УДК 621. 3.06

В.И. Долгов, А.А. Настенко

Харьковский национальный университет радиоэлектроники, Харьков

БОЛЬШИЕ ШИФРЫ – СЛУЧАЙНЫЕ ПОДСТАНОВКИ. ПРОВЕРКА СТАТИСТИЧЕСКИХ СВОЙСТВ ШИФРОВ, ПРЕДСТАВЛЕННЫХ НА УКРАИНСКИЙ КОНКУРС С ПОМОЩЬЮ НАБОРА ТЕСТОВ NIST STS

Представляются материалы по дополнительному обоснованию справедливости гипотезы о том, что большие шифры асимптотически являются случайными подстановками. Теперь сравниваются между собой статистические свойства ряда современных шифров и их уменьшенных моделей с помощью тестов NIST STS. В их числе рассмотрены шифры, представленные на украинский конкурс, а также финалист конкурса AES шифр Rijndael. Установлено, что по рассмотренным показателям украинские шифры Калина, Мухомор и Лабиринт превосходят признанного мирового лидера блочного симметричного шифрования – шифр AES.

Ключевые слова: *доказуемая стойкость, тесты NIST STS, показатели случайности модели и прототипа, случайная подстановка, уменьшенная модель шифра.*

Введение

Одним из важных вопросов, решаемых в процессе разработки ускоренной методики криптоанализа современных блочных шифров, предложенной в работах [1, 2], остается адекватность использования уменьшенных моделей вместо их больших прототипов. Привести строгое обоснование соответствия малых моделей большим все еще представляет известные трудности в части определения и оценки степени ″эквивалентности″ замены операций над ″большими″ блоками соответствующими операциями над ″малыми″ блоками. Естественным в таких условиях представляется стремление получить необходимые аргументы в пользу развиваемого подхода хотя бы на уровне сопоставительного анализа свойств и показателей малых моделей и больших шифров. Уже выполненные исследования ряда таких уменьшенных моделей для шифров Rijndael, а также шифров, представленных на украинский конкурс по выбору претендента на национальный стандарт блочного симметричного шифрования (Лабиринт, ADE, Калина, Мухомор), показали, что эти шифры допускают масштабирование, при котором свойства больших шифров переносятся на их малые версии. В частности изучены дифференциальные и линейные свойства уменьшенных моделей и их прототипов [3, 4 и др.], выполнен анализ их показателей статистической безопасности (лавинных и корреляционных) [5], подтвердившие повторение в малых моделях свойств больших прототипов.

В этой работе ставится задача выполнить сравнение показателей случайности больших шифров и их уменьшенных моделей с помощью тестирования с помощью набора тестов NIST STS. Будут представлены результаты их применения для анализа статистических свойств шифров, представленных на украинский конкурс. Для сравнения будут также представлены результаты тестирования с помощью набора тестов NIST STS и шифра Rijndael (AES), считающегося лидером в технологиях блочного симметричного шифрования.

1. Методика выполнения исследований

Одной из популярных методик статистических исследований шифрующих преобразований является тестирование выходного потока битов, полученных после зашифрования с помощью тестов NIST STS, используемых для выяснения наличия признаков псевдослучайности [6, 7].

Набор тестов NIST STS был предложен в ходе проведения конкурса на новый национальный стандарт блокового шифрования США [7]. Этот набор тестов использовался и для исследования статистических свойств кандидатов на новый блоковый шифр в ходе конкурса, проводимого и в Украине. На сегодня методика тестирования, предложенная NIST, содержащая 189 тестов, является наиболее распространенной у разработчиков криптографических средств защиты информации.

Для проверки шифров на прохождение тестов NIST STS используется такой алгоритм:

1) подготавливается реализацию алгоритма для шифрования в режиме CBC (режим сцепления блоков);

2) подаётся на вход для зашифрования произвольный файл размером более 10 Мб;

3) результат шифрования сохраняется в произвольном файле для последующего его анализа;

4) используя тесты NIST STS, тестируется полученный файл на прохождение всех 189 тестов;

5) осуществляется анализ полученных результатов и делается вывод относительно причин не прохождения тестов (если такие случаи есть).

Напомним, как работает режим сцепления блоков.

Режим сцепления блоков шифра включает использование n-разрядного двоичного вектора инициализации (для n битного входа в шифр), который обозначен IV. В схему добавляется регистр или буфер обратной связи, в который сначала записывается значение IV, а затем последующие значения блоков зашифрованного текста. На рис. 1 показана схема CBC.

На вход алгоритма поступает k-битный ключ K, n-битный вектор инициализации IV и последовательность n-битных блоков открытого текста $P = p_1, p_2, \ldots, p_{t-1}, p_t$.

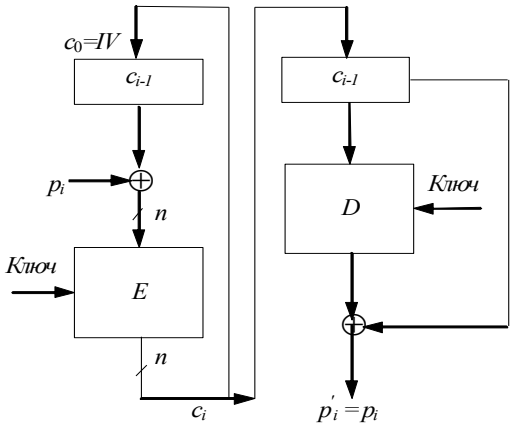

Рис. 1. Режим сцепления блоков шифра

Последовательность блоков шифртекста $C = c_1, c_2, \ldots, c_t$ вычисляется по правилу:

$$c_i = E_k(p_i \oplus c_{i-1}); \quad i = 1,\ldots,t; \quad c_0 = IV.$$

Дешифрование осуществляется соответственно так:

$$p_i = c_{i-1} \oplus D_k(c_i); \quad i = 1,\ldots,t; \quad c_0 = IV.$$

Порядок тестирования отдельной двоичной последовательности S включает в себя следующие этапы [7]:

1. Выдвигается нулевая гипотеза H_0 – предположение о том, что данная двоичная последовательность S случайная.

2. По последовательности S рассчитывается статистика теста $c(S)$.

3. С использованием специальной функции и статистики теста рассчитывается значение вероятности $P = f(c(S)), \ P \in [0,1]$.

4. Значение вероятности P сравнивается с уровнем значимости α, $\alpha \in$ [0,001, 0,01], Если $P \geq \alpha$, то гипотеза H_0 принимается. В противоположном случае принимается альтернативная гипотеза.

Пакет включает в себя 16 статистических тестов. Фактически, в зависимости от входных параметров вычисляется 189 значений вероятностей P, которые можно рассматривать как результаты работы отдельных тестов. В табл. 1, заимствованной из [7], приводятся собранные данные по всем тестам с определением сущности каждого из них, физического содержания статистики теста и дефекта, на выявление которого направлен тест.

Таким образом, в результате тестирования двоичной последовательности формируется вектор значений вероятностей $P = \{P_1, P_2, \ldots, P_{189}\}$. Анализ составляющих P_1 данного вектора позволяет указать на конкретные дефекты случайной последовательности, которая тестируется.

Методика тестирования реализуется в таком порядке [6]:

1. Для каждого ГВС необходимо оценить его статистические показатели и принять решение о том, что он формирует случайную двоичную последовательность. Генератор должен формировать двоичные последовательности $S = \{s_1, s_2, ..., s_n\}$, $s_i \in \{0,1\}$ произвольной длины n (здесь уже n используется для обозначения общей длины последовательности, формируемой генератором).

2. Для фиксированного значения n формируют множество из m двоичных последовательностей:

$$S_1 = s_1, s_2, .., s_n$$
$$S_2 = s_1, s_2, .., s_n$$
$$\ldots\ldots\ldots\ldots$$
$$S_m = s_1, s_2, .., s_n.$$

Таким образом, для тестирования необходимо сформировать выборку объемом $N = m \times n$.

3. Каждую последовательность проверяют с использованием пакета NIST STS. В результате формируется статистический портрет генератора (табл. 2)

Таблица 2

Статистический портрет генератора

№ теста j / № посл-ти i	1	2	…	q
S_1	$P_{1,1}$	$P_{1,2}$		$P_{1,q}$
S_2	$P_{2,1}$	$P_{2,2}$		$P_{2,q}$
:	:			
S_m	$P_{m,1}$	$P_{m,2}$		$P_{m,q}$

или в матричном виде $\begin{pmatrix} P_{11} & P_{12} & \cdots & P_{1q} \\ P_{21} & P_{22} & \cdots & P_{1q} \\ \vdots & \vdots & \ddots & \vdots \\ P_{m1} & P_{m2} & \cdots & P_{mq} \end{pmatrix}$.

Статистический портрет генератора является матрицей размерностью $m \times q$, где m – количество двоичных проверяемых последовательностей, а q – количество статистических тестов, используемых для тестирования каждой последовательности. Элементы матрицы $P_{ij} \in [0,1]$, ãäå $i = \overline{1,m}$, $j = \overline{1,q}$ представляют

Таблица 1

Характеристики тестов

Номер	Статистический тест	Статистика теста c(S)	Дефект, который выявляется
1	Частотный (монобитный) тест	Нормализованная абсолютная сумма значений элементов последовательности	Дисбаланс единичных и нулевых битов
2	Частотный тест (в середине блока)	Мера согласованности количества единиц, которые наблюдаются с тем, что ожидается теоретически.	Локализованные отклонения частоты появления единиц в блоке от идеального значения 1/2
3	Проверка накопленных сумм	Максимальное отклонение значений накопленной суммы элементов последовательности от начальной точки отсчета (точка 0)	Большое количество единиц или нулей в начале или конце двоичной последовательности
4	Проверка серий	Общее количество серий на всей длине последовательности	Слишком быстрая или слишком медленное изменение знака в ходе генерации последовательности
5	Проверка максимальной длины серии в блоке.	Мера согласованности значений максимальной длины, которые наблюдаются, со значением, которое можно ожидать теоретически	Отклонение от теоретического закона распределения максимальных длин серий
6	Проверка ранга двоичной матрицы	Мера согласованности значений рангов разного порядка, которые наблюдаются, со значением, которое можно ожидать теоретически	Отклонение эмпирического закона распределения значений рангов матриц от теоретического, что указывает на зависимость символов в последовательности
7	Спектральный анализ на основе дискретного преобразования Фурье	Нормализованная разность количества частотных компонент, которые наблюдаются, от той, которую можно ожидать, превышающие 95% уровень порога	Выявление периодических составляющих (трендов) в двоичной последовательности
8	Проверка шаблонов, которые перекрываются	Мера согласованности количества наблюдаемых шаблонов, которые перекрываются, в последовательности с теоретическим значением	Большое количество m-битных серий из единиц в последовательности
9	Универсальный тест Маурера	Сума логарифмов расстояний между битовыми шаблонами.	Возможность сжатия последовательности.
10	Энтропийный тест	Мера согласованности наблюдаемого значения энтропии источника с тем, что теоретически можно ожидать для случайного источника.	Неравномерность распределения *m*-битных слов в последовательности (регулярность свойств источника)
11	Проверка случайных отклонений	Мера согласованности наблюдаемого количества попаданий при случайном блуждании в заданное состояние в середине цикла с тем, что можно ожидать теоретически	Отклонение от теоретического закона распределения попаданий в конкретное состояние при случайном блуждании
12	Проверка случайных отклонений	Общее количество попаданий при случайном блуждании	Отклонения от теоретически ожидаемого общего количества визитов при случайном блуждании в заданное состояние
13	Последовательный тест	Мера согласованности количества всех вариантов m-битных шаблонов, которое наблюдается, с тем, что можно ожидать теоретически	Неравномерность распределения m - битовых слов в последовательности
14	Проверка сжатия согласно алгоритма Лемпела-Зива	Количество в последовательности разных слов	Большая степень сжатия и соответственно, избыточность тестируемой последовательности
15	Проверка шаблонов, которые не перекрываются	Мера согласованности ожидаемого количества непериодических шаблонов в последовательности с теоретическим значением.	Большое число заданных непериодических шаблонов в последовательности
16	Проверка линейной сложности	Мера согласованности наблюдаемого количества событий, которые заключаются в появлении фиксированной длины эквивалентного ЛРР для заданного блока с теоретическим.	Отклонение эмпирического распределения длин эквивалентных ЛРР для последовательностей фиксированной длины от теоретического закона распределения для случайной последовательности, что указывает на недостаточную сложность последовательности, которая тестируется.

