические группы. Необходимость таких систем можно объяснить требованиями практических задач, для которых должна быть реализована модель взаимного недоверия и взаимной защиты. Были разработаны и практически нашли применение криптографические алгоритмы под названием "алгоритмы с открытыми ключами" (RSA [1]), "с открытым распределением ключей" (Диффи-Хелмана), алгоритмы цифровой подписи с открытыми ключами, базирующиеся на RSA и преобразованиях класса Эль-Гамаля. В последние годы получили распространение криптографические алгоритмы, использующие группы точек в эллиптических кривых. Кроме названных алгоритмов определенное распространение получили и другие, но они по своей структуре базируются на описанных выше. Отличительная особенность их в том, что ключ делится на два, один из которых является личным, другой открытым. При этом принятие такого протокола существенно снижает стойкость криптозащиты, либо требует применения "усиленных" параметров криптографических преобразований. Физически криптографическое "ослабление" можно пояснить тем, что атака производится при известных открытых ключах и параметрах. Необходимость такой модели, на наш взгляд, связана с тем, что все санкционированные пользователи не доверяют друг другу и требуют защиты.

В то же время в ряде приложений можно обеспечить, с одной стороны, применение систем с открытыми ключами, а с другой – гарантировать конфиденциальность и целостность как личных, так и открытых ключей и параметров. В таких условиях криптоаналитические атаки могут осуществляться только извне информационной системы. На наш взгляд, весьма целесообразно проведение анализа и оценки криптостойкости в условиях атаки со стороны внешних пользователей, не имеющих доступа к личным и открытым ключам и параметрам. При этом чрезвычайно важным является оценка целесообразности использования такого режима. Анализ показал, что на RSA с закрытыми параметрами криптонападения возможны при следующих условиях:

1. Когда ключи E и D неизвестны, модуль N известен.
2. Для случая, когда E, D и N неизвестны.

Рассмотрим и оценим криптонападения при указанных условиях.

1. Классическая атака на системы с открытыми ключами

Цель криптоаналитической атаки на RSA-подобные системы заключается в нахождении секретного ключа E_k, и далее передаваемого сообщения M, исходя из известных открытых параметров N, D_k и криптограммы C. В ряде источников показано, что наилучшей среди известных атак на RSA является факторизация модуля преобразования N. Суть методики криптоанализа, которую может реализовать санкционированный пользователь, заключается в следующем.

1. Перехват сертификатов атакуемого объекта. N – модуль преобразования, D_k – открытый ключ.
2. Факторизация числа $N=P*Q$.
3. Вычисление функции Эйлера $\varphi(N)=(P-1)(Q-1)$.
4. Решение сравнения $E_kD_k=1 \bmod \varphi(N)$. При известных D_k и $\varphi(N)$ это уравнение решается за полиномиальное время.

Проведем анализ сложности этой атаки [2]. Факторизация N требует реализации субэкспоненциальной сложности. Известно значительное множество методов решения задачи факторизации. Основным из них является метод Полларда (ρ-метод), Ленстры с использованием аппарата эллиптических кривых, квадратичное решето числового поля, общее решето числового поля и другие. Сложность приведенных методов уменьшается в порядке, перечисленном выше. Сложность факторизации для общего решета числового поля составляет [5] :

$$I = e^{\delta \cdot (\ln N)^{\nu} \cdot (\ln \ln N)^{(1-\nu)}} \qquad (1)$$

Известно решение задачи, где параметры δ и ν равны [5] :

$$(\delta,\nu)=(1.96,\ 1/3) \qquad (2)$$

Сложность вычисления шагов 3, 4 приведенной методики криптоанализа является полиномиальной. В табл. 1 приведены оценки сложности факторизации методом обобщенного числового поля, полученные с использованием (1) и (2).

Таблица 1

Длина модуля N	Сложность факторизации I
256	$2^{47,56}$
512	$2^{65,15}$
1024	$2^{88,43}$

Второй способ криптоатаки – это атака на операцию возведения в степень по модулю и нахождение дискретного логарифма. Цель атаки состоит в нахождении передаваемого сообщения M, исходя из криптограммы C и известных открытых параметров N, D_k.

Из приведенной методики следует, что криптоанализ успешно может быть выполнен, если сертификаты N, E_k известны криптоаналитику. Представляет интерес случай, когда E_k, D_k – неизвестны. Рассмотрим его более подробно.

