УДК 681.3.067

Ю.Є. Яремчук

ДОСЛІДЖЕННЯ СТАТИСТИЧНОЇ БЕЗПЕКИ МЕТОДІВ АСИМЕТРИЧНОГО ШИФРУВАННЯ ІНФОРМАЦІЇ НА ОСНОВІ РЕКУРЕНТНИХ ПОСЛІДОВНОСТЕЙ

Проведено дослідження статистичної безпеки методів асиметричного шифрування відповідно на основі рекурентних U_k та V_k –послідовностей та здійснено їх порівняння з відомим методом Ель-Гамаля. Результати аналізу показали, що найвищий рівень статистичної безпеки має метод на основі V_k – послідовностей, який при найжорсткішому тестуванні показав найвищі показники за усіма тестами. У цілому методи на основі V_k та U_k –послідовностей мають вищі показники статистичної безпеки порівняно з існуючим методом шифрування Ель-Гамаля, особливо на менших розмірах ключа.

Ключові слова: криптографія, асиметричне шифрування, криптостійкість, статистична безпека, рекурентні послідовності.

Вступ

Вирішення задачі забезпечення конфіденційності інформації здійснюється за допомогою шифрування [1–4], яке поділяють на симетричне [1, 2] та асиметричне [3, 4]. Основною перевагою останнього є відсутність необхідності розподілу ключів секретним каналом зв'язку або третьої сторони (посередника) для реалізації цього.

Найбільш відомими асиметричними методами шифрування інформації є метод, що реалізує відомий стандарт RSA [5], стійкість якого базується на складності факторизації великих цілих чисел, а також метод Ель-Гамаля [6], стійкість якого базується на проблемі дискретного логарифмування.

В роботі [7] представлено метод асиметричного шифрування інформації на основі математичного апарату рекурентних V_k^+ та U_k –послідовностей. У порівнянні з відомим методом асиметричного шифрування Ель-Гамаля запропонований метод при забезпечені достатнього рівня криптостійкості має за певних умов меншу складність обчислень, а також має простішу процедуру завдання параметрів.

В роботі [8] запропоновано метод асиметричного шифрування інформації на основі математичного апарату лише рекурентних V_k –послідовностей, який, у порівнянні з методом представленим у роботі [7], забезпечив підвищення криптографічної стійкості шифрування за рахунок поєднання під час шифрування відкритого повідомлення та елементу послідовності, обчисленого за мультиплікативним, а не адитивним способом зміни індексу.

При цьому актуальним залишається визначення рівня практичної стійкості шляхом дослідження статистичної безпеки запропонованих у [7] та [8] методів асиметричного шифрування інформації та порівняння їх з відомим аналогом – методом Ель-Гамаля.

Дослідження статистичної безпеки методів асиметричного шифрування інформації на основі U_k та V_k –послідовностей.

Для дослідження статистичної безпеки асиметричних методів шифрування інформації використаємо пакет NIST STS (National Institute of Standard and Technologies Statistical Test Suite) [9], який на сьогодні є одним з кращих пакетів для статистичного тестування криптографічних схем та протоколів.

Пакет NIST STS включає у себе набір з 16 статистичних тестів. Дослідження методів асиметричного шифрування за допомогою цього пакету тестів будемо здійснювати за такою методикою [10]. Нехай задана двійкова послідовність S довжиною n бітів, тобто $S = \{S_1, S_2, ..., S_n\}$, $S_i \in \{0,1\}$. Для фіксованого значення n формуємо множину з m двійкових послідовностей. Сформована вибірка при цьому складатиме $N = m \times n$.

1) Далі будемо тестувати за допомогою пакету NIST STS кожну послідовність сформовану методом, в результаті якого отримаємо статистичний портрет сформованого секретного ключа.

2) Статистичний портрет послідовності являє собою масив розмірністю $m \times q$, де m – кількість послідовностей, що тестуються; q – кількість статистичних тестів, які використовуються для тестування кожної послідовності. Елементи масиву $P_{i,j} \in [0,1]$, де $i = \overline{1,m}$, $j = \overline{1,q}$, являють собою значення ймовірності, що отримана в результаті тестування i-ї послідовності j-м тестом.

3) За отриманим статистичним портретом визначаємо долю послідовностей, які пройшли кожен статистичний тест. Для цього задають рівень значимості $\alpha \in [0{,}001; 0{,}01]$ і здійснюють підрахунок значень імовірності P, що перевищує заданий рівень α для кожного з q тестів. У результаті формується вектор коефіцієнтів $R = \{r_1, r_2, ..., r_q\}$, елементи якого характеризують у процентному співвідношенні проходження послідовності S_i усіх статистичних тестів. Після цього здійснюється статистичний аналіз статистичного портрету. Отримані значення ймовірностей P_{ij} повинні задовольняти рівномірному закону розподілу на інтервалі $[0,1]$.