собой значения вероятностей, полученных в результате тестирования i-й последовательности j-м тестом.

4. По полученным статистическим портретам определяют судьбу последовательностей, прошедших каждый статистически тест. Для этого задают уровень значимости $\alpha \in [0{,}001,\ 0{,}01]$ и осуществляют подсчет значений вероятностей, превышающих установленный уровень α для каждого из q тестов, т.е. определяют коэффициент

$$r_j = \frac{\#\left\{P_{ij} \ge \alpha \middle| i = 1, 2, \ldots, m\right\}}{m}.$$

В результате формируется вектор коэффициентов $R = \{r_1, r_2, \ldots, r_q\}$, элементы которого характеризуют, в процентах, прохождение последовательности S_i всех статистических тестов. При этом решение принимается в соответствии с правилами:

Правило 1. Считается, что генератор G прошел тестирование по j-му тесту, если значение коэффициента r_j находится в пределах доверительного интервала $[r_{max}, r_{min}]$. Границы доверительного интервала определяются соответственно выражению

$$r_{max(min)} = \hat{p} \pm 3\sqrt{\frac{\hat{p}(1-\hat{p})}{m}},$$

где $\hat{p} = 1 - \alpha$.

5. Осуществляется статистический анализ статистического портрета. Полученные значения вероятностей P_{ij} должны подчиняться равномерному закону распределения на интервале $[0,1]$. Для каждого вектора-столбца статистического портрета строится гистограмма частостей F_k попадания значений P_{ij} в каждый из k = 1, 2, …, 10 подинтервалов, на которые разбит интервал [0,1]. Равновероятность распределения значений вероятностей P_{ij} проверяется с использованием критерия χ^2. Для этого рассчитывается статистика вида

$$\chi_j^2 = \sum_{k=1}^{10} \frac{\left(F_k - m/10\right)^2}{m/10},$$

которая подчиняется χ^2 распределению с девятью степенями свободы.

Правило 2. Считается, что генератор G прошел тестирование по j-му тесту, если выполняется условие $P(\chi_j^2) > 0{,}0001$.

6. Окончательное решение принимается в соответствии с правилом: считается, что генератор G прошел статистическое тестирование пакетом NIST STS, если значения коэффициентов r_j для всех $j = \overline{1,q}$ находятся в границах доверительного интервала $[r_{max}, r_{min}]$ и для всех $j = \overline{1,q}$ выполняется условие $P(\chi_j^2) > 0{,}0001$.

2. Результаты выполнения статистических экспериментов

Далее предлагаются результаты экспериментов с большими и малыми вариантами шифров.

На рис. 2 – 9 представлены результаты тестирования шифра Лабиринт.

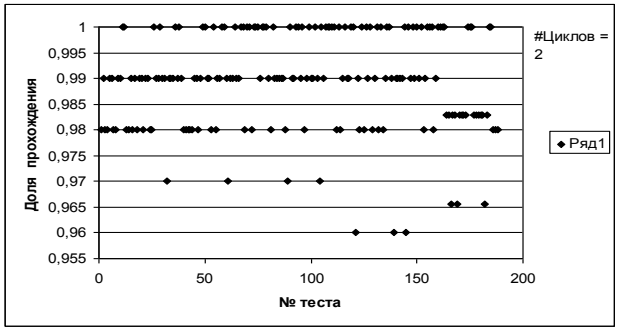

Рис. 2. Прохождение тестов 1-но цикловым шифром

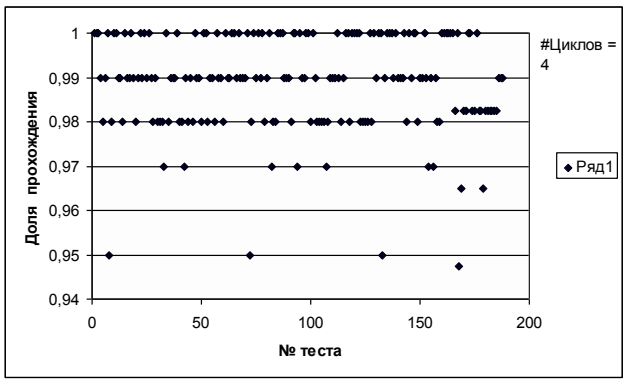

Рис. 3. Прохождение тестов 2-х цикловым шифром

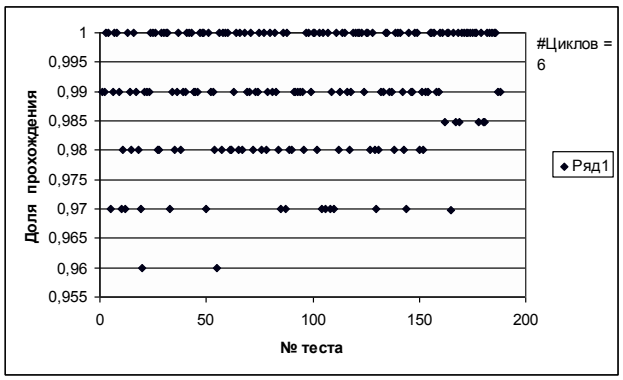

Рис. 4. Прохождение тестов 3-х цикловым шифром

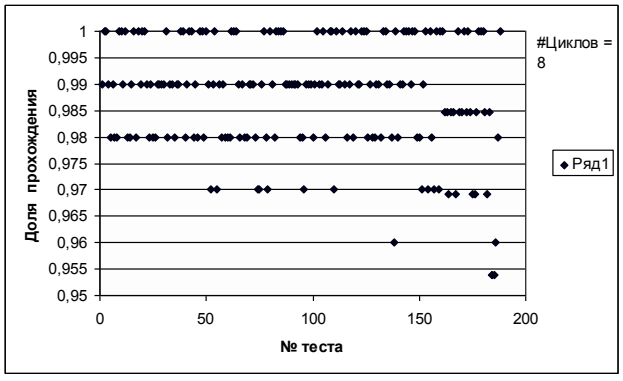

Рис. 5. Прохождение тестов 4-х цикловым шифром

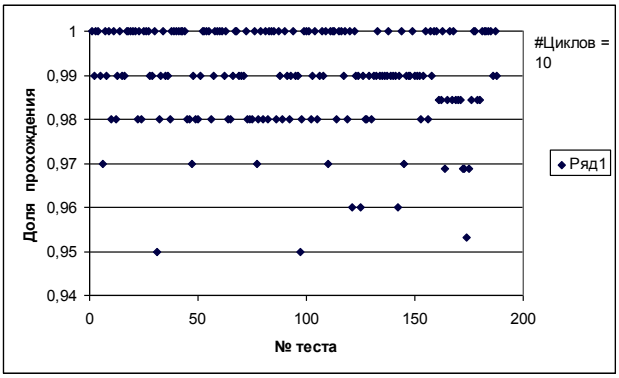

Рис. 6. Прохождение тестов 5-ти цикловым шифром

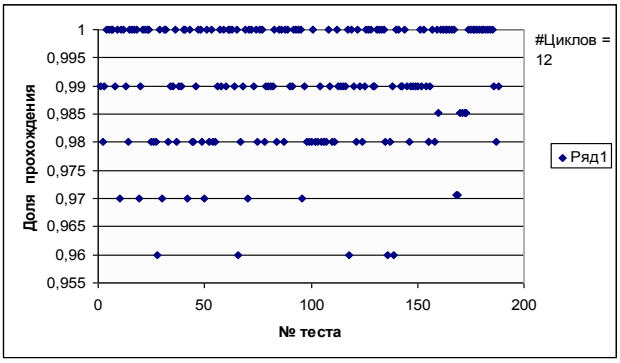

Рис. 7. Прохождение тестов 6-ти цикловым шифром

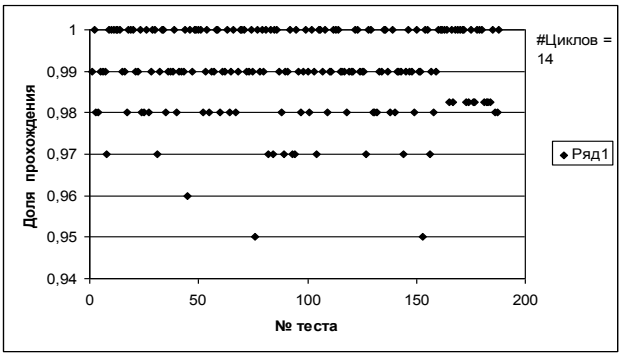

Рис. 8. Прохождение тестов 7-ти цикловым шифром

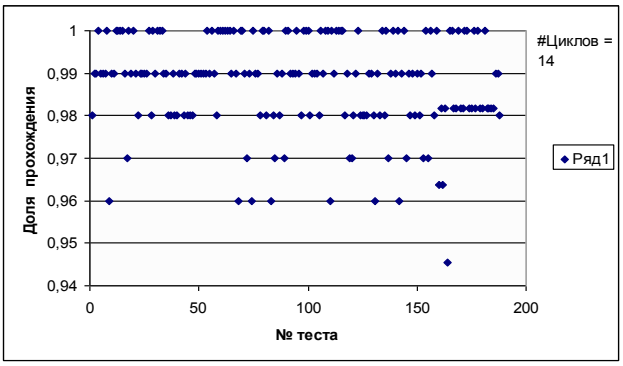

Рис. 9. Прохождение тестов 8-ти цикловым шифром

Тесты выполнены для 100 последовательностей по 1 млн. бит каждая.

Заметим, что рассмотренные шифры по спецификациям имеют Мухомор-128 – 11 циклов зашифрования, Лабиринт – 8 циклов, Калина 128/256 – 14 циклов, ADE 128/128 – 10 циклов, Rijndael – от 10-ти до 14-ти циклов в зависимости от длины блока и ключа.

Как следует из представленных результатов, для различных циклов получаются результаты прохождения и 96% и 95% и.даже 94%. Анализ показывает, что картина распределения прохождений по циклам меняется в зависимости от используемого мастер-ключа. Далее на рис. 10 – 20 представлены результаты тестирования шифра Мухомор.

