УДК 681.3.067

МЕТОДЫ И АЛГОРИТМЫ ГЕНЕРАЦИИ МНОГОРАЗРЯДНЫХ ПРОСТЫХ ЧИСЕЛ В КРИПТОГРАФИЧЕСКИХ СИСТЕМАХ

ГОРБЕНКО И.Д., МЕЛЬНИКОВА О.А

Проведены анализ и сравнение методов проверки простоты чисел с точки зрения их соответствия требованиям криптографических приложений. Приведена методика проверки и оценки характеристик тестов простоты, позволяющая сравнить их эффективность по различным параметрам (времени выполнения единичного теста, поиска простого числа, эффективности отсеивания и т.д.) при изменении режима выбора начальных приближений. Предлагаются рекомендации по разработке комплексного метода поиска простого числа.

В настоящее время в системах защиты информации широко используются несимметричные криптографические преобразования (например, RSA – схемы шифрования и подписи, класс подписей типа Эль – Гамаля, схема Диффи – Хеллмана и другие). В несимметричной криптографии в качестве ключевых параметров или их секретных составляющих повсеместно используются простые числа (или пары *простое число – первообразный элемент*). Отметим, что для обеспечения требуемого уровня стойкости криптографических систем необходимо использовать простые числа большой разрядности (например, не менее 512 бит) и, следовательно, использовать трудоемкие операции арифметики многократной точности. Кроме того, используемые простые числа во многих криптографических схемах должны удовлетворять еще ряду довольно жестких требований и ограничений, что создает дополнительные трудности при их формировании и требует значительных вычислительных затрат на повторную перегенерацию при неудовлетворительном качестве сформированных чисел. Поскольку в криптографических системах вычислительная сложность алгоритмов является, как правило, критическим параметром, то особую актуальность приобретает проблема быстрого формирования простых чисел с заданными свойствами (т.е. создания быстрого комплексного теста проверки простоты задаваемых чисел, обеспечивающего требуемый уровень достоверности).

1. Анализ методов проверки простоты чисел

К настоящему времени разработан ряд методов проверки простоты чисел. Их можно разделить на три группы. К первой относятся математически строгие методы, которые позволяют однозначно ответить на вопрос о простоте числа. Методы Монте-Карло (группа вероятностных методов) позволяют подтвердить предположение о простоте числа только с определенной вероятностью. К третьей группе относятся методы, базирующиеся на использовании гипотез, в частности, на предположении истинности очень правдоподобной, но не доказанной гипотезы.

К математически строгим (аналитическим) методам относятся: метод пробных делений, решето Эратосфена, методы прямой факторизации с использованием различных вычислительных алгоритмов, использование чисел специального вида (Ферма, Мерсенна и других), а также методы, использующие известные разложения чисел $N \pm 1$ и других. Вероятностные методы базируются на использовании так называемых вероятностных тестов проверки на простоту. Основными из них являются: тест, основанный на использовании теоремы Ферма, тест Лемана, тест Соловея -Штрассена, тест Рабина, стохастический тест Малма и другие. К основным методам, базирующимся на использовании предположения о справедливости определенной гипотезы (в частности, расширенной гипотезы Римана), относятся методы, использующие следующие алгоритмы: Полларда, Миллера, Адлемана-Румели, Ленстры-Коэна и другие.

Все названные методы могут быть использованы для проверки чисел на простоту. При работе с криптографическими системами основным критерием предпочтительности выбора того или иного метода проверки простоты чисел является минимизация вычислительной сложности (а следовательно, и времени построения простых чисел). Здесь подразумевается построение больших простых чисел (например, не менее 512-битных чисел).

Обобщим результаты сравнения трех групп методов. Аналитические методы дают строгое решение вопроса о простоте, но обладают рядом существенных недостатков: требуют полного или частичного разложения на простые сомножители, что является трудоемкой задачей; часто сложны для реализации из-за высокой вероятности сбоя или ошибки программирования. Методы гипотез относительно легко реализуемы и принятые ими числа действительно будут простыми, если будет доказана соответствующая гипотеза. Однако если изначальная гипотеза окажется неверной, то методы нельзя считать строгими доказательствами простоты. Методы гипотез требуют также выполнения длительных вычислений. Вероятностные методы не дают строгого математического доказательства простоты числа, но легко реализуемы, не требуют разложения на сомножители и обеспечивают быстрое выполнение проверки.