Заключний висновок щодо методу асиметричного шифрування будемо приймати таким чином. Будемо вважати, що метод шифрування G пройшов статистичне тестування пакетом NIST STS, якщо значення коефіцієнтів r_j для усіх $j = \overline{1,q}$ знаходяться всередині довірчого інтервалу $[r_{\min}, r_{\max}]$, де

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

і дотримується умова $\chi^2 > 0{,}0001$ для усіх $j = \overline{1,q}$, де χ^2 – критерій підкорення результатів рівномірному закону розподілу на інтервалі $[0,1]$.

Тестування методів асиметричного шифрування будемо проводити для різних довжин ключів, а саме 1024, 2048, 4096 бітів. Довжина послідовностей, які будуть отримуватись у результаті виконання шифрування буде 10^6 бітів. Дана довжина послідовності дозволяє виконувати тестування для усіх 16 тестів пакету NIST STS.

Для виконання тестування було обрано такі параметри:

– довжина послідовності, яка тестується $n = 10^6$ бітів;

– кількість послідовностей, які тестуються, для кожної довжини ключа, $m = 100$;

– кількість тестів $q = 188$;

– рівень значимості $\alpha = 0{,}001$ та $\alpha = 0{,}01$ відповідно у першому та другому експериментах.

Таким чином маємо: об’єм вибірки по 10^6 бітів для тестування кожного методу асиметричного шифрування. Статистичний портрет коду для кожної довжини ключа буде вміщувати у собі 18800 значень імовірності P.

Застосовуючи правило довірчого інтервалу для r_j, обчислюємо значення нижньої границі $r_{\min}$ за формулою (1). Для першого випадку, коли $\alpha = 0{,}001$, це складе

$$r_{\min} = 0{,}999 \pm 3\sqrt{\frac{0{,}999(1-0{,}999)}{100}} = 0{,}98952,$$

а для другого випадку, коли $\alpha = 0{,}01$, це складе

$$r_{\min} = 0{,}99 \pm 3\sqrt{\frac{0{,}99(1-0{,}99)}{100}} = 0{,}96015.$$

Вибір додаткових параметрів зроблено у відповідності з рекомендаціями описаними в NIST STS [9].

На основі цих початкових даних проаналізуємо отримані результати тестування послідовностей. У таблицях 1 і 2 наводяться дані про проходження результуючих послідовностей розміром 1024, 2048 та 4096 бітів усіма тестами згідно описаної методики.

Таблиця 1

Результати тестування методів асиметричного шифрування для $\alpha = 0{,}01$ та різних довжин ключів

Метод	Кількість тестів, які успішно пройшли тестування більше 99% послідовностей			Кількість тестів, які успішно пройшли тестування більше 96% послідовностей		
	1024 бітів	2048 бітів	4096 бітів	1024 бітів	2048 бітів	4096 бітів
Ель-Гамаля	41 (21,81%)	45 (23,94%)	61 (32,45%)	143 (76,06%)	158 (84,04%)	160 (85,11%)
U_k	53 (28,19%)	58 (30,85%)	56 (29,79%)	161 (85,64%)	162 (86,17%)	160 (85,11%)
V_k	59 (31,38%)	61 (32,45%)	57 (30,32%)	158 (84,04%)	159 (84,57%)	156 (82,98%)

Таблиця 2

Результати тестування методів асиметричного шифрування для $\alpha = 0{,}001$ та різних довжин ключів

Метод	Кількість тестів, які успішно пройшли тестування більше 99% послідовностей			Кількість тестів, які успішно пройшли тестування більше 98% послідовностей		
	1024 бітів	2048 бітів	4096 бітів	1024 бітів	2048 бітів	4096 бітів
Ель-Гамаля	126 (67,02%)	143 (76,06%)	149 (79,26%)	143 (76,06%)	161 (85,64%)	162 (86,17%)
U_k	153 (81,38%)	151 (80,32%)	145 (77,13%)	160 (85,11%)	162 (86,17%)	161 (85,64%)
V_k	143 (76,06%)	147 (78,19%)	142 (75,53%)	162 (86,17%)	162 (86,17%)	162 (86,17%)

З таблиць 1 та 2 видно, що при довжині ключа 1024 біти відсоток проходження тестів методами на основі U_k та V_k –послідовностей при порозі проходження $\alpha = 0{,}01$ вищий (на 7% і 10% відповідно), ніж у метода Ель-Гамаля, а при пониженні порогу до $\alpha = 0{,}001$, найкращі результати показав саме метод на основі U_k –послідовностей.