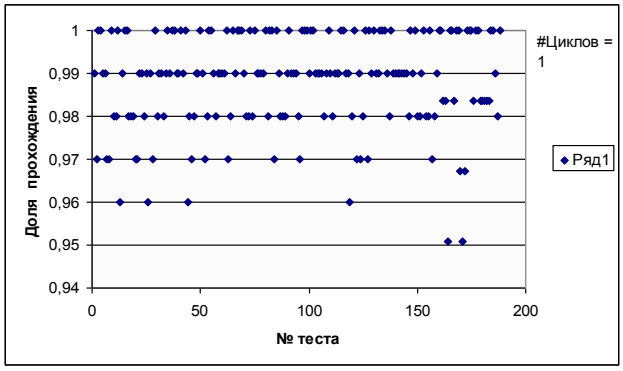

Рис. 10. Прохождение тестов 1-но цикловым шифром

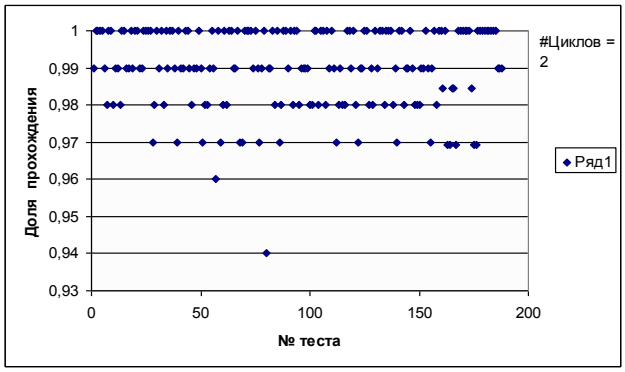

Рис. 11. Прохождение тестов 2-х цикловым шифром

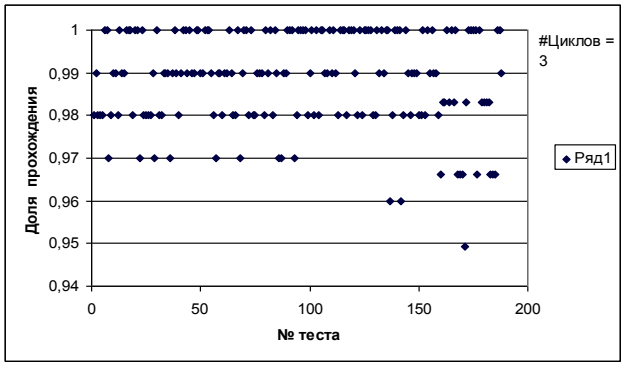

Рис. 12. Прохождение тестов 3-х цикловым шифром

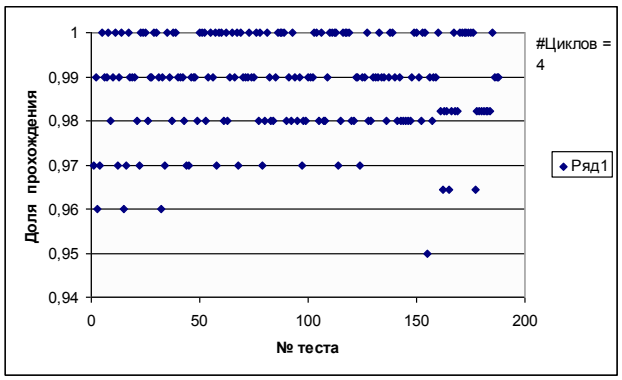

Рис. 13. Прохождение тестов 4-х цикловым шифром

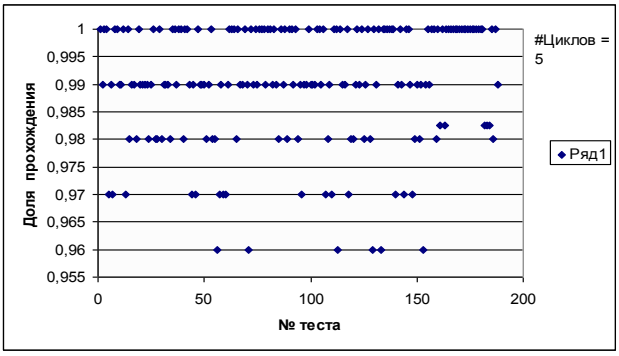

Рис. 14. Прохождение тестов 5-ти цикловым шифром

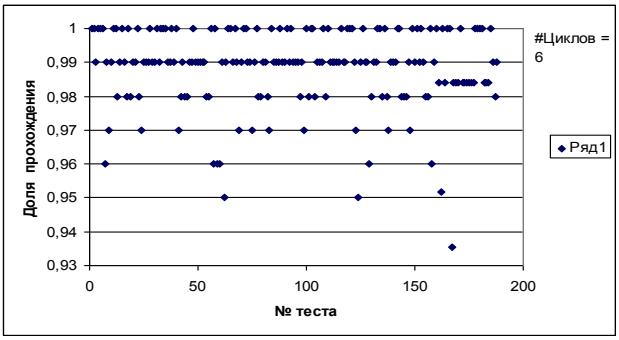

Рис. 15. Прохождение тестов 6-ти цикловым шифром

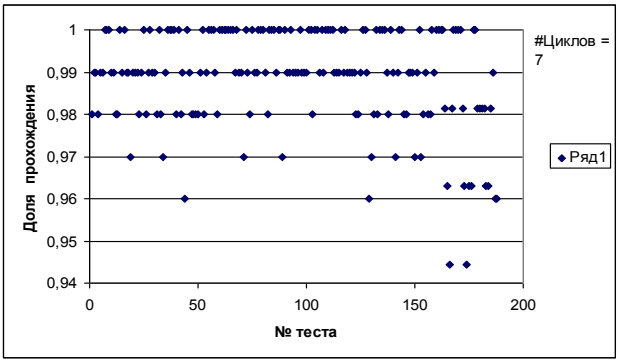

Рис. 16. Прохождение тестов 7-ми цикловым шифром

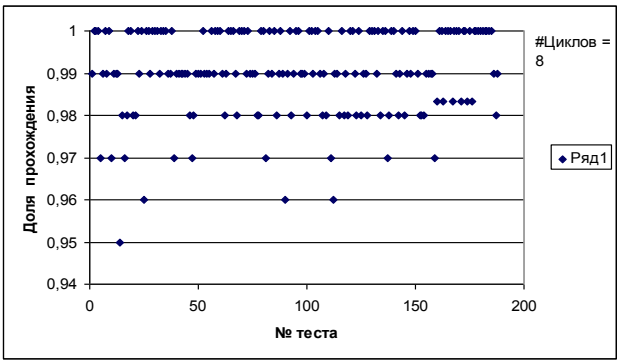

Рис. 17. Прохождение тестов 8-ми цикловым шифром

Для этого шифра также наблюдается варьирование результата в зависимости от числа циклов, причём есть цикловые длины, на которых результат прохождения тестов опускается ниже 95%-го уровня (для 2-х циклов – 94%, для 6-ти циклов – 93%).

Примечательно, что на полной цикловой длине (11-ть циклов) в нашем эксперименте и здесь не получился 96%: уровень прохождения.

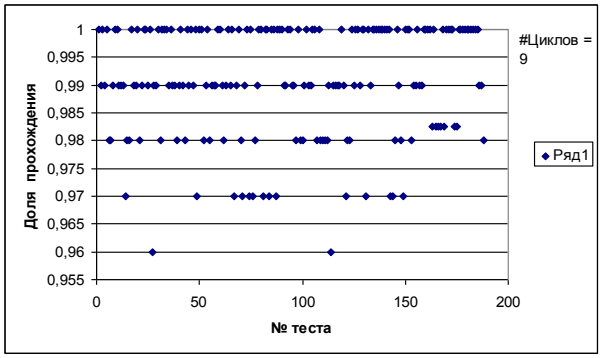

Рис. 18. Прохождение тестов 9-ти цикловым шифром

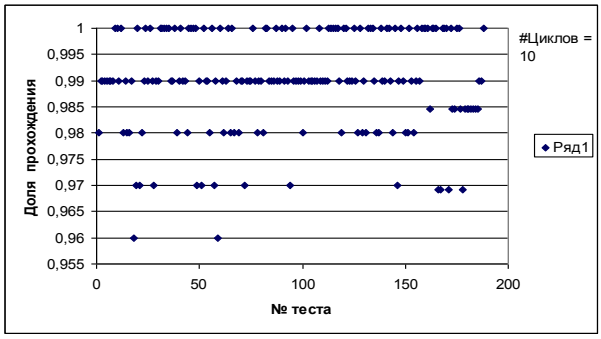

Рис. 19. Прохождение тестов 10-ти цикловым шифром

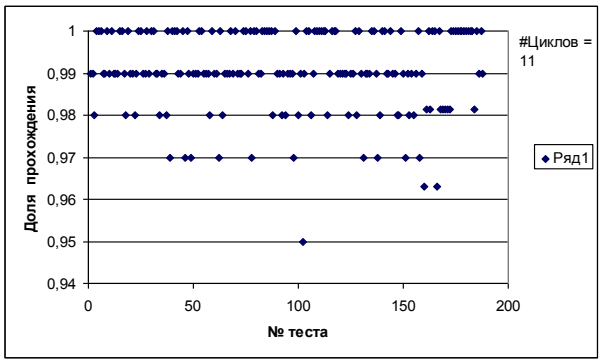

Рис. 20. Прохождение тестов 11-ти цикловым шифром

Для использованного мастер-ключа реализовался 95% уровень прохождения.

Получается, что хоть в одноцикловом варианте использования шифров Лабиринт и Мухомор, хоть в многоцикловом, они в зависимости от циклового подключа могут выступать генераторами псевдослучайных последовательностей, не уступающими по характеристикам лучшим из известных.

На рис. 21 – 34 представлены результаты тестирования шифра Калина.

