УДК 681.3.067

Informatics and Mathematical Methods in Simulation
Vol. 4 (2014), No. 1, pp. 26-34

ДОСЛІДЖЕННЯ СТАТИСТИЧНОЇ БЕЗПЕКИ МЕТОДІВ ВІДКРИТОГО РОЗПОДІЛУ СЕКРЕТНИХ КЛЮЧІВ НА ОСНОВІ РЕКУРЕНТНИХ ПОСЛІДОВНОСТЕЙ

Ю.Є. Яремчук

Вінницький національний технічний університет,
вул. Хмельницьке шосе, 95, Вінниця, 21021, Україна; e-mail: yurevyar@vntu.net

Проведено дослідження статистичної безпеки методів відкритого розподілу секретних ключів відповідно на основі рекурентних U_k та V_k –послідовностей та здійснено їх порівняння з відомим методом Діффі-Хеллмана. Результати аналізу показали, що найвищий рівень статистичної безпеки має метод на основі V_k – послідовностей, пройшовши вдвічі більшу кількість тестів порівняно з методом Діффі-Хеллмана, у той же час метод на основі U_k –послідовностей пройшов у 1.5 рази більшу кількість тестів, ніж відомий аналог.

Ключові слова: криптографія, розподіл секретних ключів, криптостійкість, статистична безпека, рекурентні послідовності.

Вступ

Відкритий розподіл ключів [1] дозволяє двом сторонам виробляти спільний секретний ключ шляхом обміну відкритими повідомленнями без використання будь-якої заздалегідь виробленої спільної секретної інформації. При цьому жодна із сторін не може наперед визначити значення ключа, так як ключ залежить від повідомлень, що безпосередньо передаються в процесі обміну.

Вперше метод відкритого розподілу секретних ключів був запропонований Діффі та Хеллманом [2].

В роботі [3] представлено метод розподілу секретних ключів відкритим каналом, який базується на рекурентних V_k^+ та U_k –послідовностях. У порівнянні з відомим методом розподілу ключів Діффі-Хеллмана запропонований метод забезпечує для кожного користувача майже вдвічі меншу складність обчислень, а також має простішу процедуру завдання параметрів.

В роботі [4] запропоновано метод відкритого розподілу секретних ключів на основі математичного апарату лише рекурентних V_k –послідовностей, який, у порівнянні з методом представленим у роботі [3], забезпечив підвищення криптографічної стійкості розподілу ключів за рахунок отримання спільного ключа на завершальному етапі розподілу у вигляді 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 [3] та [4] методів відкритого розподілу секретних ключів та порівняння їх з відомим аналогом.

Метою роботи є дослідження статистичної безпеки запропонованих у [3] та [4] методів відкритого розподілу секретних ключів на основі рекурентних U_k та V_k –послідовностей та порівняння їх з відомим методом Діффі-Хеллмана.

Дослідження статистичної безпеки методів розподілу секретних ключів на основі U_k та V_k –послідовностей

На сьогодні одним з кращих пакетів для статистичного тестування криптографічних схем та протоколів є розроблений у 1999 році пакет NIST STS (National Institute of Standard and Technologies Statistical Test Suite) [5], який був розроблений в рамках проекту AES (Advanced Encryption Standard) і включає у себе набір з 16 статистичних тестів, які на сьогодні найкращим чином відповідають висунутим вимогам щодо статистичного тестування криптографічних схем/протоколів.

Для дослідження методів розподілу ключів використаємо пакет NIST STS за такою методикою. 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 $N = m \times n$.

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

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.

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 стосовно методу розподілу секретними ключами будемо приймати таки чином. Вважатимемо, що метод розподілу секретних ключів G пройшов статистичне тестування пакетом NIST STS, якщо значення коефіцієнтів r_j для усіх $j = \overline{1,q}$ знаходяться всередині довірчого інтервалу $[r_{\max}, r_{\min}]$, де

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

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 буде проходити для різних довжин ключів, а саме 1024, 2048 та 4096 бітів. Довжина послідовностей, які будуть отримуватись у результаті виконання

розподілу ключів буде 1024, 2048 та 4096 бітів відповідно. Дана довжина послідовностей дозволяє виконувати тестування лише для 11 тестів, що виключає тест на перевірку шаблонів, що перекриваються, універсальний тест Маурера, тест на перевірку стискання за алгоритмом Лемпеля-Зіва, тест на перевірку випадкових відхилень та модифікований тест на перевірку випадкових відхилень, так як необхідна довжина послідовностей, що проходять тестування, є недостатньою для успішного проходження чи отримання достовірних результатів даних тестів.