2. Атака на RSA-алгоритм при неизвестных открытом ключе D и известном модуле N

Напомним, что RSA-преобразования выполняются в кольце целых чисел, содержащем единицу, по модулю N. В таком кольце существует множество пар ключей (E_k, D_k), удовлетворяющих сравнению

$$E_kD_k\equiv 1 \bmod \varphi(N) \qquad (3)$$

Действительно, из ((3) следует, что E_k и D_k принимают значения, не превышающие $\varphi(N)$. Для чисел в кольце введены основные операции. Если предъявить требования, чтобы кольцо содержало "1" (т.е. существовало решение сравнения), тогда в качестве E_k могут быть выбраны такие числа, что (E_k, $\varphi(N)$)=1, поэтому число решений сравнения можно определить как [4]

$$n_{реш}=\varphi(\varphi(N))=\varphi((P-1)(Q-1))=\varphi(P-1)\,\varphi(Q-1) \qquad (4)$$

Предварительный анализ соотношения показывает, что количество решений зависит от вида разложения P-1 и Q-1. Например, если P-1 содержит большие числа, то $n_{реш}$ будет большим числом.

Вероятность подбора пары (E_k, D_k) равна

$$Вер(E_k, D_k)=Вер(E_k) \qquad (5)$$

В табл. 2 приведены вероятности подбора пары (E_k, D_k) при известном N.

Таблица 2

Длина числа N, (бит)	Для простых чисел	Для сильных простых чисел вида R|P-1	Для сильно простых чисел вида R|P-1, S|P+1
511	$2^{-508,72}$	$2^{-508,86}$	$2^{-508,86}$
1024	$2^{-1020,45}$	$2^{-1020,72}$	$2^{-1020,72}$
2048	$2^{-2044,22}$	$2^{-2044,45}$	$2^{-2044,45}$

Число попыток, которые необходимо выполнить для удачного подбора N, можно оценить как

$$n_N=P_{треб}*1/Вер(P,Q)\ , \qquad (6)$$

где $P_{треб}$- требуемая вероятность подбора N.

3. Атака на RSA алгоритм при неизвестных открытых модуле N и ключе D

Проведем анализ возможных атак и дадим оценку сложности их выполнения для случая, когда один или несколько параметров используются в режиме конфиденциальных параметров.

Известно, что, используя метод грубой силы, можно подобрать модуль N и ключи D_k, E_k. Выполняя атаку по этой схеме, нужно подобрать сначала модуль N. Определим количество вариантов перебора n_N. Величину n_N можно определить, зная количество простых чисел P,Q – n_P и n_Q.

Если P есть простое, то, используя теорему Чебышева [3], число простых чисел, находящихся в интервале [1, P-1], можно определить как:

$$n_p=\frac{P}{\ln P} \qquad (7)$$

В интервале $[P_1, P_2]$ число простых чисел Δn_P можно оценить как

$$\Delta n_P = \frac{P_2}{\ln P_2} - \frac{P_1}{\ln P_1} \tag{8}$$

где $[P_1, P_2]$ – заданный интервал.

Для Q аналогично находим:

$$\Delta n_Q = \frac{Q_2}{\ln Q_2} - \frac{Q_1}{\ln Q_1} = \Delta n_P \tag{9}$$

Если P простое число общего вида, то вероятность подбора числа N можно определить через вероятности подбора чисел P и Q:

$$\text{Вер}(P, Q) = \text{Вер}(P)\ \text{Вер}(Q) = \frac{1}{\Delta n_P} \cdot \frac{1}{\Delta n_Q} =$$

$$= \frac{\ln P_1 \cdot \ln P_1}{P_2 \cdot \ln P_1 - P_1 \cdot \ln P_2} \cdot \frac{\ln Q_1 \cdot \ln Q_1}{Q_2 \cdot \ln Q_1 - Q_1 \cdot \ln Q_2} \tag{10}$$

Для случая многократного подбора:

$$\text{Вер}(N) = n * \text{Вер}(P, Q), \tag{11}$$

где n – число попыток

В табл. 3 приведены оценки вероятности подбора числа N для случая, когда l_N=256, 512, 1024, 2048 бит.