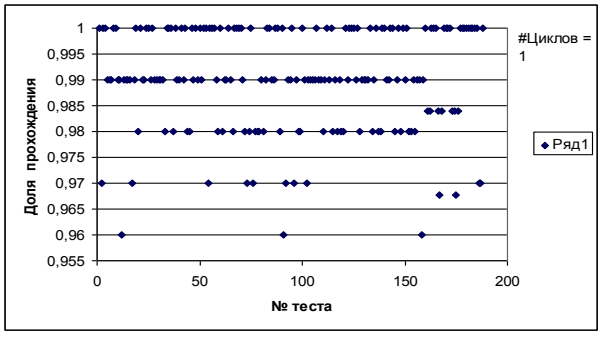

Рис. 21. Прохождение тестов 1-но цикловым шифром

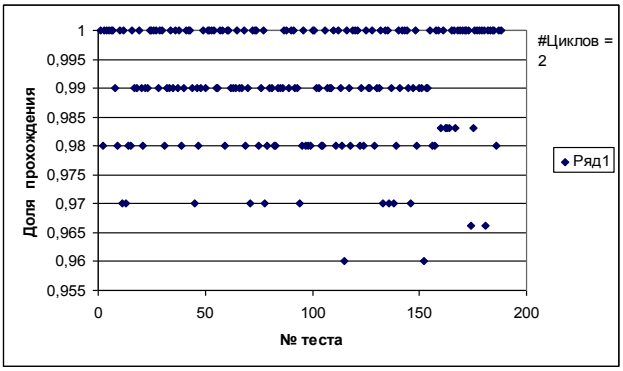

Рис. 22. Прохождение тестов 2-х цикловым шифром

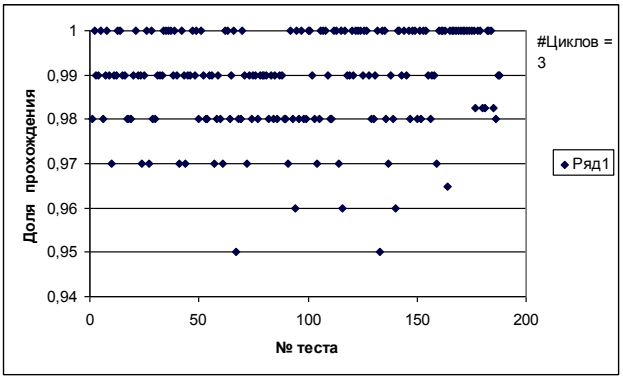

Рис. 23. Прохождение тестов 3-х цикловым шифром

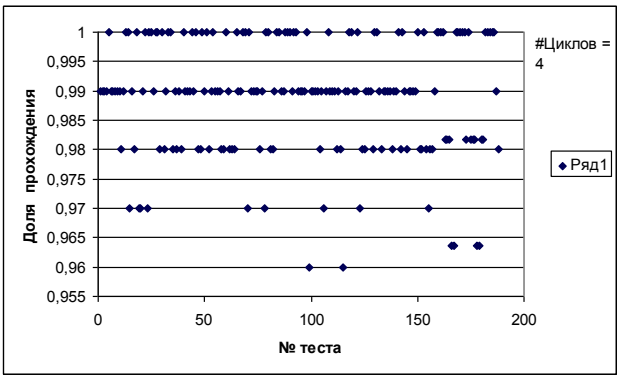

Рис. 24. Прохождение тестов 4-х цикловым шифром

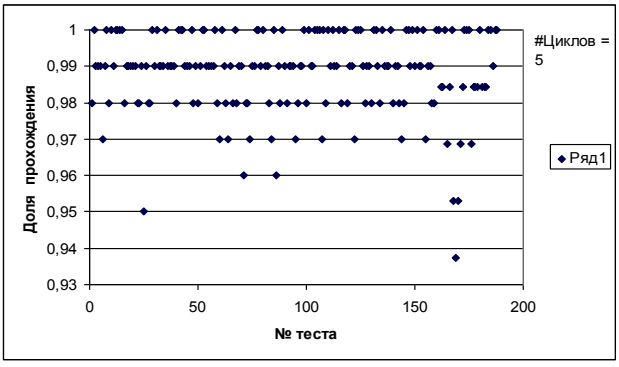

Рис. 25. Прохождение тестов 5-ти цикловым шифром

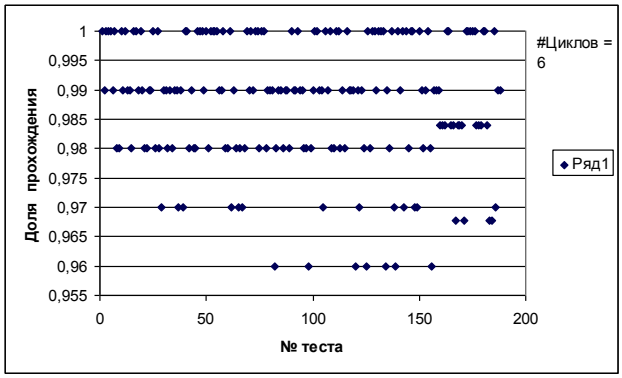

Рис. 26. Прохождение тестов 6-ти цикловым шифром

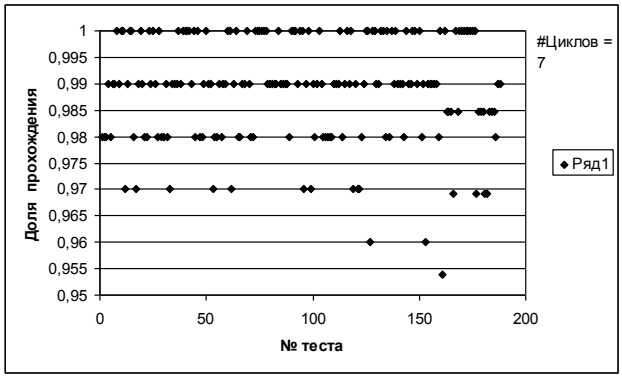

Рис. 27. Прохождение тестов 7-ми цикловым шифром

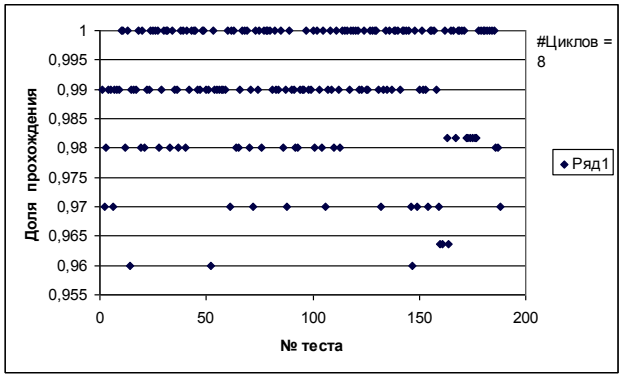

Рис. 28. Прохождение тестов 8-ми цикловым шифром

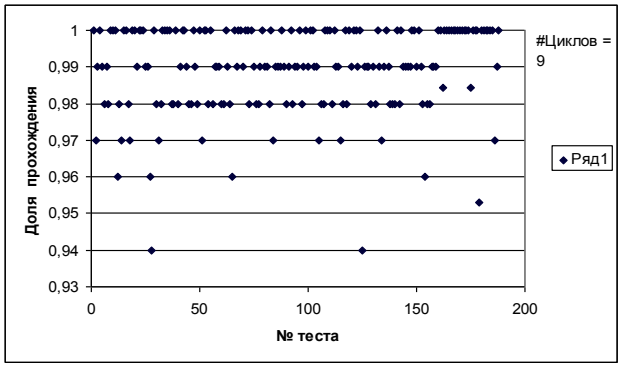

Рис. 29. Прохождение тестов 9-ти цикловым шифром

Этот шифр практически повторяет свойства рассмотренных выше шифров. Отдельные цикловые длины демонстрируют 96% уровень прохождения тестов, в то время как имеются и циклы с пониженным до 94% уровнем прохождения тестов, хотя и в рассмотренном примере он показывает 96% уровень прохождения тестов при одноцикловом зашифровании. В то же время и здесь имеются циклы, на которых шифр реализует лишь 94% уровень прохождения тестов. Из 14 циклов шифрования 6 имеют 96% уровень прохождения, 5 – 95% уровень прохождения и 3 имеют 94% уровень прохождения тестов. Напомним ещё раз,

что результаты привязаны к значению мастер-ключа. По-видимому, наличие циклов с пониженным до 94% уровнем прохождения тестов – это не слабости шифров, а проявление механизмов случайности (шифрование на каждом из мастер-ключей изменяет свойства шифрующего преобразования).

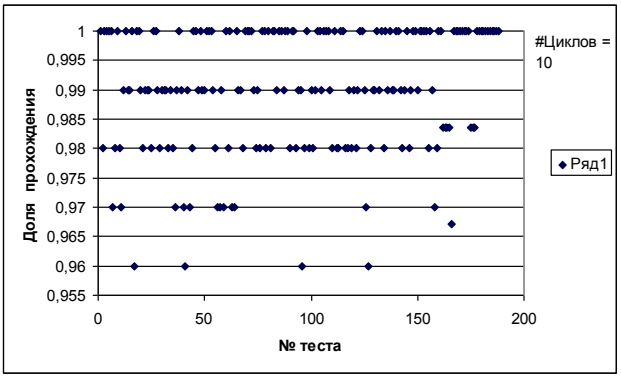

Рис. 30. Прохождение тестов 10-ти цикловым шифром

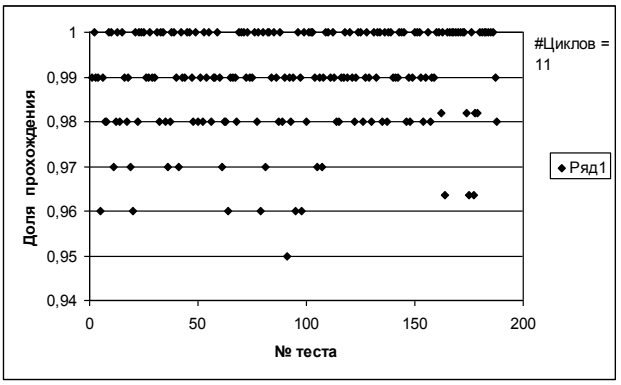

Рис. 31. Прохождение тестов 11-ти цикловым шифром

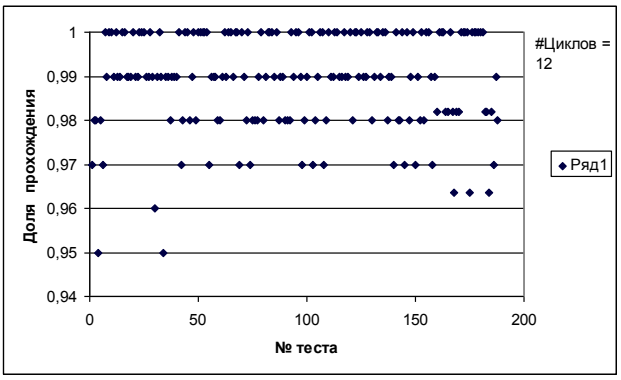

Рис. 32. Прохождение тестов 12-ти цикловым шифром

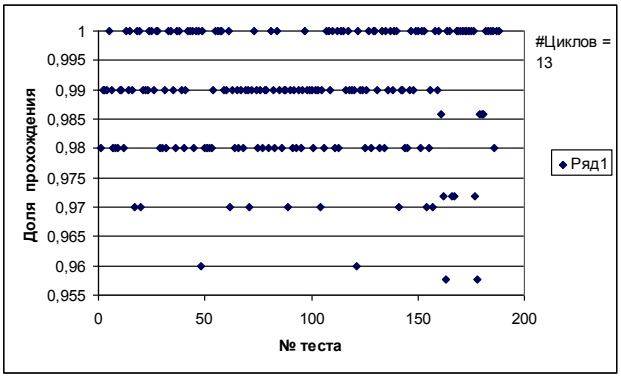

Рис. 33. Прохождение тестов 13-ти цикловым шифром

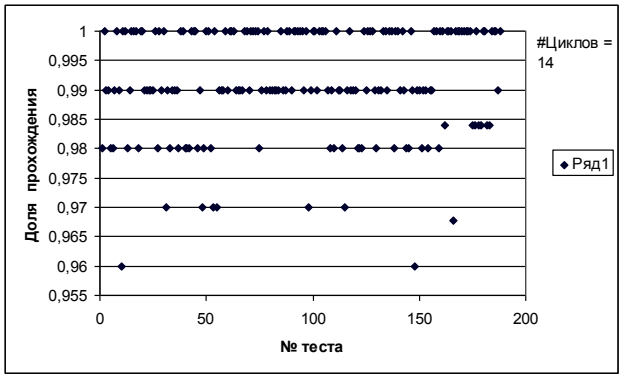

Рис. 34. Прохождение тестов 14-ти цикловым шифром

В последней серии экспериментов представляются результаты тестирования шифра ADE (рис. 35 – 44).

