АНАЛИЗ ВЛИЯНИЯ ПАРАМЕТРОВ НЕПОЗИЦИОННОГО ШИФРА НА ЕГО НАДЕЖНОСТЬ

С. Е. Нысанбаева, М. М. Мағзом, А. Б. Кабылханов

Институт информационных и вычислительных технологий КН МОН РК

УДК 004.056.5

Приводятся результаты исследования разработанного блочного алгоритма шифрования на предмет его криптостойкости. Этот алгоритм разработан на основе сети Фейстеля, режима шифрования США «Режим сцепления блоков по шифртексту» и системы шифрования на базе непозиционных полиномиальных систем счисления. Проведен анализ его статистических свойств.

Ключевые слова: шифрование, непозиционные полиномиальные системы счисления, модулярная арифметика, тесты, псевдослучайные последовательности, статистические свойства, программирование.

В Институте информационных и вычислительных технологий (ИИВТ) Министерства образования и науки Республики Казахстан выполняются работы по созданию, исследованию и реализации криптографических алгоритмов защиты хранимой и передаваемой информации. Эти алгоритмы разрабатываются с использованием непозиционных полиномиальных систем счисления (НПСС) или модулярных систем счисления.

При разработке блочных алгоритмов шифрования одним из используемых криптографических преобразований является многократная, состоящая из нескольких циклов (раундов), обработка одного блока открытого текста. В каждом цикле данные подвергаются криптографическому преобразованию при участии вспомогательного ключа, полученного из заданного секретного ключа. Выбор числа циклов определяется требованиями по криптостойкости блочного шифра и эффективности его реализации. Как правило, чем больше циклов, тем выше криптостойкость, но при может снижаться эффективность реализации блочного шифра [1].

Многие современные блочные алгоритмы шифрования построены на основе сети Фейстеля или подстановочно-перестановочной сети (SP-сеть, которая также предложена Хорстом Фейстелем). По своей сути сеть Фейстеля является альтернативой SP-сетям и используется намного шире. На основе сети Фейстеля построены американский стандарт DES и российский стандарт ГОСТ 28147-89 [2], а на базе SP-сетей разработан стандарт AES. Но сеть Фейстеля не потеряла своей актуальности, так как зашифрование и расшифрование могут проводится одним и тем же устройством, но с обратным порядком используемых ключей [3].

Цель данной работы - исследовать влияние на свойства алгоритма шифрования, разработанного на базе НПСС [4, 5], применения дополнительных криптографических преобразований (или процедур) таких, как сеть Фейстеля и режим блочного шифрования «Режим сцепления блоков по шифртексту». Таким образом, исследуемый алгоритм криптографического преобразования построен на основе системы непозиционного шифрования (т.е. на базе НПСС), сети Фейстеля и режима «Режим сцепления блоков по шифртексту» [6]. Назовем эти 3 криптопреобразования «составляющими процедурами» разработанного алгоритма шифрования, схема которого показана на рис. 1.

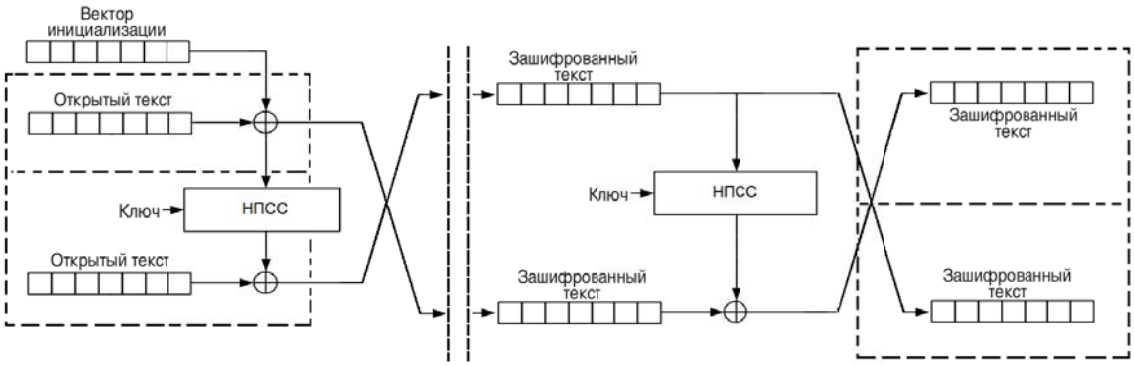

Рис. 1. Схема криптографического преобразования одного блока
в рассматриваемом алгоритме шифрования на базе НПСС

В данной работе приведены результаты исследования влияния сети Фейстеля и режима «Режим сцепления блоков по шифртексту» на надежность разработанного криптоалгоритма и его статистические свойства по получаемым криптограммам.