Анализ показал, что наиболее оптимальными по вычислительным затратам являются вероятностные алгоритмы. Учитывая особенности криптографических приложений, требующих быстрого оперирования с числами большой разрядности, в настоящее время предпочтительней использовать класс вероятностных методов проверки простоты. Рассмотрим кратко основные вероятностные тесты. Эти тесты проверяют выполнение некоторых условий на последовательности равномерно распределенных случайных чисел из отрезка $[1, N]$. При выполнении условий для всех случайно выбранных значений можно с некоторой вероятностью (зависящей от вида теста) утверждать, что N является простым числом. Вероятность зависит от объема выборки случайных чисел, а также от качества случайности используемой выборки.

Тест Ферма [1,2] использует малую теорему Ферма и проверяет выполнение условия

$$a_i^{N-1} = 1 \bmod N \qquad (1)$$

для случайных чисел a_i из интервала $[1, N]$. Вычислительная сложность теста может быть оценена как $O\left(|N| \cdot M\left(|N|\right)\right)$ шагов [2], где $M(|N|)$ – количе-

ство шагов для умножения двух чисел длины |*N*| при использовании стандартной техники [3].

Числа *N*, удовлетворяющие (1), принято называть псевдопростыми по основанию a_i или a_i-псп [2]. Известно, что существует бесконечно много составных a_i-псп чисел. Существуют также составные числа Кармайкла, которые являются псевдопростыми для любого a_i, такого, что $(a_i, N) = 1$ (абсолютно псевдопростые). Таким образом, тест Ферма может оказаться неудачным для составного числа *N*, если оно является числом Кармайкла, или поиск первого a_i, не удовлетворяющего (1), может потребовать слишком больших вычислительных затрат. Черник дал метод получения чисел Кармайкла [4], но до сих пор еще не известно, существует ли бесконечное множество таких чисел и неизвестен их закон распределения. В ходе исследований при создании методики проверки и оценки характеристик тестов для эмпирической проверки эффективности отсеивания тестов был реализован метод Черника и получены 28800 чисел Кармайкла вида $N = (6t+1)(12t+1)(18t+1)$ в диапазоне до 10 байт (минимальное число – 1729 = 7·13·19, максимальное число – 43606UL·938121998UL·3946586977UL=51180631UL 102361261UL 153541891 UL). Отличие диапазона чисел Кармайкла, используемых при проведении экспериментов в данной работе, от диапазона реально используемых в криптографии чисел (256 – 1024 бит) объясняется вычислительными ограничениями в методе генерации достоверных трехкомпонентных чисел Кармайкла. В дальнейшем предполагается проведение и публикация результатов отдельных углубленных исследований по данному вопросу: разработка методики и алгоритма формирования «вероятностных» чисел Кармайкла большой длины (256, 512 бит), исследование их распределения и свойств (возможности отсеивания различными тестами) для данных длин. Для целей настоящей работы данное ограничение не является критичным.

Тест Лемана [5] основан на использовании малой теоремы Ферма (1) в преобразованном виде:

$$\left(a_i^{\beta}+1\right)\left(a_i^{\beta}-1\right) \equiv 0 \bmod N, \quad \beta = \frac{N-1}{2}, \quad \text{или} \quad \begin{cases} a_i^{\beta} \equiv 1 \bmod N, \\ a_i^{\beta} \equiv -1 \bmod N. \end{cases} \qquad (2)$$

В классическом варианте теста Лемана условия (2) проверяются на k случайных значениях чисел a_i из интервала [1, *N*] и ставится требование хотя бы одного появления "–1" на наборе $\{a_1, \ldots, a_k\}$. При этом вероятность ошибки (ошибочного принятия составного числа) [5] не превышает 2^{-k}.

Основными недостатками классического варианта теста Лемана является то, что при малых (в соотношении с размерностью N) значениях k тест может ошибочно браковать простые числа, а также то, что в большинстве случаев возникает необходимость выполнения проверки на всех k значениях a_i. Другие вероятностные тесты позволяют при выполнении проверок на составных числах досрочно выходить из цикла по k, что значительно уменьшает среднее время выполнения теста при поиске простых чисел (подтверждается приведенными далее экспериментальными данными).

