Институт вычислительной математики и математической геофизики СО РАН
Институт информационных и вычислительных технологий КН МОН РК
Тринадцатая международная азиатская школа-семинар
«Проблемы оптимизации сложных систем»

Тема: Анализ влияния параметров непозиционного шифра на его надежность

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

г. Новосибирск, 2017 г.

Введение

В Институте информационных и вычислительных технологий МОН РК выполняются работы по созданию, исследованию и реализации криптографических алгоритмов защиты хранимой и передаваемой информации.

Алгоритмы разрабатываются с использованием непозиционных полиномиальных систем счисления (НПСС) или модулярных систем счисления.

Цель работы заключается в исследовании влияния параметров на свойства алгоритма шифрования, разработанного на базе НПСС, применения дополнительных криптографических преобразований (или процедур) таких, как сеть Фейстеля и режим блочного шифрования «Режим сцепления блоков по шифртексту».

Задачи:

- разработать компьютерную программу для применения дополнительных криптографических преобразований к системе шифрования на базе НПСС;
- провести анализ статистических свойств получаемых криптограмм с использованием графического и оценочного теста.

Научная новизна полученных результатов состоит в разработке моделей алгоритма шифрования на базе НПСС с целью их использования на практике:

- применение к алгоритму шифрования на базе НПСС дополнительных криптографических преобразований;
- разработка программной реализаций для модели «криптографические преобразования - нетрадиционное шифрование»;
- анализ и сравнение статистических характеристик получаемых криптограмм.

Непозиционные системы счисления

В классических системах остаточных классов (СОК) целые положительные числа представляются в виде набора остатков (вычетов), полученных от их деления на основания СОК. В соответствии с Великой китайской теоремы об остатках представление числа в виде последовательности вычетов будет единственным, если основания будут попарно просты между собой.

Объем диапазона представимых чисел равен $P = p_1 p_2 \cdots p_n$.

Целое положительное число N представляется в виде последовательности чисел $N = (\alpha_1, \alpha_2, ..., \alpha_n)$, α_i – это вычет (остаток) от его деления N на основания $p_1, p_2, ..., p_n$:

$$\alpha_i = N - \left[\frac{N}{p_i}\right] p_i, \; i = \overline{1, n},$$

Цифра i-го разряда α_i числа N есть наименьший положительный остаток от деления N на p_i и $\alpha_i < p_i$.

Отличие от позиционной системы счисления: образование цифры каждого разряда производится независимо друг от друга. Представление числа N в виде последовательности цифр $\alpha_1, \alpha_2, ..., \alpha_n$ будет единственным, если числа p_i попарно просты между собой.

Системы симметричного блочного шифрования на базе непозиционных полиномиальных систем счисления

Рассматриваемый алгоритм шифрования создается в полиномиальных системах счисления в остаточных классах, в которых основаниями служат неприводимые многочлены над полем *GF*(2).

Полиномы с двоичными коэффициентами можно также представить в виде последовательности вычетов, полученных в результате их деления на выбранную систему полиномиальных оснований.

Нетрадиционные методы и алгоритмы криптографии, построенные на базе непозиционных полиномиальных систем счисления, позволяют существенно повысить надежность алгоритма шифрования.

Криптостойкость в этом случае определяется полным ключом, зависящим не только от длины ключа (ключевой последовательности), но и от выбранной системы полиномиальных оснований, а также от количества перестановок оснований в системе.