З таблиць 1 і 2 також видно, що при довжині ключа 2048 бітів при більш жорстких параметрах проходження тестування ($\alpha = 0{,}01$) метод на основі V_k –послідовностей показав найкращі результати (36,70%) порівняно з методом Ель-Гамаля та методом на основі U_k –послідовностей (23,94% і 30,85% відповідно). Зі зменшенням порогового значення у 10 разів ($\alpha = 0{,}001$) відсоток проходження тестів послідовностями за методом Ель-Гамаля зріс у 3 рази і показав кращі показники порівняно з методом на основі V_k –послідовностей (76,06% порівняно з 71,28%). Найкращим для даного випадку виявився метод на основі U_k –послідовностей, пройшовши 80,23% тестів.

При тестуванні послідовностей з довжиною ключа 4096 бітів відсотки проходження тестів методом Ель-Гамаля збільшуються. З таблиць 1 і 2 видно, що відсоток проходження тестів послідовностями на основі V_k – та U_k –послідовностей гірший, ніж в метода Ель-Гамаля (30,32% та 29,79% порівняно з 32,45%) при найжорсткішому порозі проходження (проходженням 99% послідовностей тестів при $\alpha = 0{,}01$).

Порівняємо коди з рівнем значимості $\alpha = 0{,}001$ до оцінки за приведеною методикою. В таблиці 3 наведено результати порівняння для різних довжин ключів.

Таблиця 3

Відсотки проходження кожного з 16 тестів для $\alpha = 0{,}001$ та різних довжин ключів

№ тесту	Назва статистичного тесту	1024 бітів			2048 бітів			4096 бітів		
		Е-Г	**U_k**	**V_k**	**Е-Г**	**U_k**	**V_k**	**Е-Г**	**U_k**	**V_k**
1	Частотний (монобітний) тест	100%	100%	99%	100%	100%	100%	100%	100%	100%
2	Частотний тест всередині блоку	100%	100%	100%	99%	100%	100%	98%	100%	99%
3	Послідовний тест	100%	99%	100%	99%	100%	100%	83%	100%	100%
4	Перевірка максимальної довжини серії в блоці	100%	100%	100%	100%	99%	100%	96%	100%	100%
5	Перевірка рангу двійкової матриці	100%	100%	99%	100%	100%	100%	100%	100%	100%
6	Спектральний тест на основі дискретного перетворення Фур'є	100%	100%	100%	100%	100%	100%	100%	100%	100%
7	Перевірка шаблонів, які не перекриваються	100%	100%	100%	100%	100%	100%	100%	100%	100%
8	Перевірка шаблонів, які перекриваються	100%	100%	100%	100%	100%	99%	94%	100%	100%
9	Універсальний тест Маурера	99%	100%	100%	99%	100%	100%	100%	99%	100%
10	Перевірка лінійної складності	99%	100%	100%	100%	100%	100%	99%	100%	100%
11	Перевірка серій	100%	100%	100%	100%	100%	100%	93%	100%	100%
12	Ентропійний тест	100%	100%	99%	100%	100%	100%	91%	100%	100%
13	Перевірка накоплених сум	100%	100%	100%	100%	100%	100%	100%	100%	100%
14	Перевірка випадкових відхилень	61%	64%	57%	68%	60%	64%	51%	64%	67%
15	Перевірка випадкових відхилень (модифікація)	61%	64%	57%	68%	60%	64%	51%	64%	67%
16	Перевірка стиснення по алгоритму Лемпеля-Зіва	100%	100%	99%	100%	100%	100%	100%	100%	100%

Як видно з результатів наведених у таблиці 3, усі послідовності мають майже однакові показники для усіх видів тестів, найнижчі показники тести отримали при тестуванні послідовностей звичайним та модифікованим тестами на перевірку випадкових відхилень. При розмірі ключа у 1024 біти найвищі показники має метод на основі U_k –послідовностей (61%). Проте при довжині ключа у 2048 бітів найвищі показники в цих тестах отримав саме метод Ель-Гамаля (68%). При найбільшій довжині ключа у 4096 біт, найкращі результати отримав метод на основі V_k –послідовностей. Також видно, що при даній довжині ключа методи на основі V_k та U_k –послідовностей зберегли показники 99–100% по іншим тестам, а метод Ель-Гамаля знизив показники до 83–94%. Це дає підстави говорити, що методи на основі V_k та U_k –послідовностей у цілому є більш статистично безпечними, ніж метод Ель-Гамаля.

Порівняємо коди, збільшивши рівень значимості $\alpha = 0{,}01$, що є більш жорстким підходом до оцінки за приведеною методикою. В таблиці 4 наведено результати порівняння для різних довжин ключів.