Более эффективным является тест Соловея-Штрассена [1,2,6,7], который, по существующему в некоторых источниках мнению [1,2], способен отсеивать большинство чисел Кармайкла (однако теоретическая оценка эффективности отсеивания неизвестна). При выполнении условий

$$(a_i, N) = 1, \quad a_i^{\frac{N-1}{2}} \equiv J(a_i, N) \bmod N, \qquad (3)$$

где $J(a_i, N)$ – символ Якоби, для k случайно выбранных значений a_i из интервала $[1, N-1]$ нечетное число *N* является простым числом с вероятностью ошибки не более 2^{-k}. Вычислительная сложность теста, по сведениям [7], может быть оценена как $O\left((\log N)^{2+\varepsilon}\right)$ $\forall\, \varepsilon > 0$ и определяется сложностью вычисления степени по модулю [3] и вычислительной сложностью определения символа Якоби [8].

Тест Рабина, по имеющимся сведениям [2], является обобщенной и более сильной версией теста Соловея-Штрассена. Поскольку проверяемое число *N* нечетно, то его можно представить в виде $N = 2^r \cdot s + 1$, где s – нечетное число.

При выполнении условий

$$a_i^s = 1 \bmod N, \quad \left(a_i^{2^j}\right)^s = -1 \bmod N, \text{ для некоторого } j = \overline{1, r-1} \qquad (4)$$

для k случайно выбранных из интервала [1,*N*–1] значений a_i, *N* является простым числом с вероятностью ошибки не более 4^{-k} (оценка лучше, чем для теста Соловея-Штрассена). Вычислительная сложность, по данным [7], оценивается как $O(\log_2 N)$ операций над большими целыми числами.

Стохастический тест Малма [2] использует результаты Лемера и дает вероятность ошибки не более $2^{-k\cdot(m-1)}$, где *m* – количество различных простых делителей числа *N*. Этот тест более трудоемок, чем рассматривавшиеся ранее тесты Соловея-Штрассена и Рабина, но при этом не снижает вероятность ошибки.

Проведенный предварительный теоретический анализ вероятностных тестов показал, что наиболее оптимальным соотношением эффективности отсеивания непростых чисел и вычислительной сложности теста обладают алгоритмы Соловея-Штрассена и Рабина. Учитывая приблизительную эквивалентность вычислительных затрат и тот факт, что тест Рабина, как показали эмпирические результаты, как правило, отсеивает большинство непростых чисел уже при проверке первого условия из (4) и, следовательно, дает лучшие временные характеристики, а также является обобщенной и более усиленной версией теста Соловея-Штрассена, приходим к выводу о предпочтительности использования именно этого вероятностного теста в качестве одного из составных частей при разработке комплексного теста проверки простоты числа. В ходе исследований для более тщательной оценки тестов и разработки комплексного теста проверки простоты была разработана методика экспериментальной проверки и оценки характеристик тестов, позволяющая сравнить эффективность тестов по различным параметрам (время выполнения единичного теста, время поиска простого числа, эффективность отсеивания и т.д.) при изменении режима выбора начальных приближений формируемых простых чисел.

2. Методика проверки и оценки характеристик тестов проверки простоты.

Позволяет провести дополнительную проверку правильности реализации тестов, сравнить эффективность тестов по различным параметрам (времени выполнения единичного теста, времени поиска простого числа, эффективность отсеивания) при изменении режима выбора начальных приближений формируемых простых чисел, а также сформулировать предложения по созданию комплексного теста. В процессе исследования тестов необходимо выполнить следующие этапы проверок, проводящиеся отдельно для наиболее часто используемых в настоящее время в криптографических системах длин простых чисел: **1.** Проверить эмпирические вероятности эффективности проверки для заведомо составных чисел (для RSA-модуля $N = P \cdot Q$) при различных значениях k (количества итераций теста); **2.** То же для заведомо простых чисел (например, для используемых в RSA-схеме и в Эль - Гамаля-подобных схемах).

Первые два шага позволяют удостовериться в правильности выполнения тестов и оценить достаточное минимальное значение параметра k для каждого теста и для данной длины формируемых чисел. Проведенные по первым двум этапам исследования показали, что для длин 256 и 512 бит все тесты, кроме теста Лемана, правильно распознают заведомо простые и составные числа даже при $k = 1$. Тест Лемана при малых значениях k может ошибочно браковать простые числа и требует минимально допустимого значения $k = 9$ для 256-битных чисел и $k = 4$ для 512-битных чисел.