Схема криптографического преобразования

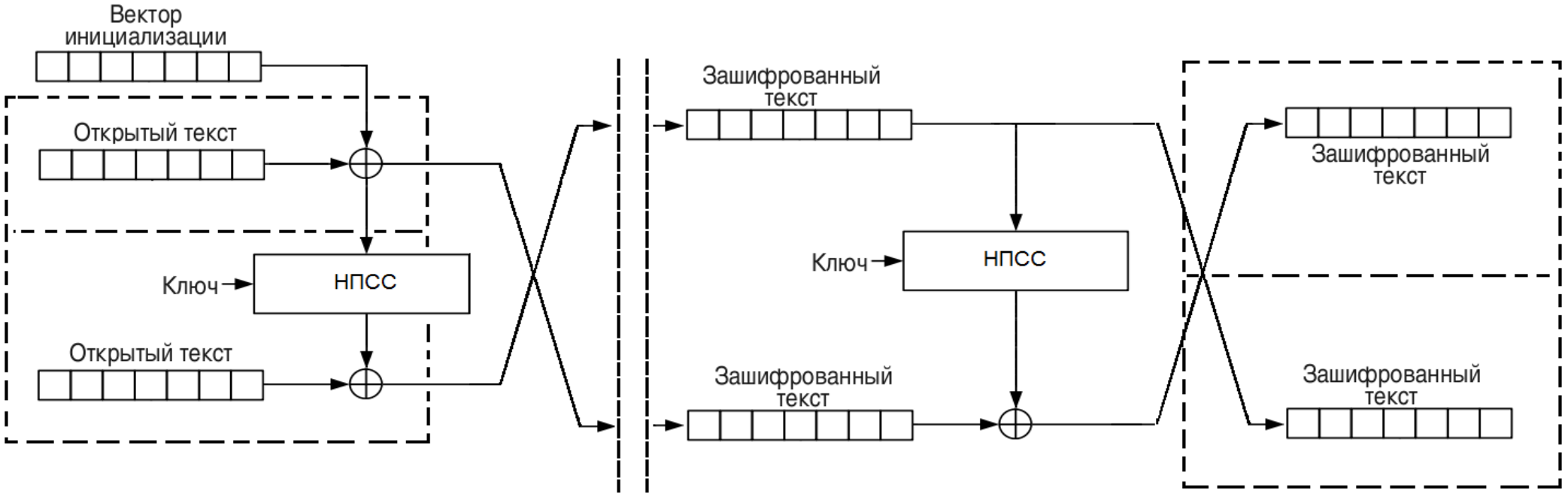
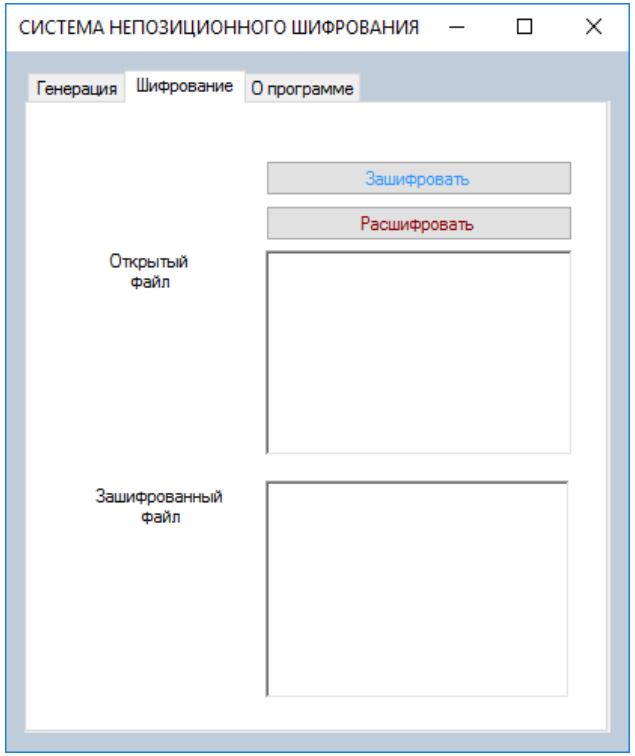
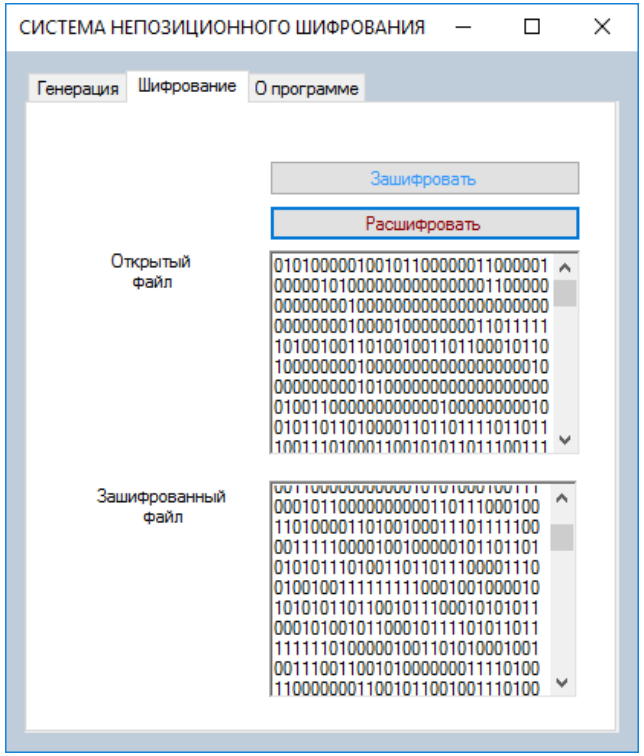