Анализ разработанного алгоритма шифрования позволил выявить достоинства и недостатки «составляющих процедур» алгоритма. При шифровании выявлялась зависимость между зашифрованными блоками двух соседних раундов шифрования. Исследовалось также влияние изменения размера блока и количества раундов на характеристики зашифрованных блоков для каждого раунда. Такой подход позволяет построить алгоритм, обеспечивающий его криптографическую безопасность. Выходные данные тестируемого алгоритма по своим вероятностным характеристикам должны быть близки к случайной последовательности. Таким образом, варьируя длину блока и количество раундов при шифровании можно существенно улучшить надежность разработанного алгоритма шифрования.

Для исследования статистической безопасности разработанного алгоритма шифрования использованы следующие тесты [7, 8]:

– оценочный тест «Overlapping Template Matching Test»;

– графический тест «Проверка серий».

В оценочных тестах статистические свойства последовательностей определяются конкретными числовыми величинами, которые позволяют однозначно сделать вывод о том, пройден тест или нет.

С помощью теста «Overlapping Template Matching Test» выполняется проверка последовательности на случайность, путем анализа количества повторяющихся серий длины m бит перекрывающих предыдущую серию на $m - k$ бит. Данный тест позволяет оценить равномерность распределения символов в исследуемой последовательности на основе выбранной серий длины m бит, и их сцепления выбранным сдвигом на k бит. В рассматриваемом случае длина серии $m=3$, сдвиг $k=2$.

Анализ алгоритма был произведен для длин блоков 64, 128, 256 бит и количестве раундов 8, 16, 32 для каждой из указанных длин блока. Для оценки полученного результата используется таблицы распределения хи-квадрат .

В методике оценки результатов Д. Кнут предлагает считать последовательности, для которых вероятность появления данного результата лежит в интервалах [0; 0,01] и [0,99; 1] - неслучайными, (0,01; 0,1] и [0,9; 0,99) - подозрительными на случайность, (0,1; 0,9) - случайными. Таким образом, для истинно случайной последовательности вероятность должна стремиться к 0,5. Полученные результаты приведены в табл. 1, 2.

Таблица 1 – Сравнение исходного и зашифрованного файла

Значения χ^2 квадрат	Исходный файл	Количество раундов		
		8	16	32
	Длина блока - 64 бит			
1	7,375	5,875	13,375	6,125
	Длина блока - 128 бит			
2	13,4375	23,44	6,1875	8,6875
	Длина блока - 256 бит			
3	25,844	4,594	9,844	3,719

Таблица 2 – Распределение χ^2 с числом степени свободы, равным 7

Длина блока - 64 бит				
Количество раундов	χ^2	$[\chi^2_\alpha;\chi^2_\beta]$	$[p_\alpha; p_\beta]$	Оценка
8	5,875	4,67-6,35	0,70-0,50	случайный
16	13,375	12,0-14,1	0,10-0,05	подозрительный
32	6,125	4,67-6,35	0,70-0,50	случайный
Длина блока - 128 бит				
Количество раундов	χ^2	$[\chi^2_\alpha;\chi^2_\beta]$	$[p_\alpha; p_\beta]$	Оценка
8	23,44	22,6-24,3	0,002-0,001	неслучайный
16	6,1875	4,67-6,35	0,70-0,50	случайный
32	8,6875	8,4-9,8	0,30-0,20	случайный
Длина блока - 256 бит				
Количество раундов	χ^2	$[\chi^2_\alpha;\chi^2_\beta]$	$[p_\alpha; p_\beta]$	Оценка
8	4,594	3,82-4,67	0,80-0,70	случайный
16	9,844	9,8-12,0	0,20-0,10	случайный
32	3,719	2,83-3,82	0,90-0,80	случайный

В графических тестах статистические свойства исследуемых последовательностей отображаются в виде графических зависимостей. По их виду делают выводы о свойствах исследуемой последовательности для определения зависимости между элементами и для оценки равномерности распределения символов. Эти тесты позволяют наглядно представить изменение статистических характеристик получаемых криптограмм разработанного алгоритма шифрования в зависимости от параметров шифрования (длины блока и количества раундов).