3. Оценить эффективности отсеивания различных составных чисел специального вида, трудно обнаруживаемых тестами, при различных значениях параметра k. Для каждого теста определить минимально допустимые значения k для обеспечения оптимальной эффективности отсеивания чисел.

4. Оценить временные характеристики вероятностных тестов на числах различного типа (гарантировано простых и составных, на числах специального вида) и для часто используемых длин.

В нашем случае в качестве чисел специального вида использовались, как указывалось ранее, числа Кармайкла. Как показали исследования (табл. 1, 2), лучшими соотношениями вероятности отсеивания и среднего времени выполнения единичного теста обладают тесты Рабина и Соловея-Штрассена, причем по временным характеристикам тест Рабина значительно лучше, а минимально допустимыми значениями параметра k для эффективного отсеивания чисел Кармайкла являются 5, 10 и 20 для тестов Рабина, Соловея-Штрассена и Лемана.

5. Оценить эффективность отсеивания при различных значениях параметра k при выполнении поиска простых чисел различной длины среди случайных нечетных чисел. Для каждого теста определить минимально допустимые значения k для обеспечения оптимальной эффективности отсеивания составных чисел. Исследования показали: поиск простых чисел среди нечетных случайных чисел неприемлем по значительным временным затратам.

6. Учитывая значительные временные затраты вероятностных тестов при проведении поиска простых чисел среди нечетных случайных чисел и, следовательно, необходимость проведения предварительного быстрого отбора чисел, провести оценку эффективности отсеивания составных чисел частичными тестами деления на одно- и двухбайтовые простые числа при выполнении поиска простых чисел различной длины среди случайных нечетных чисел или другими быстрыми тестами предварительного отбора. Некоторая информация о подобной методике предварительного отсеива-

Таблица 1

Параметр теста	Эмпирическая вероятность отсеивания чисел Кармайкла тестом		
	Лемана	Соловея – Штрассена	Рабина
1	0.9782	0.9340	0.9465
2	0.9664	0.9458	0.9479
3	0.9601	0.9505	0.9536
4	0.9568	0.9525	0.9540
5	0.9555	0.9534	0.9541
10	0.9540	0.9541	0.9541
20	0.9541	0.9541	0.9541

Таблица 2

Параметры тестируемых чисел :		Характеристики вероятностного теста							
		Ферма		Лемана		Соловея - Штрассена		Рабина	
тип	длина (бит)	M_t	D_t	M_t	D_t	M_t	D_t	M_t	D_t
Простые P	256	$1.2 \cdot 10^{-2}$	$1.04 \cdot 10^{-5}$	$1.38 \cdot 10^{-2}$	$2.29 \cdot 10^{-5}$	$1.46 \cdot 10^{-2}$	$2.74 \cdot 10^{-5}$	$0.94 \cdot 10^{-2}$	$1.51 \cdot 10^{-5}$
	512	$8.33 \cdot 10^{-2}$	$4.55 \cdot 10^{-6}$	$8.39 \cdot 10^{-2}$	$7.33 \cdot 10^{-6}$	$9.04 \cdot 10^{-2}$	$7.80 \cdot 10^{-6}$	$7.59 \cdot 10^{-2}$	$5.51 \cdot 10^{-6}$
Случайные составные	256	$1.17 \cdot 10^{-2}$	$5.20 \cdot 10^{-4}$	$1.19 \cdot 10^{-2}$	$5.07 \cdot 10^{-4}$	$1.46 \cdot 10^{-2}$	$6.13 \cdot 10^{-4}$	$1.00 \cdot 10^{-2}$	$1.74 \cdot 10^{-4}$
	512	$8.04 \cdot 10^{-2}$	$7.50 \cdot 10^{-4}$	$7.54 \cdot 10^{-2}$	$7.39 \cdot 10^{-4}$	$7.91 \cdot 10^{-2}$	$7.54 \cdot 10^{-4}$	$5.11 \cdot 10^{-2}$	$0.92 \cdot 10^{-4}$
Случайные нечетные	256	$8.60 \cdot 10^{-3}$	$4.22 \cdot 10^{-4}$	$2.95 \cdot 10^{-3}$	$1.61 \cdot 10^{-4}$	$3.22 \cdot 10^{-3}$	$1.51 \cdot 10^{-4}$	$2.17 \cdot 10^{-3}$	$0.46 \cdot 10^{-4}$
	512	$4.94 \cdot 10^{-2}$	$2.94 \cdot 10^{-4}$	$1.26 \cdot 10^{-2}$	$5.37 \cdot 10^{-4}$	$1.27 \cdot 10^{-2}$	$5.46 \cdot 10^{-4}$	$0.93 \cdot 10^{-2}$	$1.68 \cdot 10^{-4}$
Случ. с дел. на 1 байт	256	$2.30 \cdot 10^{-3}$	$1.17 \cdot 10^{-4}$	$3.80 \cdot 10^{-3}$	$1.94 \cdot 10^{-4}$	$1.76 \cdot 10^{-3}$	$0.94 \cdot 10^{-4}$	$3.06 \cdot 10^{-3}$	$0.74 \cdot 10^{-4}$
	512	$1.47 \cdot 10^{-2}$	$5.83 \cdot 10^{-4}$	$1.30 \cdot 10^{-2}$	$5.32 \cdot 10^{-4}$	$1.41 \cdot 10^{-2}$	$5.64 \cdot 10^{-4}$	$0.86 \cdot 10^{-2}$	$1.59 \cdot 10^{-4}$
Случ. с дел. на 2 байта	256	$2.20 \cdot 10^{-3}$	$1.17 \cdot 10^{-4}$	$2.42 \cdot 10^{-3}$	$1.17 \cdot 10^{-4}$	$1.82 \cdot 10^{-3}$	$0.84 \cdot 10^{-4}$	$3.05 \cdot 10^{-3}$	$0.76 \cdot 10^{-4}$
	512	$1.20 \cdot 10^{-2}$	$5.16 \cdot 10^{-4}$	$1.27 \cdot 10^{-2}$	$5.46 \cdot 10^{-4}$	$1.21 \cdot 10^{-2}$	$5.25 \cdot 10^{-4}$	$1.02 \cdot 10^{-2}$	$1.79 \cdot 10^{-4}$
Кармайкла	до 10б.	$8.01 \cdot 10^{-4}$	$4.03 \cdot 10^{-5}$	$8.00 \cdot 10^{-4}$	$4.08 \cdot 10^{-5}$	$8.50 \cdot 10^{-4}$	$4.35 \cdot 10^{-5}$	$15.4 \cdot 10^{-4}$	$3.94 \cdot 10^{-5}$