Таблиця 4

Відсотки проходження кожного з 16 тестів для $\alpha = 0{,}01$ та різних довжин ключів

№ тесту	Назва статистичного тесту	1024 бітів			2048 бітів			4096 бітів		
		Е-Г	**U_k**	**V_k**	**Е-Г**	**U_k**	**V_k**	**Е-Г**	**U_k**	**V_k**
1	Частотний (монобітний) тест	98%	98%	100%	97%	98%	100%	100%	100%	99%
2	Частотний тест всередині блоку	93%	98%	99%	99%	100%	97%	98%	100%	98%
3	Послідовний тест	74%	99%	98%	98%	98%	100%	98%	98%	100%
4	Перевірка максимальної довжини серії в блоці	96%	99%	100%	99%	98%	99%	99%	99%	98%
5	Перевірка рангу двійкової матриці	99%	99%	99%	100%	100%	99%	100%	100%	98%

6	Спектральний тест на основі дискретного перетворення Фур'є	98%	99%	100%	99%	99%	100%	100%	98%	99%
7	Перевірка шаблонів, які не перекриваються	98%	99%	99%	99%	99%	99%	99%	99%	99%
8	Перевірка шаблонів, які перекриваються	91%	100%	100%	98%	99%	97%	95%	98%	99%
9	Універсальний тест Маурера	100%	99%	98%	98%	98%	98%	99%	99%	99%
10	Перевірка лінійної складності	97%	98%	99%	98%	99%	99%	98%	97%	99%
11	Перевірка серій	90%	99%	100%	97%	98%	99%	100%	98%	100%
12	Ентропійний тест	89%	99%	99%	97%	98%	100%	100%	99%	98%
13	Перевірка накоплених сум	98%	98%	99%	97%	98%	98%	100%	99%	99%
14	Перевірка випадкових відхилень	51%	64%	67%	67%	60%	64%	60%	63%	57%
15	Перевірка випадкових відхилень (модифікація)	50%	63%	67%	67%	60%	64%	61%	63%	56%
16	Перевірка стиснення по алгоритму Лемпеля-Зіва	98%	98%	100%	97%	98%	100%	100%	100%	99%

Як видно з результатів наведених у таблиці 4, починаючи вже з довжини ключа у 1024 біти, метод Ель-Гамаля показує гірші показники порівняно з іншими методами. Так при тесті на перевірку шаблонів, які перекриваються, метод показує найгірший показник (91%) порівняно з іншими методами (100%). Також низькими значеннями виділяється послідовний тест. В ньому метод Ель-Гамаля отримав в 1,5 рази нижчі показники порівняно з іншими методами (74% порівняно з 98–99%). В тестах на перевірку випадкових відхилень найкращі показники отримав метод на основі V_k –послідовностей. При збільшенні довжини ключа статистичний портрет методу Ель-Гамаля покращується, проте показники усе одно залишаються нижчими, ніж у методах на основі V_k та U_k –послідовностей. Так при довжині ключа у 2048 бітів найкращі показники отримав метод на основі V_k –послідовностей, а при довжині ключа у 4096 бітів його на невеликий відсоток випередив метод на основі U_k –послідовностей.

На рисунках 1–3 представлено статистичні портрети методів асиметричного шифрування для довжини ключа 1024 бітів з вказанням їх параметрів і способів формування.

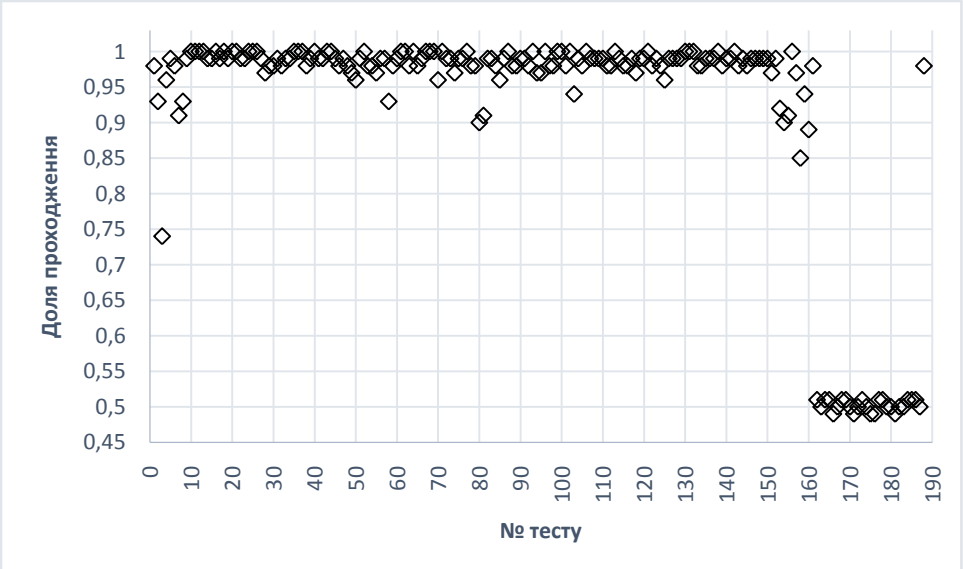

Рис. 1. Результати тестування методу шифрування Ель-Гамаля з розміром ключа 1024 біт