В тесте «Проверка серий» оценивается равномерность распределения символов в проверяемой последовательности на основе анализа частоты появления серий, состоящих из k бит, k=1,2,3,4. Для построения графика теста исследуемой последовательности определяется, сколько раз встречаются в ней нули и единицы (k =1), серии-двойки (00, 01, 10, 11: k =2), серии-тройки (000, 001, 010, 011, 100, 101, 110, 111: k =3) и т.д. У последовательности, чьи статистические свойства близки к свойствам истинно случайной последовательности, разбросы между числом появлений нулей и единиц, между числом появлений серий-пар каждого вида должны стремиться к нулю. На рис. 2–4 приведены результаты тестирования для серий из 8 бит, полученных для разного количества раундов.

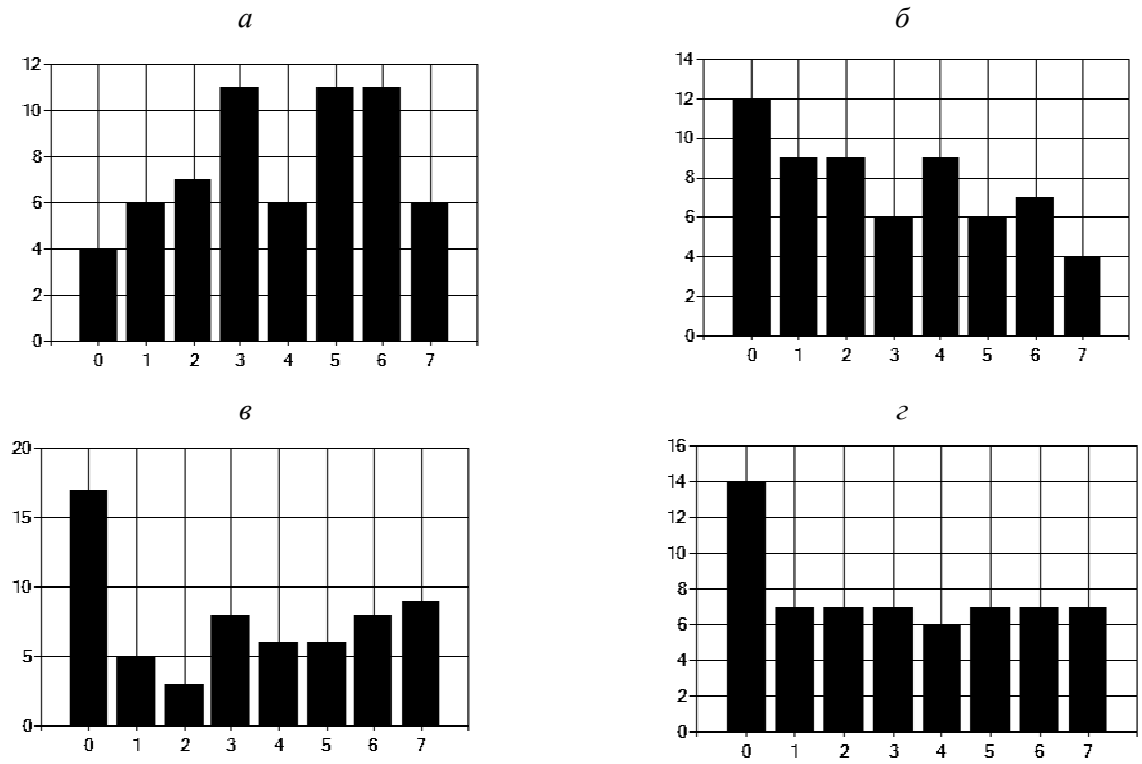

Рис. 2. Результаты теста «Проверка серии»:
исходный файл размером блока 64 бит (*а*); зашифрованные файлы
после преобразования: 8-й раунд (*б*), 16-й раунд (*в*), 32-й раунд (*г*)