Таблица 3

Длина числа N, (бит)	Для простых чисел (экспериментально)	Для простых чисел (по формуле)	Для простых чисел R|P-1	Для простых чисел R|P-1, R|P+1
511	$2^{-495,08}$	$2^{-495,05}$	$2^{-493,72}$	$2^{-492,69}$
1024	$2^{-1005,0}$	$2^{-1005,05}$	$2^{-1003,58}$	$2^{-1002,55}$
2048	$2^{-2027,19}$	$2^{-2027,05}$	$2^{-2025,44}$	$2^{-2024,41}$

Рассмотрим дальше задачу "взлома" RSA – систем при неизвестных открытых параметрах E, D и N. Безопасное время равно:

$$t_{без} = P_{треб} * n_N / (\gamma K) \tag{12}$$

Очевидно, что полная вероятность успешного криптоанализа, ввиду независимости событий равна:

$$\text{Вер}(N, (E, D)) = \text{Вер}(P,Q) * \text{Вер}(E_k) = (\ln P_1 \ln P_2)/(P_1 \ln P_2 - P_2 \ln P_1) * 1/(\varphi(P-1)\ \varphi(Q-1)) \tag{13}$$

В табл. 4 приведены значения вероятностей подбора N при неизвестных открытых параметрах E, D, N для прямой атаки при использовании простых чисел P, простых чисел в узком смысле и широком смысле.

Таблица 4

Длина числа N, (бит)	Для простых чисел P и Q	Для сильных простых чисел R|P-1	Для простых чисел R|P-1, S|P+1
511	$2^{-1003,77}$	$2^{-1002,58}$	$2^{-1001,55}$
1024	$2^{-2025,50}$	$2^{-2024,30}$	$2^{-2023,27}$
2048	$2^{-4071,27}$	$2^{-4069,89}$	$2^{-4068,86}$

Для случая, когда N – известно, E_k, D_k – неизвестны, необходимо сначала выполнить факторизацию N, а затем найти E_k и D_k.

4. Экспериментальная оценка количества сильных простых чисел

Если P, Q – ограниченные числа, например сильные простые числа в узком или широком смысле, то оценку для количества простых чисел P заданной длины можно получить экспериментально.

Суть эксперимента заключается в определении плотности распространения простых чисел на оси натуральных чисел N. Для обычных простых чисел [4]:

$$n_p = \frac{P}{\ln P} \qquad (14)$$

Плотность распределения простых чисел можно определить, взяв производную по P

$$n_p' = \frac{P' \cdot \ln P - P \cdot \frac{1}{P}}{\ln^2 P} = \frac{\ln P - 1}{\ln^2 P} = \frac{1}{\ln P} - \frac{1}{\ln^2 P} \qquad (15)$$

Если пренебречь $\frac{1}{\ln^2 P}$, то среднее расстояние Δr между простыми числами P_i и P_{i+1} на оси N можно оценить как:

$$\Delta r = \frac{1}{\ln P} \qquad (16)$$

Цель эксперимента состоит в оценке количества простых чисел из множества допустимых с длиной 256, 512, 1024 бит. Для сильно простого числа в широком смысле справедливы соотношения:

$$R_1 | P-1,\ R_2 | P+1,$$

$$l_{R1} \geq l_P/2,\ l_{R2} \geq l_P/2 \qquad (17)$$

1. Найдем сначала количество простых чисел:

а) в заданном диапазоне его можно найти путем определения количества таких чисел исходя из малого диапазона чисел длины 256, 512, 1024 бит;

б) далее, зная распределение простых чисел в малом диапазоне, сделаем оценку их количества во всем диапазоне.

Результаты эксперимента приведены в табл. 5. Результаты эксперимента можно сравнить с теоретическими данными, полученными с использованием формулы (16)

2. Оценим количество сильных простых чисел в широком и узком смысле. Для чисел большой длины эта задача не имеет простого решения, т.к. для этого необходимо разложить большие P-1 и P+1 на множители. Найдем оценки, следующим образом:

а) рассмотрим все числа длиной: 11, 12,13,...,32 битов;

б) для каждой длины найдем среднее значение количества простых чисел из 1000 рассмотренных с данной длиной;

в) найдем зависимость количества простых чисел в диапазоне длиной 1000 от длины рассматриваемого числа. Используя (16) получим, что количество простых чисел среди $k_{расам}$ чисел, сравнимых по длине с P, равно:

$$n_P = \frac{k_{рассм}}{\ln P} \qquad (18)$$

Если учесть тот факт, что длина числа P в битах равна l_P, перепишем (18) в следующем виде:

$$n = k_{рассм} \cdot \frac{\log_2 e}{\log_2 P} = k_{рассм} \cdot \frac{1{,}44}{l_P} \qquad (19)$$

где n – количество простых чисел среди $k_{рассм}$ чисел длины lP;

г) по экспериментальным данным найдем закон зависимости количества простых чисел в интервале длиной 1000 от длины простого числа. Далее обобщим полученные результаты на числа большой длины: 256, 512, 1024 бит.