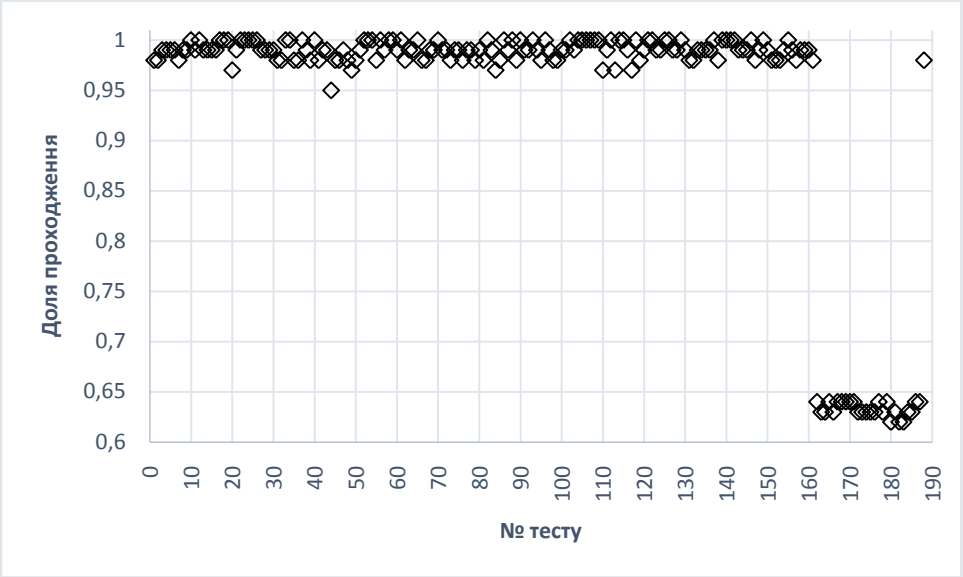

Рис. 2. Результати тестування методу шифрування на основі U_k –послідовностей з розміром ключа 1024 біт

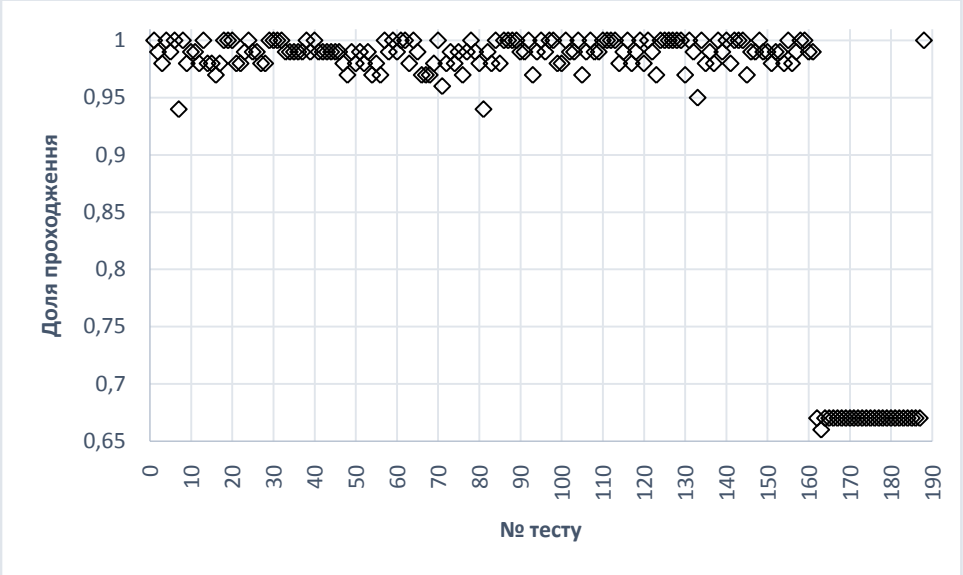

Рис. 3. Результати тестування методу шифрування на основі V_k –послідовностей з розміром ключа 1024 біт

Як видно з рисунків 1–3, статистичні портрети методів знаходяться на високому рівні, виключення становлять тести 161–186, яким відповідають тести на перевірку випадкових відхилень. Ці тести є найжорсткішими порівняно з іншими, тому ці показники є очікуваними. З рисунків видно, що частка проходження 90% тестів для послідовностей методів шифрування на основі V_k та U_k –послідовностей вища за 0,98, порівняно з методом Ель-Гамаля (0,94), що свідчить про вищу статистичну безпеку цих методів.

Узагальнимо результати тестування, показавши частку проходження для кожного тесту з статистичного пакету NIST. На рисунках 4–6 показано узагальнені графіки по кожному тесту для кожного методу шифрування та довжини ключа.