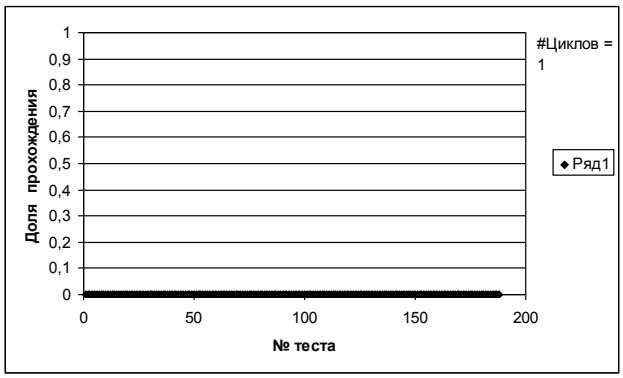

Рис. 35. Прохождение тестов 1-но цикловым шифром

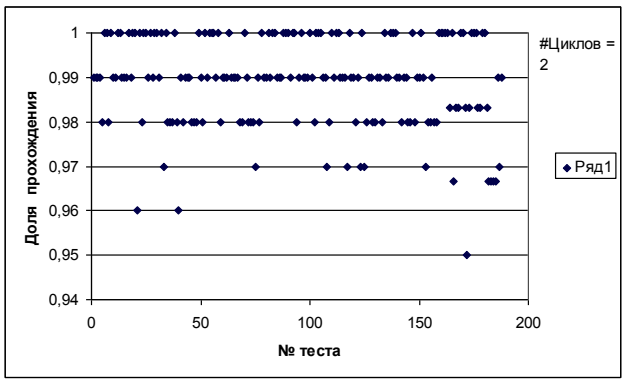

Рис. 36. Прохождение тестов 2-х цикловым шифром

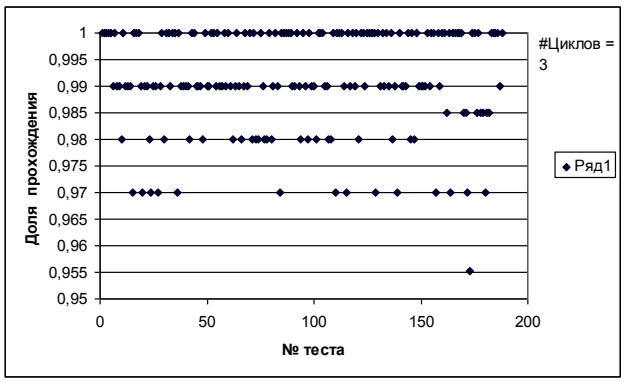

Рис. 37. Прохождение тестов 3-х цикловым шифром

Как следует из представленных результатов, в отличие от других шифров шифр ADE показал од-

ноцикловое преобразование с нулевым уровнем прохождения тестов, т.е. одноцикловое преобразование этого шифра не является шифрующим преобразованием (практически не состоялось хорошего перемешивание входного текста).

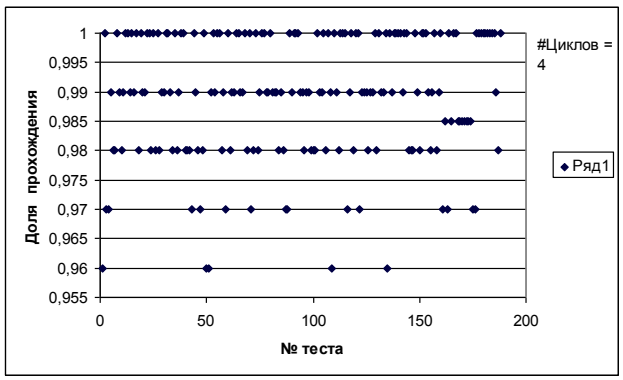

Рис. 38. Прохождение тестов 4-х цикловым шифром

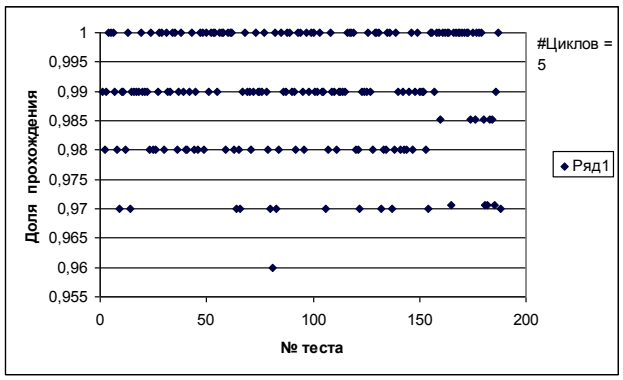

Рис. 39. Прохождение тестов 5-ти цикловым шифром

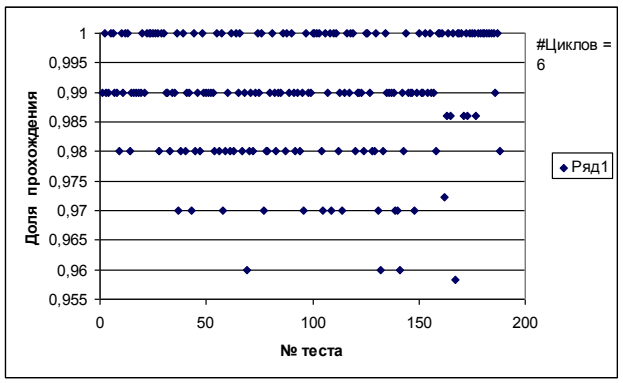

Рис. 40. Прохождение тестов 6-ти цикловым шифром

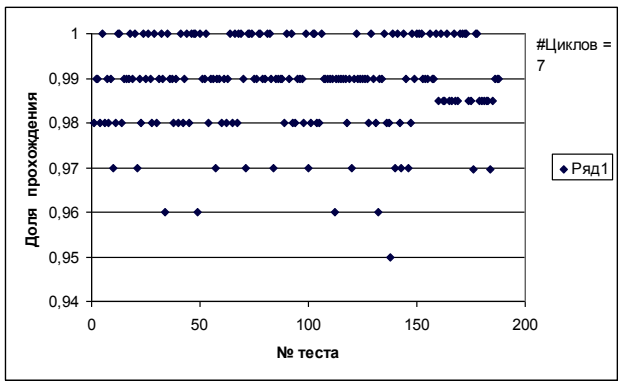

Рис. 41. Прохождение тестов 7-ми цикловым шифром

Правда на двух циклах преобразований в приведенном эксперименте шифр уже демонстрирует 96% уровень прохождения тестов. Остальные показатели повторяют общую картину: имеются циклы с 94% и 95% уровнем прохождения тестов.

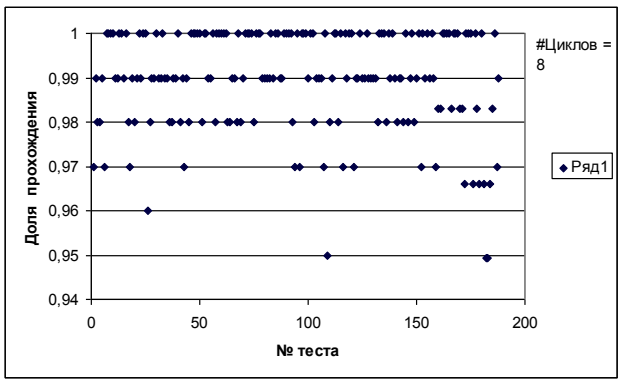

Рис. 42. Прохождение тестов 8-ми цикловым шифром

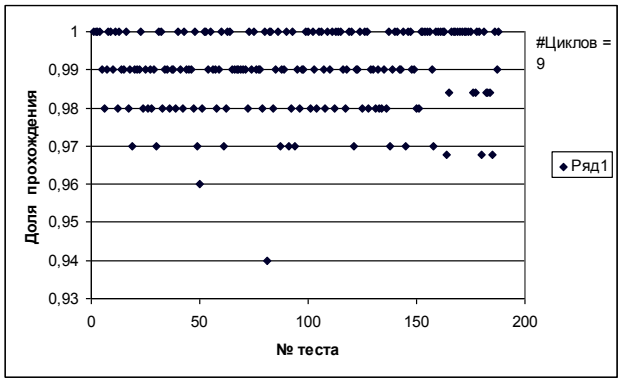

Рис. 43. Прохождение тестов 9-ти цикловым шифром

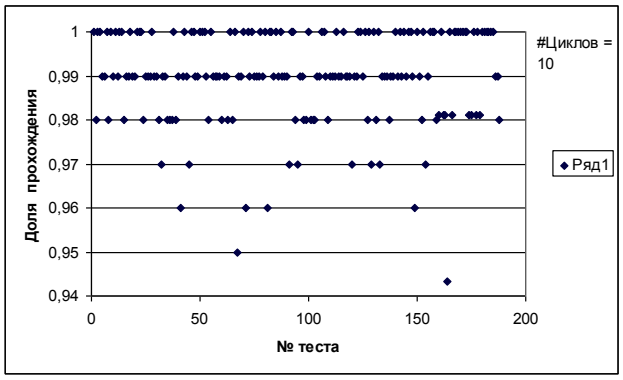

Рис. 44. Прохождение тестов 10-ти цикловым шифром

В приведенном эксперименте и на полноцикловой длине шифр демонстрирует лишь 94% уровень прохождения тестов (не повезло с мастер-ключом). В целом можно отметить, что все украинские шифры продемонтрировали практически одинаковые статистические свойства по отношению к набору тестов NIST STS.

В заключение приведём результаты тестирования большой и малой версий шифра Rijndael. Они представлены на рис. 45 – 58. На рис. 45 – 54 представлены результаты прохождения тестов 10-цикловым шифром Rijndael (128/128), а на рис. 55 – 58 – его уменьшенной версии.