Для обыкновенных простых чисел зависимость их количества от длины числа подчиняется закону (20). Для определения количества сильных простых чисел воспользуемся модифицированной формулой:

$$n = k_{рассм} \cdot c_1 \cdot \frac{1{,}44}{l_P^{c_2}}, \qquad (20)$$

где коэффициенты c_1 и c_2 будут подбираться экспериментально. В табл. 5 Количество простых и сильно простых чисел заданной длины.

Таблица 5

Длина числа P, бит	Количество простых чисел (экспериментально)	Количество сильных простых чисел R|P-1 (экспериментально)	Количество сильных простых чисел R|P-1, S|P+1 (экспериментально)	Количество простых чисел по формуле (19)	Количество простых чисел по формуле (20) c1=1,07 c2=0,93	Количество простых чисел по формуле (20) c1=1,07 c2=0,65
11	134	112	83	131	103	72
12	124	87	55	120	94	66
13	113	90	65	111	86	60
14	107	77	52	104	80	56
15	99	76	58	96	74	52
16	93	66	45	90	69	48
17	87	68	51	85	65	45
18	82	59	41	80	61	43
19	78	59	45	75	57	40
20	75	52	35	72	54	38
21	72	53	39	69	52	36
22	68	48	32	66	49	34
23	65	48	35	63	47	33
24	63	44	30	60	45	31
25	60	44	32	58	43	30
26	58	40	27	55	41	29
27	56	40	29	53	39	28
28	54	37	26	52	38	27
29	52	38	27	50	37	26
30	50	34	24	48	35	25
31	48	35	25	47	34	24
32	46	32	22	45	33	23

На рисунке показаны результаты экспериментальной и теоретической оценки числа простых чисел на 1000 чисел.

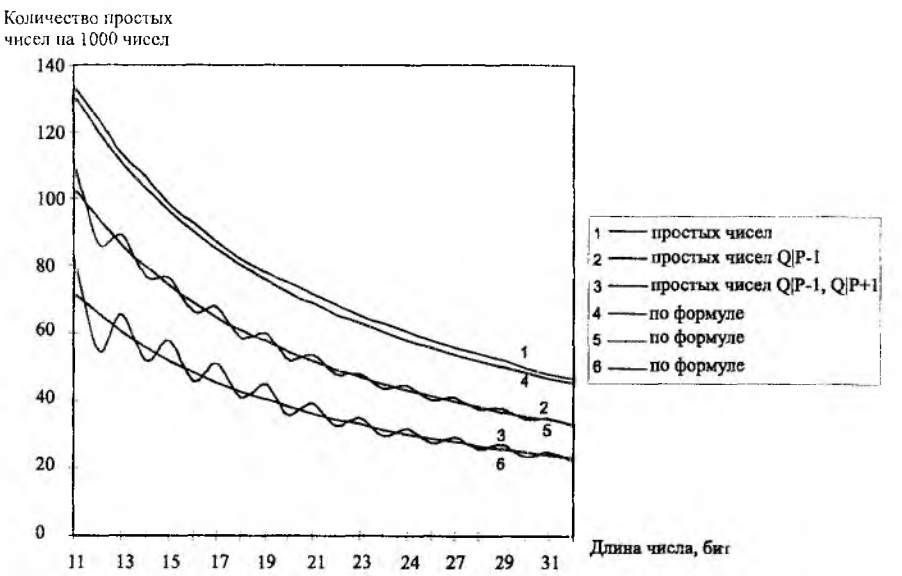

Рис. 1

На рис. 1 показана зависимость количества простых чисел на 1000 исследуемых от длины числа. Здесь объединены теоретические и практические результаты. В таблице 6 даны оценки количества простых чисел во всем диапазоне чисел заданной длины для реальных значений P и Q.