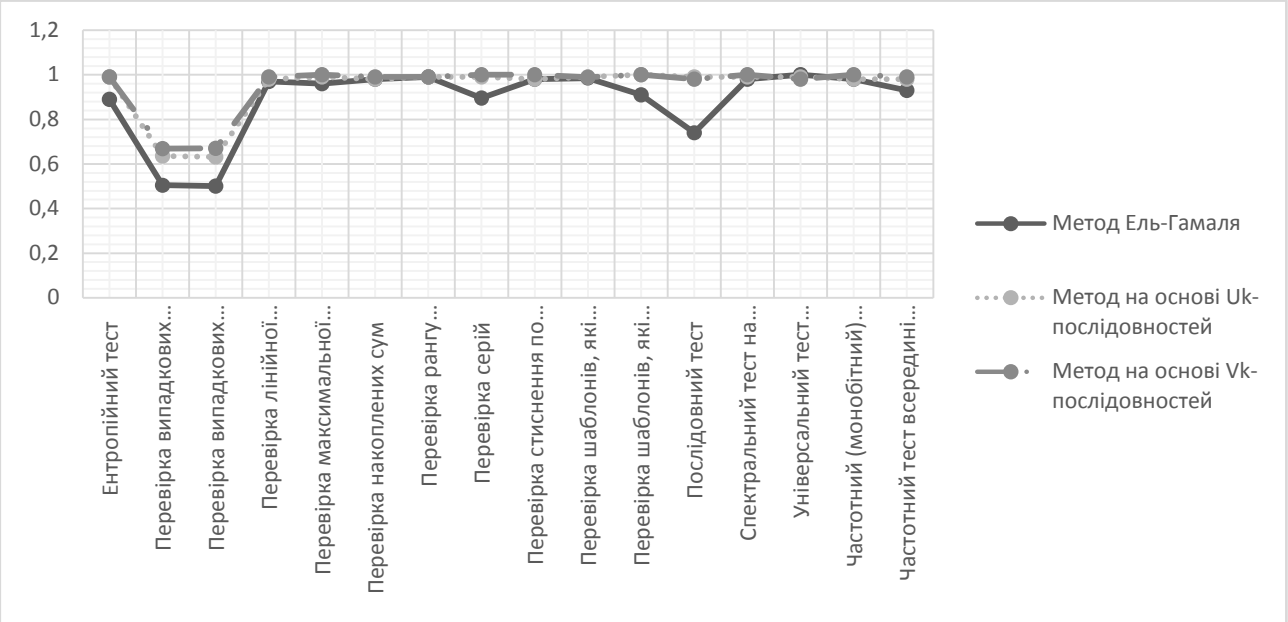

Рис. 4. Частка проходження тестів для послідовностей з розміром ключа 1024 біт

Як видно з графіків на рисунку 4, методи на основі V_k та U_k –послідовностей для довжини ключа 1024 бітів показали кращі результати майже в усіх тестах. В послідовному тесті, та тестах на перевірку серій і перевірку випадкових відхилень метод Ель-Гамаля показав найгірші показники. В усіх інших тестах отримані результати кращі, або на такому ж рівні, як в методах на основі V_k та U_k –послідовностей. Найвищі показники спостерігаються в послідовностях методу на основі V_k –послідовностей, що показує його з найкращого боку в якості генератора ПВП для довжини ключа у 1024 біти.