Рисунок 1 - Схема криптографического преобразования одного блока в рассматриваемом алгоритме шифрования на базе НПСС

Программная реализация для применения криптографических преобразований к системе шифрования на базе НПСС



а)



б)

Рисунок 2 - а) главное окно программы и б) процедуры шифрования и расшифрования криптограмм

Тестирование и анализ статистических характеристик криптограмм алгоритмов криптографического преобразования

Для анализа статистических свойств получаемых криптограмм использована разработаннная программа «Автоматизированная система подборки статистических тестов Д. Кнута и графических тестов».

Программа предназначена для исследования статистических свойств шифртекстов и генерируемых псевдослучайных последовательностей на графических и оценочных тестах.

Для исследования статистической безопасности разработанного алгоритма шифрования использованы следующие тесты:

- оценочные: «Overlapping Template Matching Test»;
- графические: «Проверка серий».

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 χ^2.

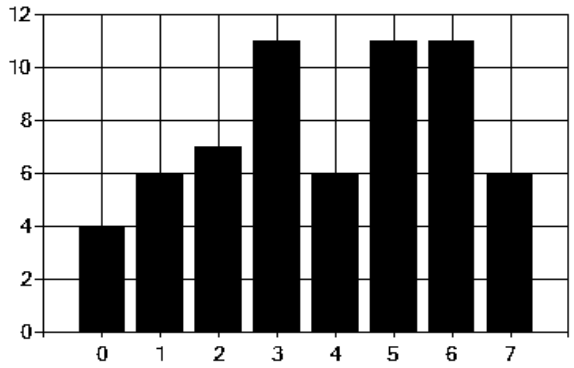
Значения χ^2 квадрат	Исходный файл	Количество раундов		
		8	16	32
	Длина блока - 64 бит			
1	7,375	5,875	13,375	6,125
	Длина блока - 128 бит			
2	13,4375	23,44	6,1875	8,6875
	Длина блока - 256 бит			
3	25,844	4,594	9,844	3,719

Таблица 1 - Сравнение исходного и зашифрованного файла

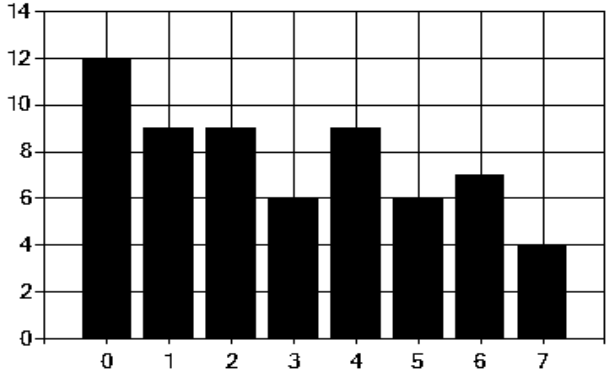
Длина блока - 64 бит				
Количество раундов	χ^2	$[\chi^2_\alpha;\chi^2_\beta]$	$[p_\alpha; p_\beta]$	Оценка
8	5,875	4,67-6,35	0,70-0,50	случайный
16	13,375	12,0-14,1	0,10-0,05	подозрительный
32	6,125	4,67-6,35	0,70-0,50	случайный
Длина блока - 128 бит				
Количество раундов	χ^2	$[\chi^2_\alpha;\chi^2_\beta]$	$[p_\alpha; p_\beta]$	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