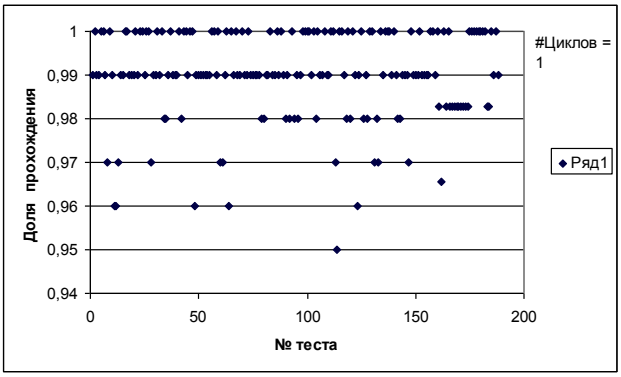

Рис. 45. Прохождение тестов 1-но цикловым шифром

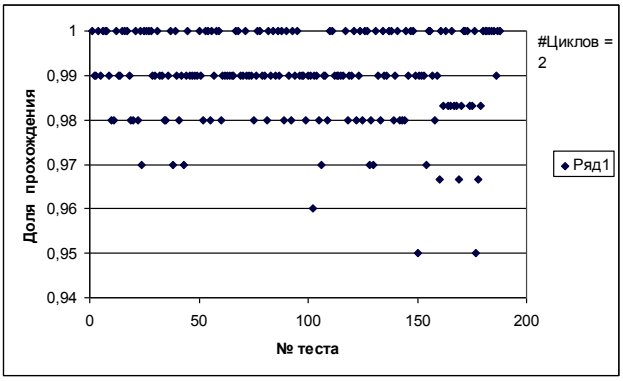

Рис. 46. Прохождение тестов 2-х цикловым шифром

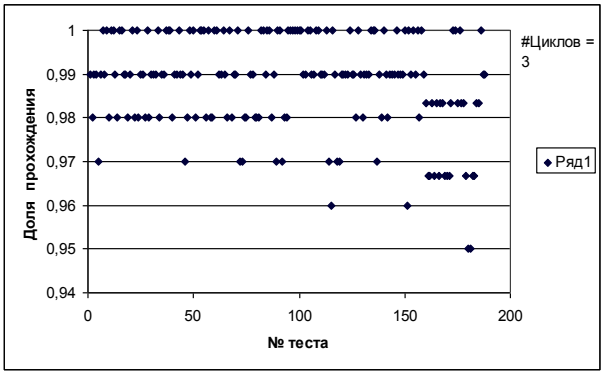

Рис. 47. Прохождение тестов 3-х цикловым шифром

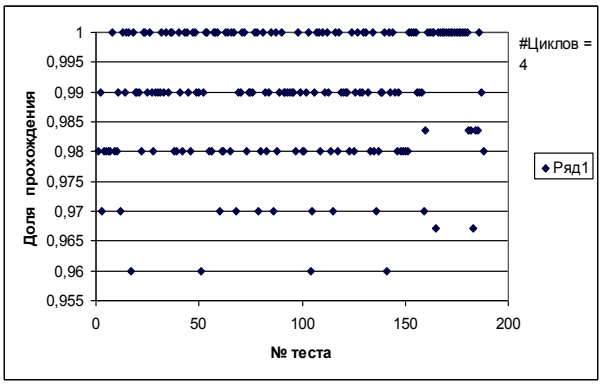

Рис. 48. Прохождение тестов 4-х цикловым шифром

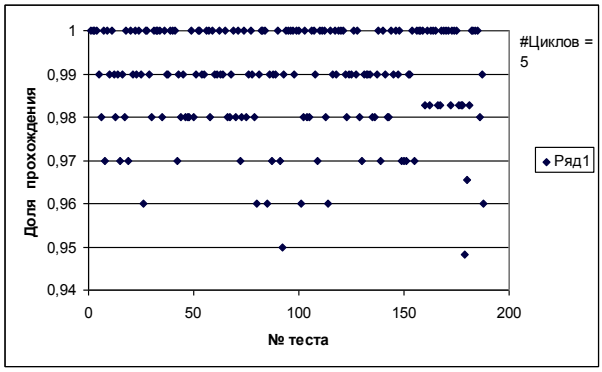

Рис. 49. Прохождение тестов 5-ти цикловым шифром

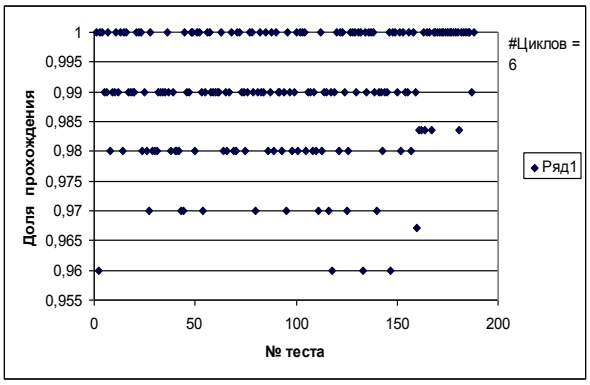

Рис. 50. Прохождение тестов 6-ти цикловым шифром

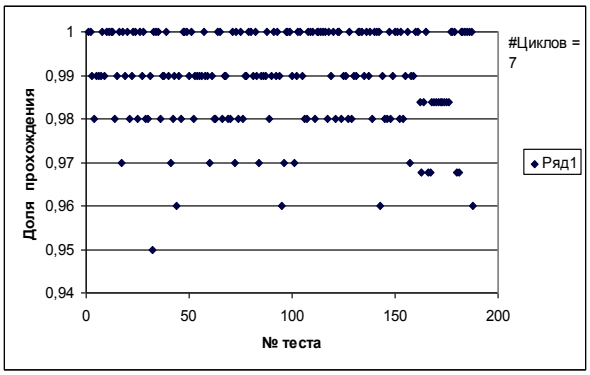

Рис. 51. Прохождение тестов 7-ми цикловым шифром

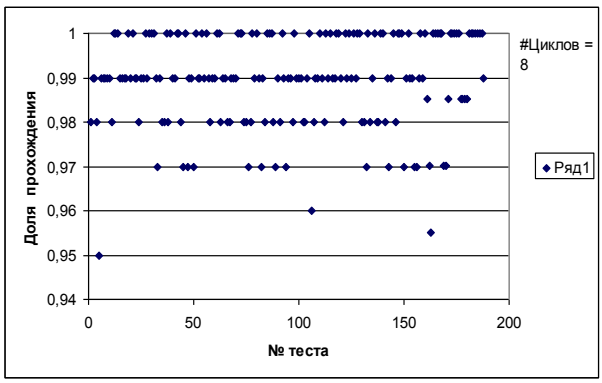

Рис. 52. Прохождение тестов 8-ми цикловым шифром

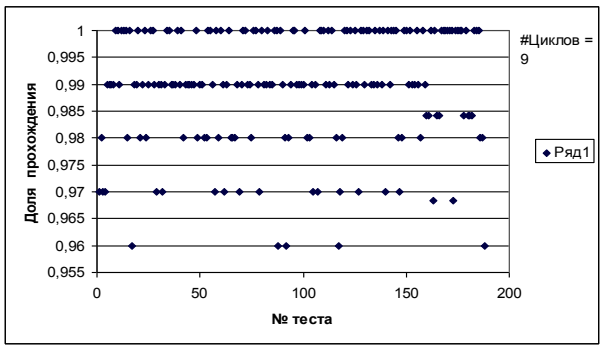

Рис. 53. Прохождение тестов 9-ти цикловым шифром

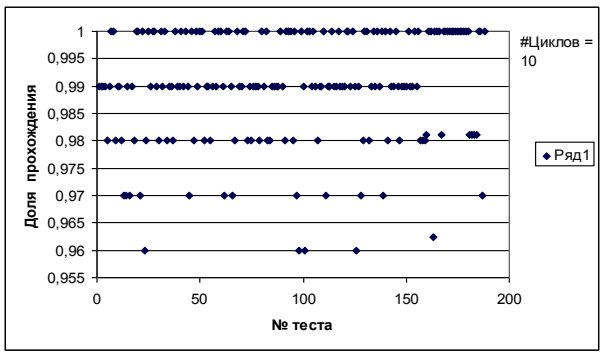

Рис. 54. Прохождение тестов 10-ти цикловым шифром

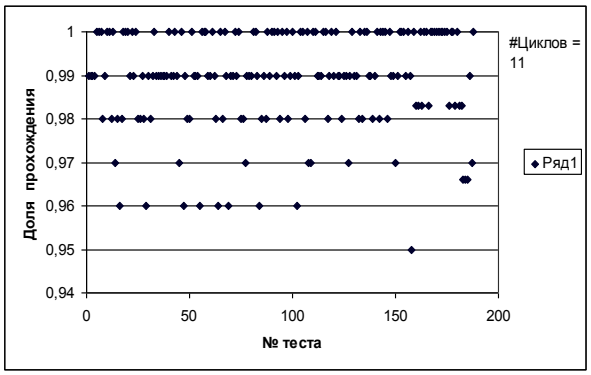

Рис. 55. Прохождение тестов 11-ти цикловым шифром

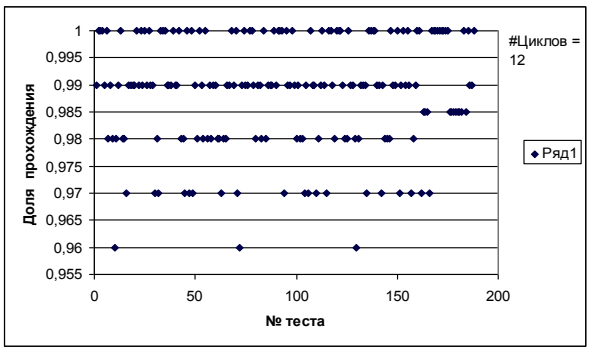

Рис. 56. Прохождение тестов 12-ти цикловым шифром

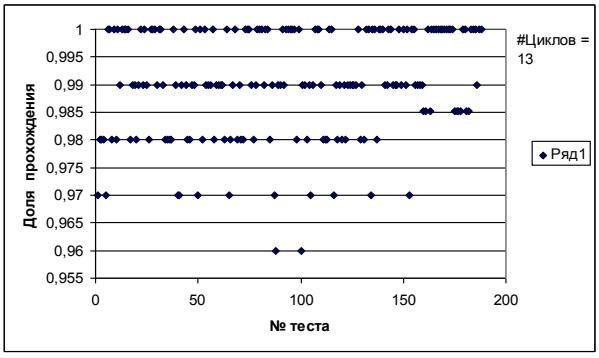

Рис. 57. Прохождение тестов 13-ти цикловым шифром

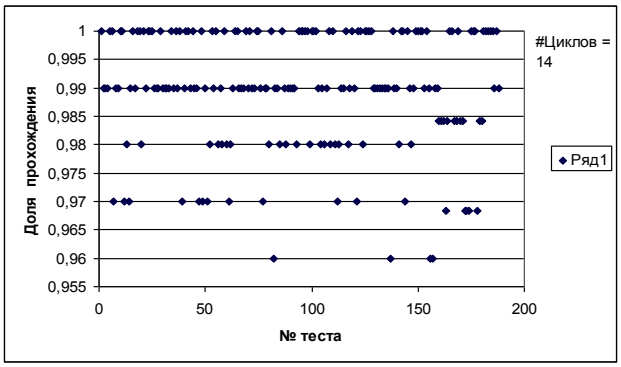

Рис. 58. Прохождение тестов 14-ти цикловым шифром

Далее (рис. 59 – 68) приводятся результаты тестирования уменьшенной версии шифра Rijndael (128/128). Видно, что и для малой модели шифра характерно наличие циклов с разными уровнями прохождения тестов, распределение которых, как показывают эксперименты, зависит от выбора мастер-ключа.