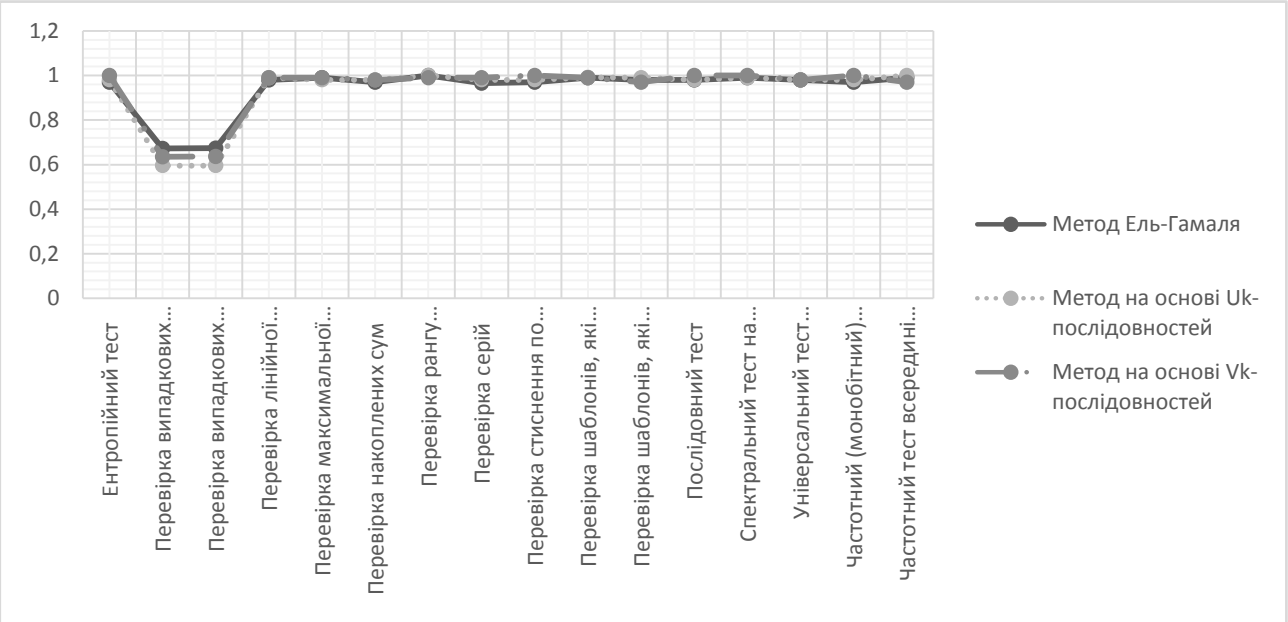

Рис. 5. Частка проходження тестів для послідовностей з розміром ключа 2048 біт

Як видно з графіків на рисунку 5, при збільшені довжини ключа статистичний портрет методів шифрування майже не змінюється. Виключенням є послідовний тест, а також тести на перевірку випадкових відхилень. Частки проходження цих тестів для послідовностей методу Ель-Гамаля збільшились і досягли того ж рівня, що методи на основі U_k та V_k –

послідовностей. Однак у цілому методи на основі рекурентних послідовностей показують себе більш стійкими, оскільки вони мають приблизно той же рівень статистичної безпеки для даної довжини ключа, але з ключами удвічі меншої довжини мають у цілому кращий рівень статистичної безпеки.

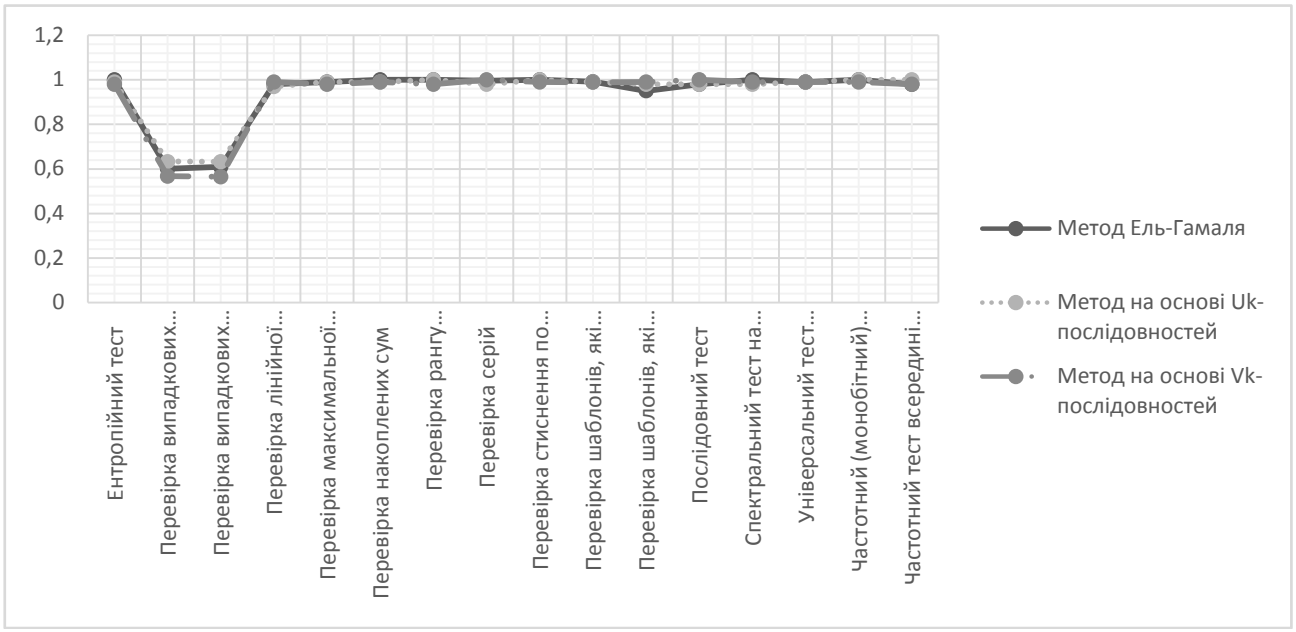

Рис. 6. Частка проходження тестів для послідовностей з розміром ключа 4096 біт

При тестуванні з довжиною ключа у 4096 (рис. 6) показники тримаються на тому ж рівні, що і у попередніх тестах, тільки послідовності метода Ель-Гамаля мають гірші показники (на 0,03) порівняно з методами на основі V_k та U_k –послідовностей у тесті на перевірку шаблонів, які перекриваються.