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

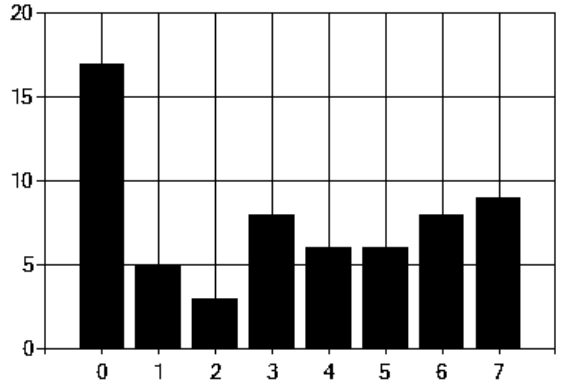
Тест «Проверка серий»



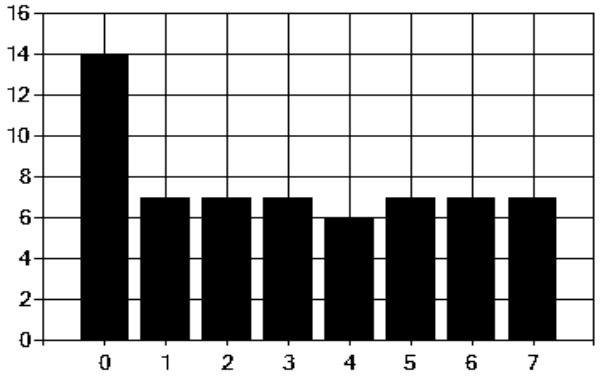
а)



б)



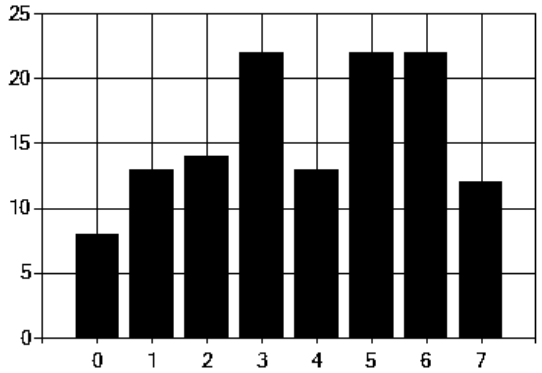
в)



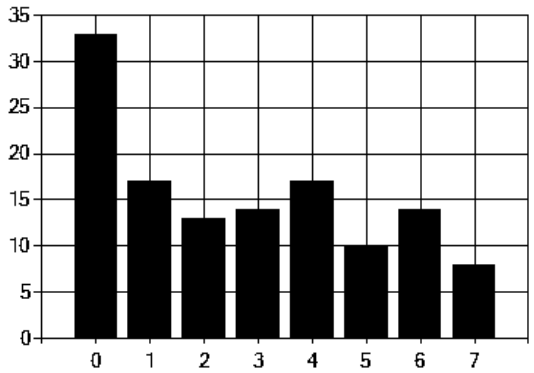
г)

Рисунок 3 - Результаты теста «Проверка серии»: исходный файл размером блока 64 бит (а), зашифрованные файлы после преобразования: 8 раунд (б), 16 раунд (в), 32 раунд (г)

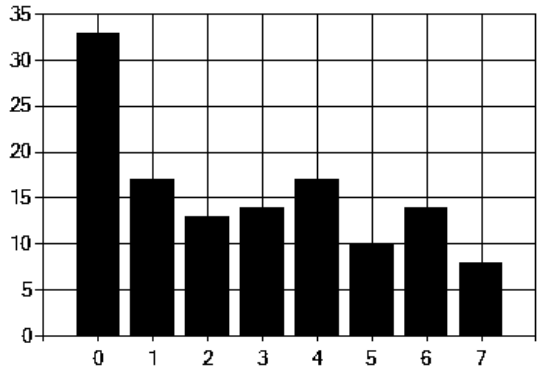
Тест «Проверка серий»



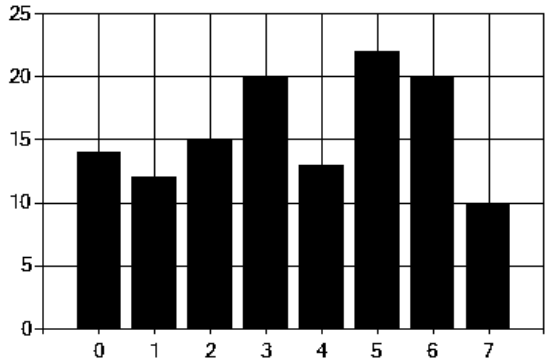
а)