Таблица 6

Длина выборки	Длина числа P, Q, (бит)	Количество простых чисел в диапазоне $[1, 2^n]$ (экспериментально)	Количество простых чисел по формуле (16)	Количество простых чисел по формуле (20) R|P-1	Количество простых чисел по формуле (20) R|P-1, R|P+1
2^{255}	256	$2^{247,54}$	$2^{247,52}$	$2^{246,86}$	$2^{246,34}$
2^{511}	512	$2^{502,51}$	$2^{502,52}$	$2^{501,79}$	$2^{501,27}$
2^{1023}	1024	$2^{1013,59}$	$2^{1013,52}$	$2^{1012,72}$	$2^{1012,20}$

5. Экспериментальная оценка значения функции Эйлера

Из теории чисел известно [3], что значение функции Эйлера для любого целого числа n, имеющего каноническое разложение вида

$$n = p_1^{\alpha_1} \cdot p_2^{\alpha_2} \cdot \ldots \cdot p_n^{\alpha_n}$$

можно определить как

$$\varphi(n) = p_1^{\alpha_1 - 1} \cdot (p_1 - 1) \cdot \ldots \cdot p_n^{\alpha_n} \cdot (p_n - 1) \qquad (21)$$

Оценим значение функции Эйлера для числа некоторой длины l_n. Минимальное ее значение будет соответствовать числу, составленному из простых чисел 2,3,5,7..., идущих подряд, начиная с 2. Это значение будет минимальным так-так в этом случае в расчете $\varphi(n)$ множитель (p_i-1) будет встречаться максимальное число раз, а все остальные множители будут равны p_i. Экспериментально найдем минимальную оценку для $\varphi(n)$. Результаты эксперимента приведены на рис. 2. По оси x показана длина числа n в битах, а по оси y значение разности длины чисел n от длины значения функции Эйлера $\varphi(n)$.

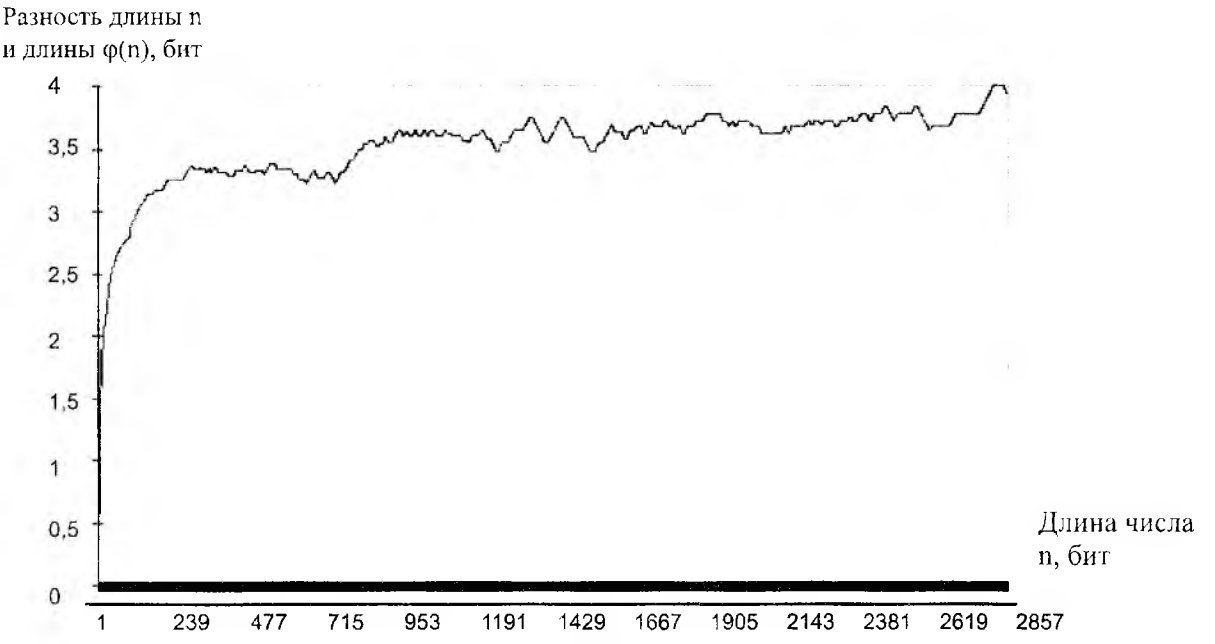

Рис. 2

Приведем пример оценки длины функции Эйлера для длины модуля преобразования N RSA-системы равному 256 бит. Из условия задачи следует, что число N состоит из двух простых множителей длиной $l_P=l_Q=128$ бит. Из $\varphi(N)= (P-1)*(Q-1)$ следует, что $l_{\varphi(N)}=256$ бит. Зная, что минимальное значение длины функции Эйлера можно вычислить по формуле