M_t — среднее время выполнения единичного теста (в секундах);
D_t — дисперсия времени выполнения единичного теста (в секундах).

ния в настоящее время уже существует и используется [9]. Нашей задачей является определение временных характеристики частичных тестов деления при различных условиях выбора тестируемых чисел (при полностью случайном выборе проверяемых значений и при случайном начальном выборе проверяемого значения с последующим увеличением на 2) и оценка эффективности и оптимального способа предварительного отсеивания в разрабатываемом комплексном методе генерации больших простых чисел.

Как показали исследования (табл. 3, 4), предварительные тесты деления отсеивают среди нечетных случайно выбираемых чисел 81,2 % и 90,8 % составных 256-битных чисел для одно- и двухбайтовых тестов деления соответственно, а для 512-битных чисел 81,5 % и 90,5 % составных чисел соответственно. По временным затратам на поиск простых чисел (для 256 и 512-битных) оптимальным является двухбайтовый тест деления.

7. Определить среднее время поиска простых чисел различной размерности среди случайных нечетных чисел, а также среди случайных нечетных чисел при предварительном использовании частичного одно- и двухбайтового теста деления и оценить процент ошибок при различных значениях параметра k вероятностных тестов.

Как показали исследования, время поиска несущественно зависит от значения параметра k. Для всех тестов, кроме Лемана, даже при $k = 1$ процент ошибок близок к нулю. Для теста Лемана минимально допустимое значение $k = 8$ для 256 - битных чисел и $k = 5$ для 512 - битных чисел.

По временным характеристикам, с учетом эффективности тестов, предпочтительным является тест Рабина. Заметим, что временные характеристики поиска значительно улучшаются при использовании двухбайтового предварительного теста деления. Для примера можно привести следующие данные по тесту Рабина: среднее время поиска простого числа (512 бит) при $k = 100$ составляет 95,83, 21,89, 15,82 с. при использовании случайных нечетных чисел, предварительного теста деления на простые числа в диапазоне 1-го и 2-х байт соответственно. В той же пропорции изменяются временные характеристики и для других тестов.