б)



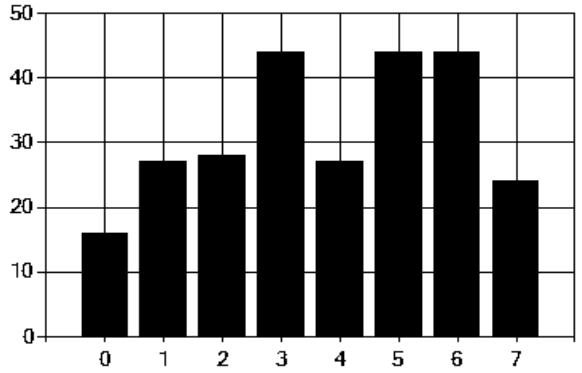
в)



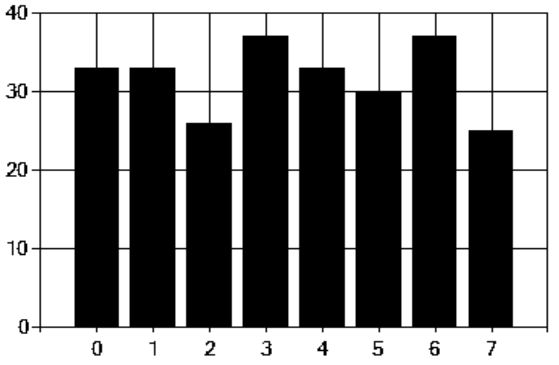
г)

Рисунок 4 - Результаты теста «Проверка серии»: исходный файл размером блока 128 бит (а), зашифрованные файлы после преобразования: 8 раунд (б), 16 раунд (в), 32 раунд (г)

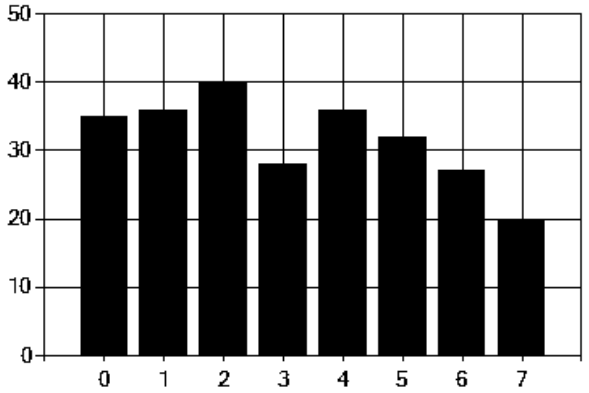
Тест «Проверка серий»



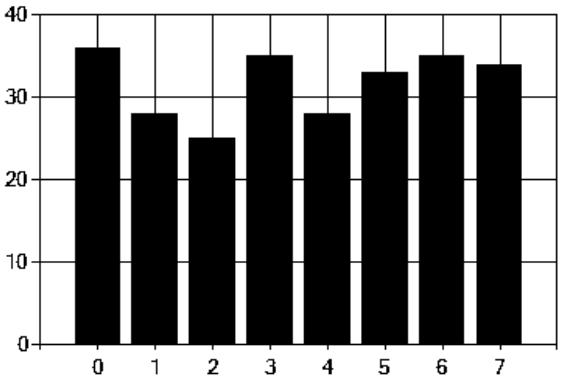
а)



б)



в)



г)

Рисунок 5 - Результаты теста «Проверка серии»: исходный файл размером блока 256 бит (а), зашифрованные файлы после преобразования: 8 раунд (б), 16 раунд (в), 32 раунд (г)

ЗАКЛЮЧЕНИЕ

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.

При выполнении данной работы получены следующие результаты:

1. Рассмотрен симметричный блочный алгоритм шифрования, разработанный с использованием непозиционных полиномиальных систем счисления (НПСС).
2. Предложена и программно реализована модель системы блочного шифрования на базе НПСС.
3. Проведено исследование статистической безопасности зашифрованных файлов различной структуры с использованием оценочных и графических тестов.

Спасибо за внимание!