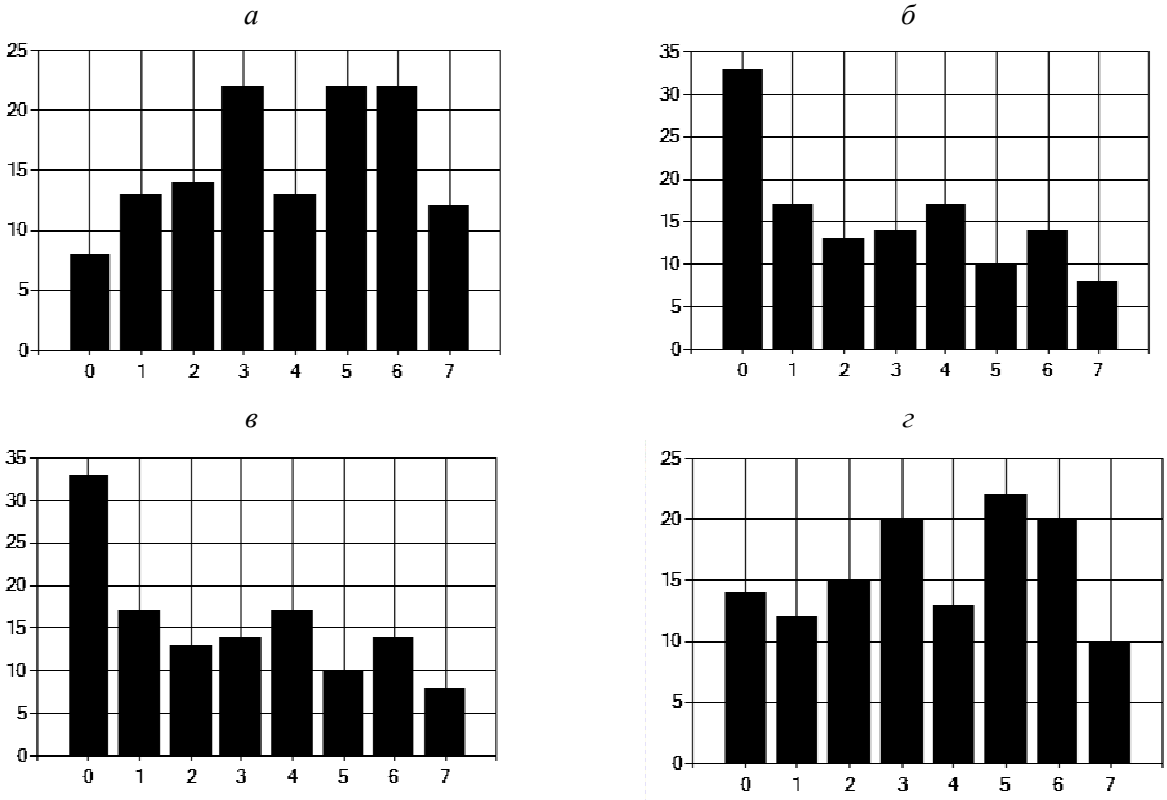

Рис. 3. Результаты теста «Проверка серии»:
исходный файл размером блока 128 бит (*а*), зашифрованные файлы
после преобразования: 8-й раунд (*б*), 16-й раунд (*в*), 32-й раунд (*г*)