Таблица 3

Длина числа (бит)	Эффективности отсеивания (в %) для длины простых делителей в пределах			
	1-го байта		2-х байтов	
	Всего отсеяно	Отсеяно из составных	Всего отсеяно	Отсеяно из составных
128	79.71	81.31	89.71	91.84
256	79.73	81.18	89.92	90.81

Таблица 4

Длина тестируемого числа (бит)	Режим выбора числа :	Среднее время поиска при выполнении деления в диапазоне	
		1-го байта	2-х байтов
256	регулярно случайный	$4.9 \cdot 10^{-4}$	$3.37 \cdot 10^{-2}$
	с увеличением случ. значения на 2	$3.9 \cdot 10^{-4}$	$3.71 \cdot 10^{-2}$
512	регулярно случайный	$9.4 \cdot 10^{-4}$	$6.29 \cdot 10^{-2}$
	с увеличением случ. значения на 2	$7.6 \cdot 10^{-4}$	$6.85 \cdot 10^{-2}$

8. Определить среднее время поиска простых чисел различной размерности при увеличении случайно выбранного начального значения тестируемого числа на 2, а также при увеличении случайно выбранного начального значения тестируемого числа на 2 и предварительном использовании одно- и двухбайтового частичных тестов деления.

Как показали эксперименты, при выборе тестируемых чисел с увеличением случайно выбранного начального значения тестируемого числа на 2 временные характеристики несущественно отличаются от варианта поиска при случайном выборе тестируемого числа, что объясняется использованием при проведении экспериментов упрощенного быстрого генератора ПСП, не обеспечивающего требуемого качества характеристик ПСП. Однако в реальных ситуациях, при необходимости использования достаточно сложных генераторов ПСП, обеспечивающих требуемые характеристики начальных приближений, вариант при увеличении случайно выбранного начального значения на 2 чаще всего дает выигрыш во времени.

Проведенные в соответствии с разработанной методикой экспериментальные исследования подтвердили предварительные теоретические выводы о предпочтительности использования вероятностного теста Рабина в качестве одного из составных частей при разработке комплексного теста проверки простоты числа. При разработке комплексного теста поиска простого числа рекомендуется для улучшения временных характеристик использовать предварительное отсеивание с использованием двухбайтового теста деления. Режим выбора проверяемых чисел (случайный или с увеличением на 2) также может влиять на время поиска простого числа и должен анализироваться и выбираться отдельно для каждого используемого генератора ПСП (при большой вычислительной сложности выполнения случайной генерации режим с увеличением случайного начального значения на 2 является более эффективным).

Литература: 1. *Мафтик С.* Механизмы защиты в сетях ЭВМ.- М.: Мир.- 1993.- 216 с. 2. *Уильямс Х.* Проверка чисел на простоту с помощью вычислительных машин // Кибернетический сборник.- Вып. 23.- М.: Мир.- 1986.- С. 51- 99. 3. *Кнут Д.* Искусство программирования для ЭВМ. Т.2. Получисленные алгоритмы.- М.: Мир.- 1977.- 724 с. 4. *Muller W.B., Oswald A.* Dickson Pseudoprimes and Primality Testing // Crypto'85.- P. 512- 516. 5. *Schneier B.* Applied cryptography second edition: protocols, algorithms, and source code in C.- New York: John Wiley & Sons, 1996.- 758 p. 6. *Василенко О.Н.* Современные способы проверки простоты чисел // Кибернетический сборник.- Вып. 25.- М.: Мир.- 1988.- С. 162-188. 7. *Ленстра Х.* Алгоритмы проверки на простоту [по Эдлеману, Румли и Уильямсу] // Алгебра и теория чисел: избранные доклады семинара Н.Бурбаки.- М.: Мир.- 1987.- С. 47- 66. 8. *Бухштаб А.А.* Теория чисел.- М.: Просвещение.- 1966.- 384 с. 9. *Wunderlich M.C.* Computational methods for factoring large integers/ / ABACUS.- No. 2- 1988.- P. 19-33.

Поступила в редакцию 15.12.97

Горбенко Иван Дмитриевич, проф., д-р техн. наук., проректор по научной работе ХТУРЭ. Научные интересы: защита информации в компьютерных системах и сетях. Адрес: 310726, Харьков, пр.Ленина 14, тел. 30-24-50.

Мельникова Оксана Анатольевна, аспирантка кафедры ЭВМ ХТУРЭ. Научные интересы: криптография. Адрес: 310726, Украина, Харьков, пр.Ленина, 14, тел. 30-24-50.