Висновки

Дослідження запропонованих у [7] та [8] методів асиметричного шифрування відповідно на основі U_k та V_k –послідовностей порівняно з відомим методом асиметричного шифрування Ель-Гамаля показало, що методи на основі рекурентних послідовностей, а особливо метод на основі V_k –послідовностей, мають значні переваги щодо статистичного безпеки перед існуючими аналогами, показуючи вищі показники на менших розмірах ключа.

Дослідження показало, що при довжині ключа у 1024 біти статистична безпека методів на основі V_k та U_k –послідовностей, або на такому ж рівні, або вища (на 33%), порівняно з методом Ель-Гамаля. При дослідженні з довжиною ключа у 2048 та 4096 біт, показники тестування послідовностей Ель-Гамаля зросли і зрівнялись з показниками методів основі V_k та U_k –послідовностей.

При тестуванні з рівнем значимості $\alpha = 0{,}001$ метод Ель-Гамаля має середні показники (61%) порівняно з методами на основі U_k (64%) та V_k (57%) – послідовностей. Хоча, при розмірі ключа 4096 біт, 100% проходження майже усіх тестів отримали методи на основі V_k та U_k –послідовностей, що є високим показником статистичної безпеки.

Порівнюючи результати тестування з рівнем значимості $\alpha = 0{,}01$, найкращі показники показав метод на основі V_k –послідовностей. Найменш статистично стійким виявився метод

Ель-Гамаля, отримавши нижчі показники (50–100%) порівняно з методами на основі U_k (63–100%) та V_k (67–100%) – послідовностей.

За результатами тестування можна констатувати, що запропоновані методи асиметричного шифрування на основі V_k та U_k –послідовностей мають високі показники статистичної безпеки порівняно з існуючим методом шифрування Ель-Гамаля, але при найжорсткішому тестуванні найвищий рівень статистичної безпеки показав саме метод на основі V_k –послідовностей, отримуючи найвищі показники за усіма тестами, випереджаючи результати тестування послідовностей за методом на основі U_k –послідовностей.

Література

1. Menezes, A.J. Handbook of Applied Cryptography [Текст] / A.J. Menezes, P.C. van Oorschot, S.A. Vanstone. – CRC Press, 2001. – 816 p.

2. Шнайер, Б. Прикладная криптография. Протоколы, алгоритмы, исходные тексты на языке Си [Текст] / Б. Шнайер. – М.: Триумф, 2002. – 816 с.

3. Молдавян, Н. А. Теоретический минимум и алгоритмы цифровой подписи [Текст] / Н. А. Молдавян. – СПб.: БХВ-Петербург, 2010. – 304 с.

4. Саломаа, А. Криптография с открытым ключом: Пер. с англ [Текст] / А. Саломаа. – М.: Мир. – 1995. – 318 с.

5. Rivest, R.L. A method for obtaining digital signatures and public-key cryptosystems [Текст] / R.L. Rivest, A. Shamir, and L.M. Adleman // Communications of the ACM. – 1978. – Volume 21, Issue 2. – P. 120–126.

6. ElGamal, T. A public key cryptosystem and a signature scheme based on discrete logarithms [Текст] / T. ElGamal // IEEE Intern. Symp. Informat. Theory. – 1985. – V.IT–31. №4. – P. 469–472.

7. Яремчук, Ю.Є. Метод асиметричного шифрування інформації на основі рекурентних послідовностей [Текст] / Ю.Є. Яремчук // Сучасна спеціальна техніка. – №4, 2012. – С. 79–87.

8. Яремчук, Ю.Є. Метод шифрування інформації з відкритим ключем на основі рекурентних послідовностей [Текст] / Ю.Є. Яремчук // Інформаційна безпека. – №3, 2013. – С. 123–129.

9. NIST SP 800-22 Rev. 1a. A Statistical Test Suite for Random and Pseudorandom Number Generators for Cryptographic Applications [Текст] / [A. Rukhin, J. Soto, J. Nechvatal, M. Smid, E. Barker, S. Leigh, M. Levenson, M. Vangel, D. Banks, A. Heckert, J. Dray, S. Vo]. – National Institute of Standards and Technology, 2010. – 131 p.

10. Иванов, М.А. Теория, применение и оценка качества генераторов псевдослучайных последовательностей [Текст] / М.А. Иванов, И.В. Чугунков. – М.: КУДИЦ-ОБРАЗ, 2003. – 240 с.

Надійшла 23.05.2014 р. Рецензент: д.т.н., проф. Шелест М.Є.