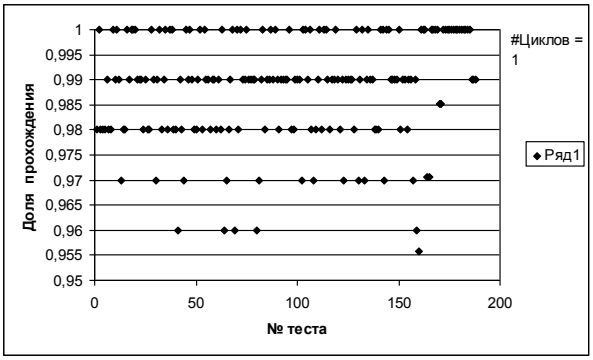

Рис. 59. Прохождение тестов 1-но цикловым шифром

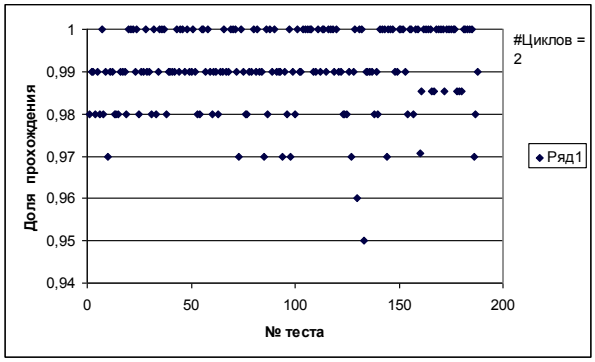

Рис. 60. Прохождение тестов 2-х цикловым шифром

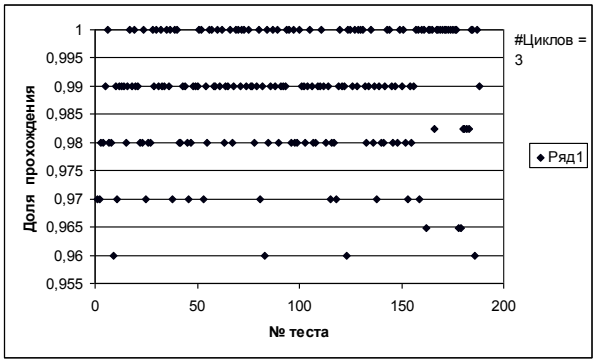

Рис. 61. Прохождение тестов 3-х цикловым шифром

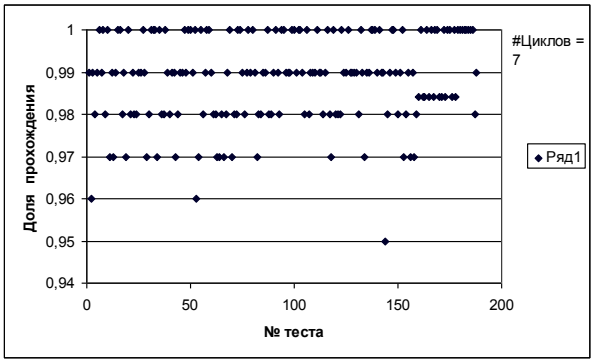

Рис. 65. Прохождение тестов 7-ми цикловым шифром

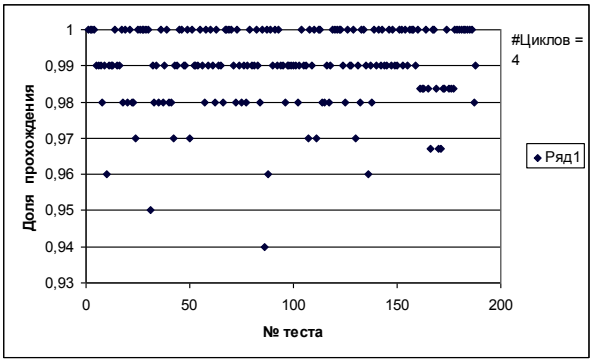

Рис. 62. Прохождение тестов 4-х цикловым шифром

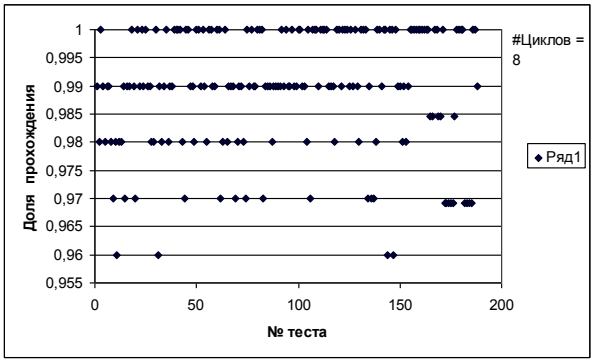

Рис. 66. Прохождение тестов 8-ми цикловым шифром

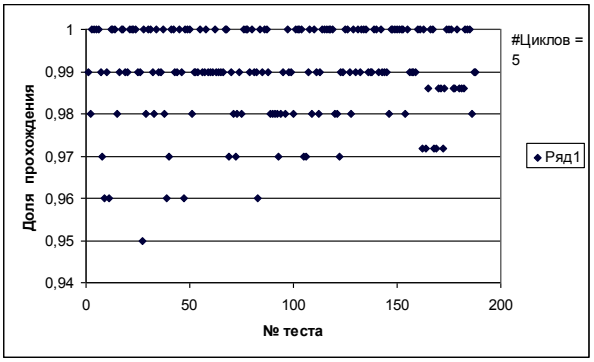

Рис. 63. Прохождение тестов 5-ти цикловым шифром

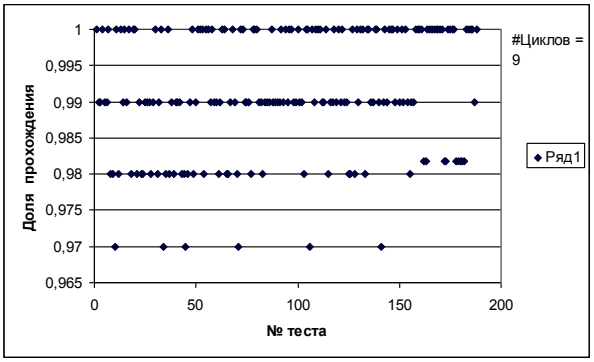

Рис. 67. Прохождение тестов 9-ти цикловым шифром

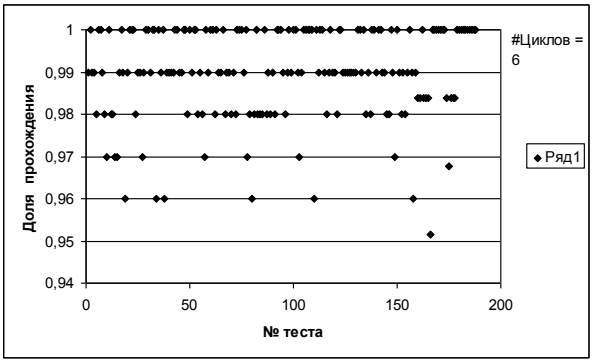

Рис. 64. Прохождение тестов 6-ти цикловым шифром

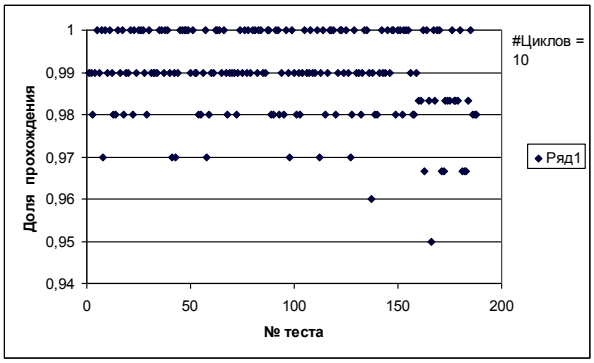

Рис. 68. Прохождение тестов 10-ти цикловым шифром

В этой уменьшенной модели рассматриваются десять циклов зашифрования.

Следует отметить, что при тестировании малых моделей пришлось искать способ их тестирования. Для малых моделей использован всё тот же самый режим OFB, но добавлено побитное сложение по модулю 2 (XOR) каждого шифртекста со счетчиком, что избавило от зацикливания программы и привело к показателям повторяющим свойства полных версий. Аналогичные измерения были выполнены и для малых моделей всех украинских шифров, представленных на конкурс. Полученные «картинки» мало

отличаются от приведенных выше. Для всех рассмотренных шифров уровень прохождения тестов не опускается ниже 92%. В то же время имеются циклы и с 96% (порой большинство) уровнем прохождения тестов. Можно сделать вывод, что результаты тестирования для уменьшенных моделей шифров и их больших их прототипов можно считать практически совпадающими, т.е. и в этом случае большие шифры повторяются своими свойствами в своих малых моделях. В целом, все украинские шифры демонстрирую свойства близкие к свойствам лидера блочного симметричного шифрования – шифра Rijndael, т.е. рассмотренные шифры можно считать эквивалентными и по этому показателю статистической безопасности.

Далее на рис. 69 – 82 представляются результаты тестирования шифра Rijndael с использованием критерия Пирсона [6].

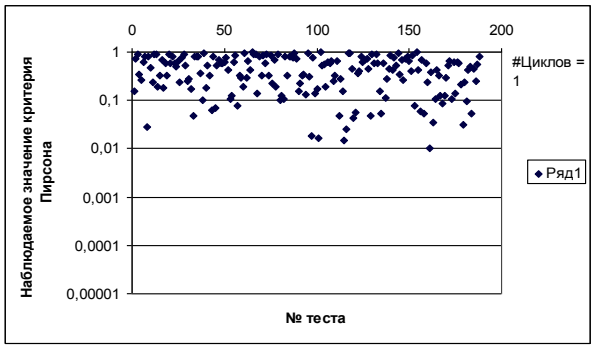

Рис. 69. Прохождение тестов 1-но цикловым шифром

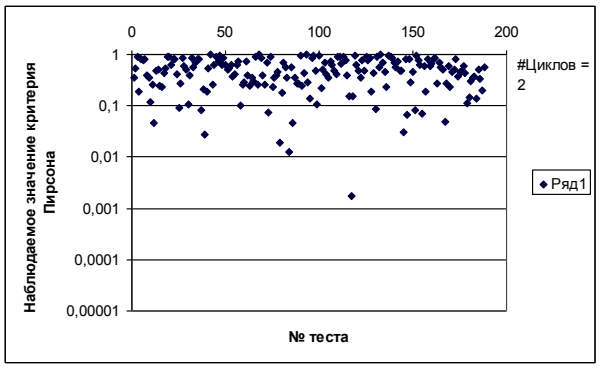

Рис. 70. Прохождение тестов 2-х цикловым шифром

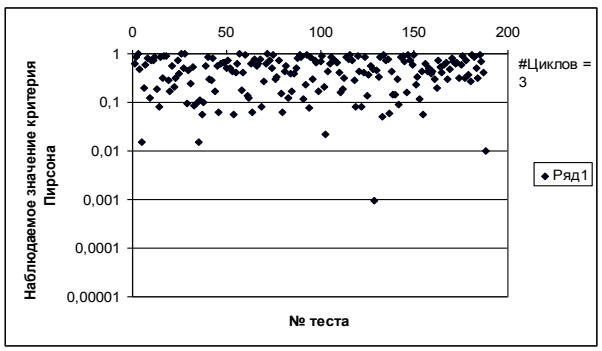

Рис. 71. Прохождение тестов 3-х цикловым шифром

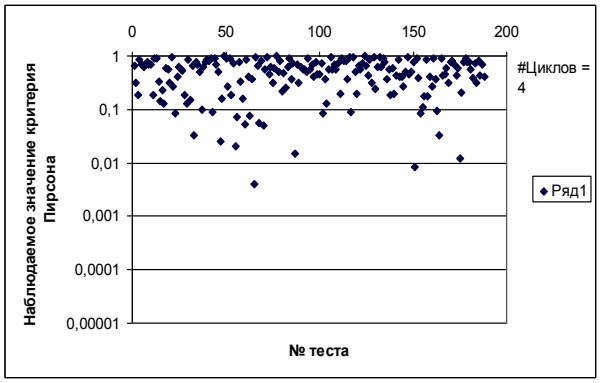

Рис. 72. Прохождение тестов для 4-х циклов

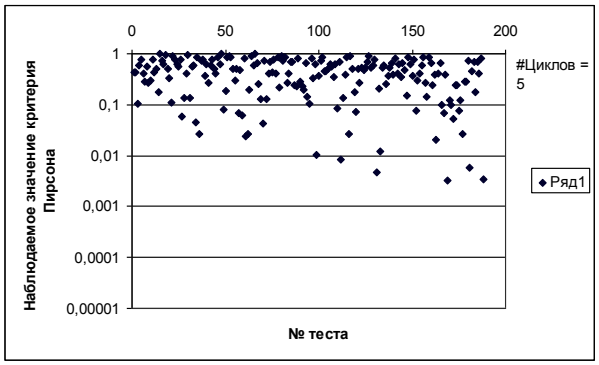

Рис. 73. Прохождение тестов для 5-ти циклов

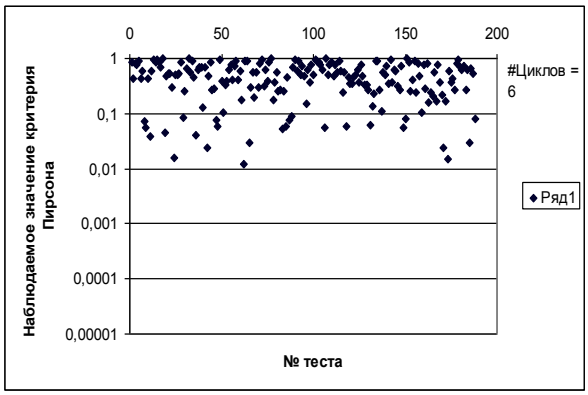

Рис. 74. Прохождение тестов для 6-ти циклов

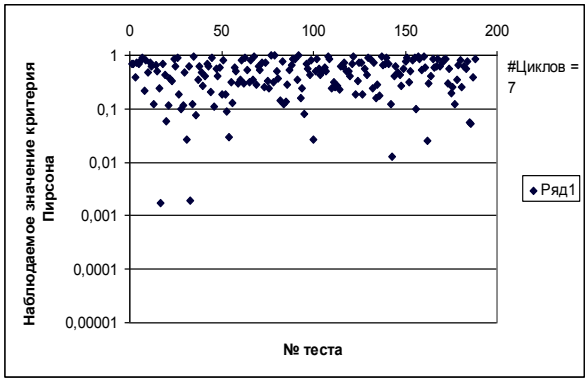

Рис. 75. Прохождение тестов для 7-ми циклов

Критический уровень прохождения для этих тестов равен 0,0001.