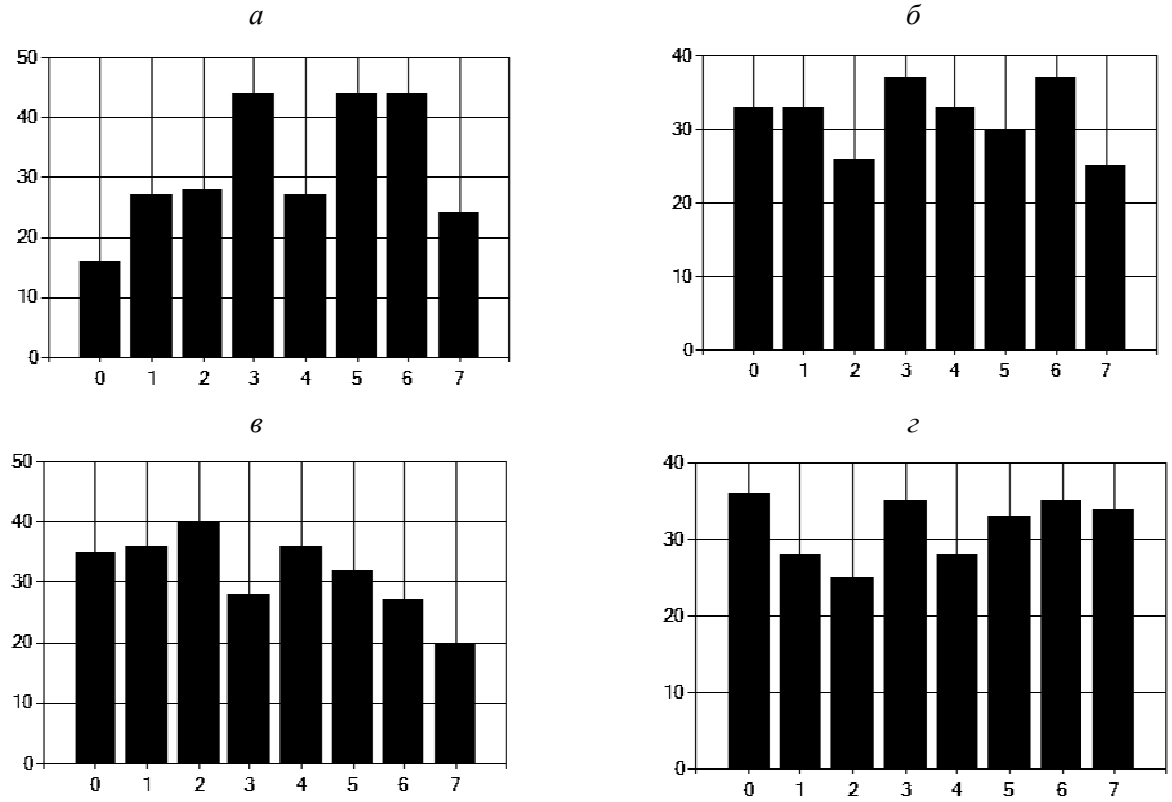

Рис. 4. Результаты теста «Проверка серии»:
исходный файл размером блока 256 бит (*а*), зашифрованные файлы
после преобразования: 8-й раунд (*б*), 16-й раунд (*в*), 32-й раунд (*г*)

Тестирование криптограмм, полученных для разного размера шифруемых блоков файлов, реализующих непозиционный алгоритм шифрования на базе НПСС, показали, что результаты тестирования зависят от структуры входных параметров.

По проведенным тестам анализа статистических свойств предложенного алгоритма шифрования можно сделать следующие выводы:

– применение к непозиционному алгоритму шифрования на базе НПСС таких «составляющих процедур», как сеть Фейстеля и режим блочного шифрования «Режим сцепления блоков по шифртексту», улучшило равномерность распределения бит в зашифрованном блоке длиной 256 бит (рис.4);

– использование вектора инициализации также способствует более равномерному распределению символов в шифртексте, что делает невозможным предсказывать выходную последовательность алгоритма при манипулировании входными данными.

Заключение. Полученные результаты проведенного анализа статистических свойств зашифрованных файлов показывают, что применение представленных подходов к построению блочных алгоритмов шифрования по количеству раундов и размеру блока данных, является целесообразным.

Список литературы

1. Recommendation for Block Cipher Modes of Operation // NIST Special Publication 800-38A. Technology Administration U.S. Department of Commerce. - 2001. - P.10.

2. ГОСТ 28147-89. Система обработки информации. Защита криптографическая. Алгоритм криптографического преобразования. - М.: Госон на работае СССР, 1989.

3. FIPS 46-3. Data Encryption Standard (DES). - USA, NIST, 1977.

4. Biyashev R., Nyssanbayeva S., Algorithm for Creation a Digital Signature with Error Detection and Correction, Cybernetics and Systems Analysis, No. 4, 2012. PP. 489-497.

5. Biyashev R., Kalimoldayev M., Nyssanbayeva S., Magzom M., Development of an encryption algorithm based on nonpositional polynomial notations // Proceedings of the International Conference on Advanced Materials Science and Environmental Engineering (AMSEE 2016). - Chiang Mai, Thailand, June 2016, PP. 243-245.

6. Калимолдаев М. Н., Кабылханов А. Б., Магзом М. М., Нысанбаева С. Е. Построение модели для системы шифрования, разработанной на базе модулярной арифметики // Вестник КазНУ. Серия математика, механика, информатика - Алматы, 2016. №3/1(90). - С. 30-40.

7. М. А. Иванов, И. В. Чугунков. Теория, применение и оценка качества генераторов псевдослучайных последовательностей. - М.: К-ОБРАЗ, 2003. - 136 с.

8. A Statistical Test Suite for Random and Pseudorandom Number Generators for Cryptographic Applications /A. Rukhin, J. Soto at al. // NIST Special Publication 800. 22, 2001. P. 48 -50.

Нысанбаева Сауле Еркебулановна – д-р техн. наук, гл. науч. сотр. Института информационных и вычислительных технологий КН МОН РК;
050010, Алматы; e-mail: sultasha1@mail.ru;
Мағзом Мирас Мұхтарұлы – Ph.D., зам. ген. директора Института информационных и вычислительных технологий КН МОН РК;
050010, Алматы; e-mail: magzommx@gmail.ru;
Кабылханов Адылжан Бердыбекулы – магистрант, инж. Института информационных и вычислительных технологий КН МОН РК;
050010, Алматы; e-mail: faircisco@gmail.ru.