где $q_ч^{min}$ – минимальное количество тепла, отдаваемого поверхностью тела человека, Вт; $q_ч^{max}$ – максимальное количество тепла, отдаваемого поверхностью тела человека, Вт.

Выводы

1. Впервые предложено рассматривать при лучистом теплообмене тело человека как модель, состоящую из геометрических тел.

2. Рассмотрен вопрос обеспечение нормальных условий микроклимата с учетом математического моделирования процессов теплообмена.

3. Впервые предложен критерий асимметричности лучистого теплообмена, который позволяет оценить микроклимат помещений и его влияние на безопасность условий труда.

1.ДСН 3.3.6.042-99. Санітарні норми мікроклімату виробничих приміщень. – К.: МОЗ України, 1993. – 8 с.

2.Губернский Ю.Д., Кореневская Е.И. Гигиенические основы кондиционирования микроклимата жилых и общественных зданий. – М.: Медицина, 1978. – 192 с.

3.Богословский В.Н. Строительная теплофизика (теплофизические основы отопления, вентиляции и кондиционирования воздуха). – 2-е изд., перераб. и доп. – М.: Высш. шк., 1982. – 415 с.

4.Уонг Х. Основные формулы и данные по теплообмену для инженеров. – М.: Атомиздат, 1979. – 187 с.

5.Михеев М.А., Михеева И.М. Краткий курс теплопередачи. – М.-Л.: Госэнергоиздат, 1960. – 208 с.

6.Суринов Ю. А. Лучистый теплообмен при наличии поглощающей и рассеивающей среды // Изв. АН СССР. ОТН. – 1952. – № 9. – С.1331-1352.

7.Ритшель Г., Гребер Г. Руководство по отоплению и вентиляции. Т.1, 2. – М.-Л.: Госстройиздат, 1932. – 391 с.

8.Чесанов Л.Г., Петренко В.О., Петренко А.О. Строительство, материаловедение, машиностроение // Сб. науч. трудов. Вып. 46. – Днепропетровск: ПГАСА, 2008. – С.29-35.

Получено 14.03.2011

УДК 517.962.27 : 004.056.55

В.Б.УФИМЦЕВА, Н.Ю.КАРПЕНКО, кандидаты техн. наук
Харьковская национальная академия городского хозяйства

ОБЕСПЕЧЕНИЕ БЕЗОПАСНОСТИ ИНФОРМАЦИИ В КОМПЬЮТЕРНЫХ СИСТЕМАХ С ИСПОЛЬЗОВАНИЕМ ТЕОРИИ ЧИСЕЛ ФИБОНАЧЧИ

Рассматривается целесообразность использования аппарата арифметики Фибоначчи в криптографии. А точнее, построение симметричного блочного преобразования с использованием обобщенных чисел и матриц Фибоначчи. Показана перспективность этого направления исследований в рамках совершенствования статистических показате-

лей симметричных криптографических преобразований информации за счет ускорения диффузионных процессов при использовании в схемах обмена подблоками сети Фейстеля матричного преобразования Фибоначчи.

Розглядається доцільність використання апарату арифметики Фібоначчі в криптографії. Точніше, побудова симетричного блочного перетворення інформації з використанням узагальнених чисел і матриць Фібоначчі. Показана перспективність цього напрямку досліджень в рамках удосконалення статистичних показників криптографічних перетворень за рахунок збільшення дифузії при використанні в схемах обміну підблоками мережі Фейстеля матричного перетворення Фібоначчі.

The article is devoted to the development of the symmetrical transformation of information which is characterized by the improved indices of mixing. The possibilities of applying the mathematical apparatus of the theory of Fibonacci's numbers for fulfilling the operations of cryptographic conversions are analyzed. Practical principles are developed and the properties of the cryptographic transformations of information with the use for the procedures of the coding of the mathematical of the generalized numbers and matrices of Fibonacci are analyzed.

Ключевые слова: симметричные криптографические системы, числа Фибоначчи, сети Фейстеля.

Широкое применение компьютерных технологий как в автоматизированных системах обработки информации и управления, так и в частной жизни, привели к тому, что одним из аспектов обеспечения безопасности жизнедеятельности стала проблема сохранности личной, банковской, финансовой информации, циркулирующей в компьютерных системах, от несанкционированного доступа. Особенно это актуально для объектов, злоумышленное вскрытие информационной системы которых может привести к серьезным катастрофам.

Радикальное решение проблем защиты электронной информации может быть получено на базе использования криптографических методов, которые позволяют решать важные задачи защищенной автоматизированной обработки и передачи информации: конфиденциальности – путем лишения противника возможности извлечь информацию; целостности – путем лишения противника возможности изменить сообщение так, чтобы изменился его смысл, или ввести ложную информацию.