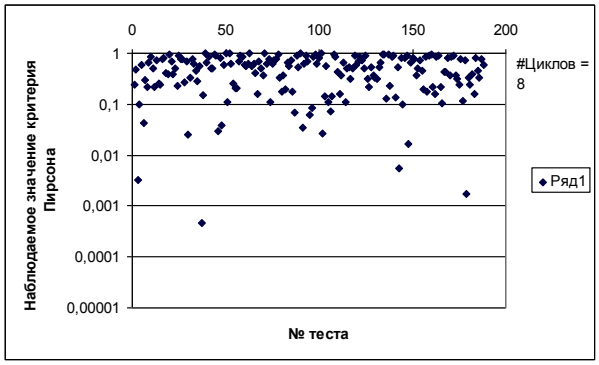

Рис. 76. Прохождение тестов для 8-ми циклов

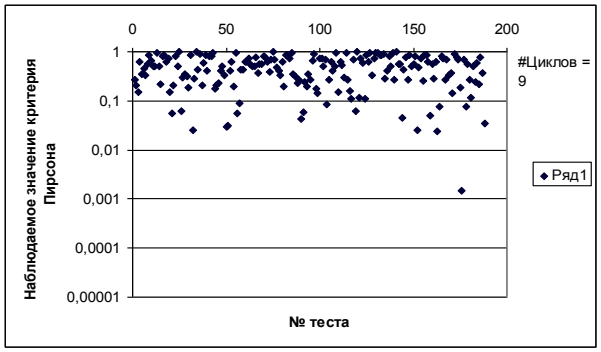

Рис. 77. Прохождение тестов для 9-ти циклов

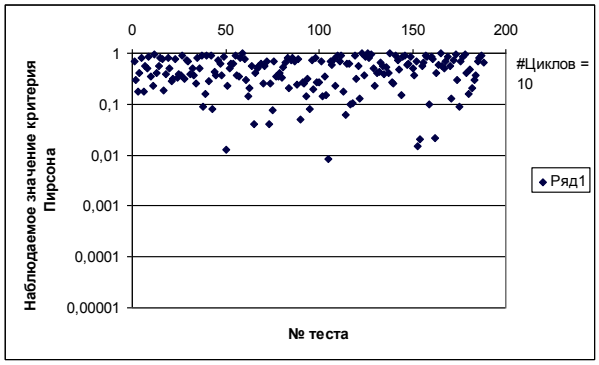

Рис. 78. Прохождение тестов для 10-ти циклов

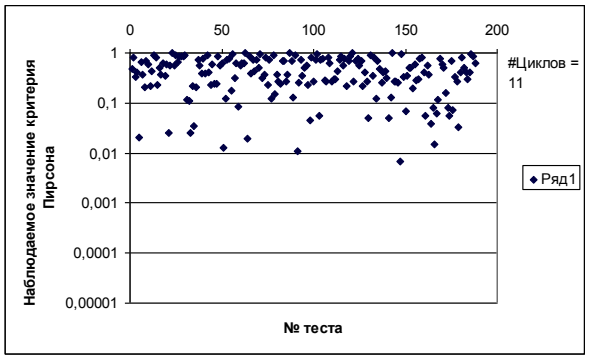

Рис. 79. Прохождение тестов для 11-ти циклов

Видно, что в данном случае для всех значений числа циклов зашифрования $P(\chi_j^2) > 0,0001$ и значит тесты успешно пройдены.

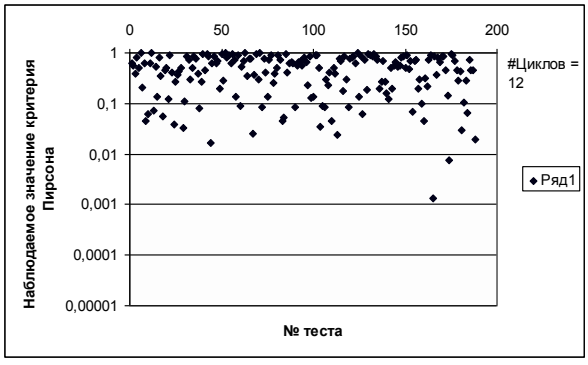

Рис. 80. Прохождение тестов для 12-ти циклов

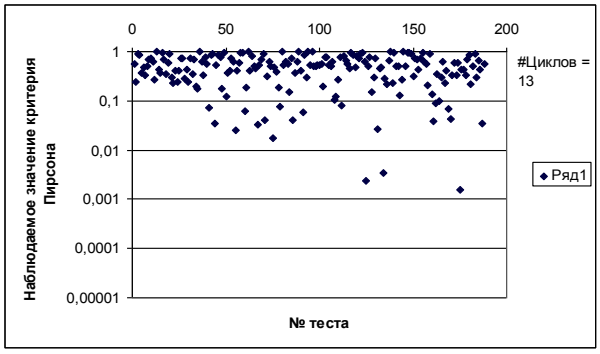

Рис. 81. Прохождение тестов для 13-ти циклов

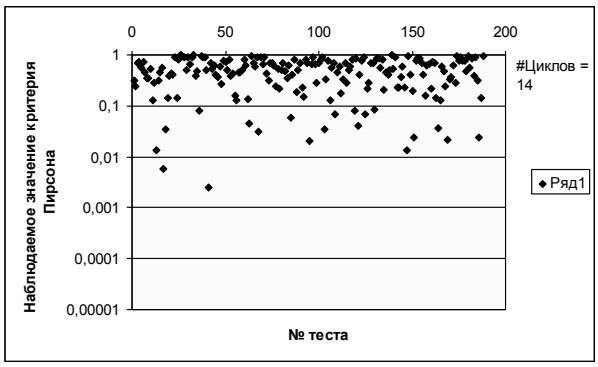

Рис. 82. Прохождение тестов: для 14-ти циклов

Видно, что в данном случае для всех значений числа циклов зашифрования $P(\chi_j^2) > 0,0001$ и значит тесты успешно пройдены.

Напомним, что в соответствии с [6] считается, что генератор G прошел статистическое тестирование пакетом NIST STS, если значения коэффициентов r_j для всех $j = \overline{1,q}$ находятся в границах доверительного интервала $[r_{max}, r_{min}]$ и выполняется условие для всех $j = \overline{1,q}$ выходит, что $P(\chi_j^2) > 0,0001$ (здесь не учитываются минимальный проходной балл для случайной экскурсии вариантного теста, где уровень прохождения может оказаться выше, чем результат, зафиксированный на соответствующем рисунке (например, для 4-х циклового результата (рис. 5) получено значение для случайной экскурсии вари-

антного теста 0,94, которое на самом деле примерно равно 57 для выборки из 60-ти двоичных последовательностей (57/60 = 0,95)), правда, здесь всё равно 96%-й уровень не пройден.

Остаётся отметить, что совершенно аналогичные результаты характерны и для всех других здесь рассмотренных шифров.

Выводы

Проверка украинских шифров на прохождение тестов NIST STS показала, что все шифры могут с успехом применяться для генерирования псевдослучайных последовательностей с высокими криптографическими показателями.

Для этого совсем не обязательно использовать шифр на полноцикловой длине. Хорошие показатели последовательности могут быть реализованы и при использовании шифров даже в одноцикловом варианте применения (кроме ADE).

Выявлена зависимость качества формируемых последовательностей от используемых мастер-ключей.

Приведенные результаты являются ещё одним свидетельством повторения в малых моделях шифров свойств прототипов. Они лишний раз подтверждают, что "большие" шифры являются случайными подстановками.

Список литературы

1. Долгов В.И. Подход к криптоанализу современных шифров / В.И. Долгов, И.В. Лисицкая, Р.В. Олейников // Материалы второй международной конференции "Современные информационные системы. Проблемы и тенденции развития", Харьков-Туапсе, Украина, 2-5 октября. – 2007. – С. 435-436.

2. Лисицкая И.В. Методология оценки стойкости блочных симметричных шифров / И.В. Лисицкая // Автоматизированные системы управления и приборы автоматики. – 2011. – № 163. – С. 123-133.

3. Долгов В.И. Дифференциальные свойства блочных симметричных шифров, представленных на украинский конкурс / В.И. Долгов, А.А. Кузнецов, С.А. Исаев // Электронное моделирование. – 2011. – Т 33, № 6. – С. 81-99.

4. Кузнецов А.А. Линейные свойства блочных симметричных шифров, представленных на украинский конкурс. / А.А. Кузнецов, И.В. Лисицкая, С.А. Исаев // Прикладная радиоэлектроника. – 2011. – Т.10, № 2. – С. 135-140.

5. Лисицкая И.В. Большие шифры – случайные подстановки. Сравнение показателей статистической безопасности блочных симметричных шифров, представленных на украинский конкурс / И.В. Лисицкая, А.А. Настенко, К.Е. Лисицкий // Восточно-Европейский журнал передовых технологий: научный журнал. – Х.: Технологический центр, 2012.

6. Rukhin A. et al. A Statistical Test Suite for Random and Pseudorandom Number Generators for Cryptographic Applications. NIST Special Publication 800-22. Washington, 2000.

7. NIST IR 6390. A Statistical Test Suite for the Validation of Random Number Generators and Pseudo Random Number Generators for Cryptographic Applications, 2000.

8. Долгов В.И. Критерии случайности таблиц подстановок алгоритма шифрования ГОСТ 28147-89 / В.И. Долгов, Р.В. Олейников и др. // Прикладная радиоэлектроника. – 2006. – Т.6, № 1. – С. 127-133.

Поступила в редколлегию 27.08.2012

Рецензент: д-р техн. наук, проф. И.Д. Горбенко, Харьковский национальный университет радиоэлектроники, Харьков.

ВЕЛИКІ ШИФРИ – ВИПАДКОВІ ПІДСТАНОВКИ. ПЕРЕВІРКА СТАТИСТИЧНИХ ВЛАСТИВОСТЕЙ ШИФРІВ, ПРЕДСТАВЛЕНИХ НА УКРАЇНСЬКИЙ КОНКУРС ЗА ДОПОМОГОЮ НАБОРУ ТЕСТІВ NIST STS

В.І. Долгов, А.А. Настенко

Представляються матеріали по додатковому обґрунтуванню справедливості гіпотези про те, що великі шифри асимптотичне є випадковими підстановками. Тепер порівнюються між собою статистичні властивості ряду сучасних шифрів та їх зменшених моделей за допомогою тестів NIST STS. У їх числі розглянуті шифри, представлені на український конкурс, а також фіналіст конкурсу AES Rijndael шифри. Встановлено, що за розглянутими показниками українські шифри Калина, Мухомор і Лабіринт перевершують визнаного світового лідера блочного симетричного шифрування – шифр AES.

Ключові слова: *доказова стійкість, тести NIST STS, показники випадковості моделі і прототипу, випадкова підстановка, зменшена модель шифру.*

LARGE CIPHERS – RANDOM PERMUTATIONS. VERIFICATION OF STATISTICAL PROPERTIES CIPHERS SUBMITTED FOR UKRAINIAN CONTECST WITH A TEST SUITE NIST STS

V.I. Dolgov, A.A. Nastenko

Materials submitted for additional substantiation of the validity of the hypothesis that large codes are asymptotically random permutations. Now compare the statistical properties of each series of advanced ciphers and reduced models with Test NIST STS. Among them are considered ciphers submitted to the Ukrainian competition, and finalist of AES cipher Rijndael. It is established that the examined parameters Ukrainian ciphers Kalina, Amanita, and Maze exceed the recognized world leader block symmetric encryption – cipher AES.

Keywords: *provable resistance, tests NIST STS, accident rates, and a prototype model, the random substitution cipher model is reduced.*