$$\varphi(\varphi(N)) = \varphi((P-1)*(Q-1)) \qquad (22)$$

можно оценить минимальную и максимальную границы для функции Эйлера в следующем виде: min $l_{\varphi(\varphi(N))}$= 250 бит, max $l_{\varphi(\varphi(N))}$= 256 бит.

Разница длин $l_{\varphi(\varphi(N))}$ и $l_{\varphi(N)}$ была определена в ходе эксперимента и составляет максимум 3 бита. Для получения результата предполагалось, что разложение чисел P-1, Q-1 может содержать сомножители любой длины. Используя результаты рис. 2 можно оценить степень уменьшения числа ключей E_k, если известна длина модуля N.

Заключение

Криптосистемы с открытыми ключами нашли применение при реализации модели взаимного недоверия и взаимной защиты. В этом случае один из ключей является личным, а второй открытым. Личный должен храниться как конфиденциальный и не выходить из-под влияния пользователя. Открытый ключ доступен всем пользователям сети. Основным требованием к открытому ключу является обеспечение его целостности и аутентичности на всех этапах жизненного цикла. Объявление одного из ключей открытым, существенно снижает криптостойкость. Если криптосистема с открытыми ключами применяется в информационных системах, в которых действует модель взаимного доверия, то в ней открытые ключи и/или параметры, например, значение модуля RSA-преобразования N, могут объявляться и использоваться на всем жизненном цикле как личные. В этом случае криптостойкость систем защиты существенно повышается, и она начинает приближаться по стойкости к симметричным системам. Наибольшая степень повышения стойкости достигается, если в RSA-системе и модуль N и открытый ключ объявляются и существуют в системе как личные. Если N или один из ключей являются открытыми, то в этом случае стойкость понижается, но остается на много выше, чем в стандартной RSA криптосистеме, в которой модуль N и ключ E являются открытыми.

В то же время, на наш взгляд, применение RSA систем в режиме защиты модуля или открытого ключа является оправданным, так как личный ключ остается конфиденциальным. Это означает, что при его использовании для цифровой подписи, лицо или объект, подписывающий информацию, несет за нее ответственность так же, как в системе взаимного недоверия. Именно в этом преимущества применения RSA системы в предлагаемых режимах обеспечения конфиденциальности открытых ключей и/или модулей преобразования.

Если RSA применяется в режиме конфиденциальности открытых ключей или модулей преобразования, то длины ключей или модулей можно уменьшить до 256 битов. Это позволит повысить скорость и уменьшить сложность прямых и обратных преобразований, причем, стойкость будет оставаться близкой к стойкости симметричных криптосистем.

Авторы будут признательны публичному обсуждению такого режима применения RSA системы и возможных областей применения. Считаем, что RSA система все-таки будет проигрывать большинству симметричных криптосистем, по крайней мере, с эквивалентной длиной ключа.

Список литературы: 1. *Диффи У.* Первые десять лет криптографии с открытым ключом // ТИИЭР. 1998. Т.76, №5. С.54-74. 2. *RSA: мифы и реальность* /Под. ред. И.Д. Горбенко, Е.Г. Качко, А.В. Свинарев и др. // Безопасность информации 1996. №2. С. 17-25. 3. *Виноградов И.М.* Основы теории чисел М.: Наука, 1981. 176 с. 4. *Menezes A., Oorschot P., Vanstone S.* Handbook of applied cryptography. CRC Press, 1996. 816 p. 5. *Buchmann J., Loho J., Zayer J.* An implementation of the general number field sieve. New York: Advances in cryptology: Proc. of Crypto'93. 1994. P.13-26.

Харьковский государственный технической университет радиоэлектроники

Поступила в редколлегию 27.03.2001