Как известно, современные шифры строятся как итерационные, и основное внимание исследователей сосредоточено на исследовании свойств булевых функций и нестойких процедур перестановок с целью улучшения показателей перемешивания (по Шеннону) [1]. Необходимым условием стойкости шифра является достижение полной диффузии. Важную роль в процессе диффузии в блоковых шифрах играют схемы обмена подблоками (СО) и F -функций, так называемые сети Фейстеля (СФ), анализ которых приведен в [2, 3].

Основным объектом исследований стали обобщенные числа Фи-

боначчи [4], называемые *p*-числами и целесообразность их использования в СФ.

Числа Фибоначчи являются линейной рекуррентной последовательностью порядка $k = p+1$ с законом рекурсии

$$F_p(i+p+1) = F_p(i+p) + F_p(i), \quad (1)$$

где $p \in Z \cap p \geq 0$ и $k \in Z$. При начальных условиях:

$$F_p(1) = F_p(2) = \ldots = F_p(p+1) = 1. \quad (2)$$

В данной работе сосредоточено внимание на возможностях улучшения показателей перемешивания на основе использования математического аппарата теории чисел Фибоначчи. В соответствии с темой работы ставится цель исследовать целесообразность применения теории чисел и матриц Фибоначчи при построении симметричных алгоритмов криптографического преобразования информации.

Для достижения поставленной цели в работе ставятся и решаются следующие задачи:

1) изучение возможностей применения математического аппарата теории чисел Фибоначчи для выполнения операций криптографических преобразований;
2) разработка практических принципов и анализ свойств криптографических преобразований информации при использовании для процедур шифрования обобщенных чисел Фибоначчи;
3) анализ и исследование показателей статистической безопасности при построении симметричных алгоритмов криптографических преобразований с использованием обобщенных чисел Фибоначчи;
4) выработка практических рекомендаций по использованию криптографических преобразований на основе обобщенных чисел Фибоначчи при построении шифров с улучшенными показателями перемешивания.

При анализе основных свойств матриц Фибоначчи показано, что использование в криптографических преобразованиях умножения матрицы данных на Q_p^n-матрицу Фибоначчи снижает вычислительную сложность преобразования $C(p)$, оцененную числом операций умножения, на $(p+1)^3$, так как операция умножения произвольной матрицы M размером $(p+1)\times(p+1)$ на Q_p^n-матрицу Фибоначчи (и, соответственно, операция возведения матрицы Фибоначчи в степень) сводятся к простым операциям сложения и сдвига.

Отмечено важное свойство матриц, которое состоит в том, что матрицы Фибоначчи являются невырожденными, так как детерминант матрицы Q_p^n равен $(-1)^{pn}$ [4]. Это свойство определяет возможность использования матриц Фибоначчи для многих приложений, и в частности, для криптографических преобразований информации.

Линейность операции умножения на матрицу Фибоначчи определила область исследования диссертационной работы в рамках применения арифметики Фибоначчи в схемах обмена подблоками симметричных методов преобразования, а в качестве оценки эффективности – показатели перемешивания.

Анализ свойств матриц Фибоначчи выявил основное препятствие, стоящее на пути их использования для операций криптографического преобразования, – операции умножения на матрицу Фибоначчи и вычисления детерминанта приводят к большой избыточности информации.

Исследования показали, что избыточность, возникающая при использовании в преобразованиях информации арифметики Фибоначчи, обратно пропорциональна порядку p матрицы Фибоначчи, но быстро возрастает при увеличении значения степени n матрицы.

Установлено, что проведения вычислений в кольце целых чисел $Z/(q)$ устраняет проблему возникновения избыточности информации при использовании обобщенных матриц Фибоначчи. Достоверность этого факта была установлена путем строгого математического доказательства выдвинутой гипотезы о гомоморфизме p-чисел и Q_p-матриц Фибоначчи в кольце целых чисел $Z/(q)$.

В ходе исследования был предложен вариант реализации симметричного шифра на основе модифицированной сети Фейстеля с использованием арифметики Фибоначчи. В традиционных схеме Фейстеля F-функция является наиболее (в вычислительном смысле) дорогой операцией в раунде и также играет ключевую роль в диффузионном процессе из-за ее свойства полноты. Поэтому оценка полной диффузии проводилась в терминах объема требуемых вычислений F-функций.

В результате проведенного анализа наиболее подходящей структуры СФ (с точки зрения диффузионного процесса) была выбрана схема смешивания функций с замкнутой цепочкой F-функций, зависящих от двух подблоков (предыдущего текущему подблока и последующего). Первый цикл делает три последних подблока полными, следующий раунд делает все другие подблоки полными. Следователь-

но, достаточно только двух раундов для полной диффузии, или более конкретно вычисления $2n$-3 F -функций.

В соответствии с целью работы была исследована целесообразность использование в СО умножения на матрицу Фибоначчи.

Были проведены исследования схем преобразования информации с использованием матриц Фибоначчи 1-го порядка (4 подблоков, аналогично RC6), 2-го порядка (9 подблоков) и сделано обобщение для схемы с N подблоками.

Проведенный анализ показал, что при использовании матриц Фибоначчи для достижения полной диффузии требуется выполнение меньшего числа раундов по сравнению с методами, не использующими такие преобразования. Таким образом, усиление процесса диффузии позволяет создавать на основе этого метода алгоритмы, быстродействие которых может быть увеличено за счет уменьшения количества итераций.

По разработанной схеме при порядке матрицы Фибоначчи $p=1$ с использованием нелинейной функции циклического сдвига шифра RC6 был построен алгоритм криптографического преобразования информации.

Результаты статистического анализа критериев строгого лавинного критерия, сбалансированности, корреляции между входом и выходом алгоритма и корреляционного иммунитета подтвердили сохранение статистической стойкости метода. Таким образом, более быстрое протекание диффузионных процессов в предложенном алгоритме дает возможность уменьшения числа итераций и, как следствие, увеличения скорости обработки данных.

Таким образом, в ходе исследования получены следующие результаты:

- выдвинута и доказана гипотеза о сохранении рекуррентных соотношений и операций для p-чисел и Q_p-матриц Фибоначчи в фактор-кольце $Z/(q)$, что позволяет при использовании теории чисел Фибоначчи избежать возникновения избыточности информации;
- разработан новый метод криптографического преобразования информации с улучшенными показателями перемешивания, который заключается в умножении входного блока данных на обобщенную матрицу Фибоначчи в фактор-кольце $Z/(q)$;
- предложена модифицированная RC6-подобная криптографическая процедура с использованием предложенного метода построения

цикловой функции и показано повышение показателей ее статистической безопасности.

Полученные научные результаты исследования позволили обосновать в качестве одного из перспективных направлений совершенствования процедур шифрования использование матричного преобразования Фибоначчи.

Разработаны алгоритмы и программные средства с использованием обобщенных чисел и матриц Фибоначчи в схемах криптографических преобразований и показано, что их применение в сочетании с другими процедурами расширяет возможности улучшения статистических показателей криптографических алгоритмов, позволяет добиться увеличения скорости обработки данных за счет уменьшения количества раундов.

1.Бабаш А.В., Шанкин Г.П. Криптография. – М.: Солон-Р, 2002. – 512 с.

2.Nakahara J. Jr., Vandewalle J., Prenceel B. Diffusion analysis of Feistel Networks (Extended version). – Belgium: Katholieke Universiteit Leuven, div. E.S.A.T. – SISTA/COSIC. – 18 p.

3.Nechvatal J., Barket E., Bassham L., Burr W., Dworkin M., Foti J., Roback E. Report on the Development of the Advanced Encryption Standard (AES) // Computer Security Division; Information Technology Laboratory; NIST: Technology Administration; U.S. Department of Commerce. – 2000. – 116 p.

4.Stakhov A.P., Massingue V., Sluchenkova A. Introduction into Fibonacci coding and cryptography. – Kharkiv: Osnova, 1999. – 236 p.

Получено 10.03.2011

УДК 519.6

А.Л.ШАПОВАЛОВ, Н.В.ГРИНЧАК, кандидаты техн. наук,
Е.В.КУЗЬМИЧЕВА
Харьковская национальная академия городского хозяйства

ИНФОРМАЦИОННЫЕ МОДЕЛИ И ТЕХНОЛОГИИ В УПРАВЛЕНИИ СИСТЕМОЙ БЕЗОПАСНОСТИ ЖИЗНЕДЕЯТЕЛЬНОСТИ

Рассматриваются механизм и технология построения структурно-функциональных и математических моделей, их анализ для целей управления и взаимосвязь для более обоснованного и эффективного принятия решений по управлению безопасности жизнедеятельности.

Розглядаються механізм і технологія побудови структурно-функціональних і математичних моделей, їх аналіз і взаємозв'язок для більш обгрунтованого і ефективного ухвалення рішень по управлінню безпеки життєдіяльності.

For more reasonable and effective acceptance of decisions on the management of safety of vital functions, the mechanism of construction is examined structurally-functional and mathematical models, their analysis for the aims of management and intercommunication.