Для виконання тестування було обрано такі параметри:

- довжина послідовності n, що тестується, дорівнює 1024, 2048 та 4096 бітів відповідно до довжини ключа;
- кількість послідовностей, які тестуються для кожної довжини ключа, $m = 100$;
- кількість тестів $q = 159$;
- рівень значимості $\alpha = 0.01$ та $\alpha = 0.001$ відповідно у першому та другому експериментах.

Таким чином маємо: об'єм вибірки 102400, 204800 та 409600 бітів при тестуванні методу розподілу секретних ключів Діффі-Хеллмана; 204800, 409600 та 919200 бітів при тестуванні методу на основі U_k –послідовностей; 307200, 614400 та 1228800 бітів при тестуванні методу на основі V_k –послідовностей. Статистичний портрет коду для кожної довжини ключа буде вміщувати у собі 15900 значень імовірності P.

Застосовуючи правило довірчого інтервалу для r_j, обчислюємо значення нижньої границі за формулою (1). Тоді для $\alpha = 0.001$ та $\hat{p} = 1 - \alpha = 0.999$ $r_{\min}$ складе

$$r_{\min} = 0.999 \pm 3\sqrt{\frac{0.999(1-0.999)}{100}} = 0.98952,$$

а для $\alpha = 0.01$ та $\hat{p} = 1 - \alpha = 0.99$ $r_{\min}$ 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 [5].

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

З таблиць 1 та 2 видно, що при довжині ключа 1024 біти відсотки проходження тестів доволі малі. Такі низькі показники зумовлені малою довжиною послідовності, а більшість тестів розраховані на довжину від 100000 біт. Проте вже видно, що методи розподілу ключів на основі рекурентних послідовностей мають кращі показники порівняно з відомим методом Діффі–Хеллмана. Відсоток проходження тестів за методами на основі V_k та U_k –послідовностей при порозі проходження $\alpha = 0.01$ має незначне відхилення від відсотку проходження за методом на основі протоколу Діффі–Хеллмана, проте, у разі пониження порогу до $\alpha = 0.001$, відсоток проходження у 1.5 рази перевищує відсоток проходження методу на соснові протоколу Діффі–Хеллмана. Такі результати досягаються завдяки успішному проходженню більшості тестів для тесту перевірки шаблонів, які не перекриваються.

Таблиця 1.

Результати тестування методів розподілу ключів згідно описаної методики 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
Діффі-Хеллмана	8 (5.03%)	6 (3.77%)	12 (7.55%)	69 (43.40%)	67 (42.14%)	112 (70.44%)
U_k	5 (3.14%)	15 (9.43%)	18 (11.32%)	69 (43.40%)	115 (72.33%)	130 (81.76%)
V_k	6 (3.77%)	15 (9.43%)	24 (15.09%)	56 (35.22%)	116 (72.96%)	134 (84.28%)

Таблиця 2.

Результати тестування методів розподілу ключів згідно описаної методики 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
Діффі-Хеллмана	30 (18.87%)	59 (37.11%)	86 (54.09%)	75 (47.17%)	112 (70.44%)	136 (85.53%)
U_k	53 (33.33%)	83 (52.20%)	92 (57.86%)	113 (71.07%)	135 (84.91%)	141 (88.68%)
V_k	48 (30.19%)	81 (50.94%)	101 (63.52%)	99 (62.26%)	128 (80.50%)	150 (94.34%)

З таблиць 1 та 2 також видно, що при довжині ключа 2048 бітів спостерігається значний приріст у відсотках проходження тестів послідовностями згідно методів на основі U_k та V_k–послідовностей. Задаючи порогове значення $\alpha = 0.01$, тестування результату ключового розподілу для методів на основі як U_k так і V_k–послідовності показало набагато більший відсоток проходження тестів (у 2.5 рази) порівняно з послідовностями на основі протоколу Діффі-Хеллмана. Зі зменшенням порогового значення у 10 разів ($\alpha = 0.001$) відсоток проходження тестів послідовностями за методом Діффі-Хеллмана зріс, проте усе одно становив нижче (у 1.5 рази) за відсотки проходження тестів послідовностями на основі методів, що базуються на U_k та V_k–послідовностях.

При тестуванні послідовностей з довжиною ключа 4096 бітів відсотки проходження тестів збільшуються. З таблиць 1 і 2 видно, що відсоток проходження тестів послідовностями на основі V_k та U_k–послідовностей відповідно у 2 та 1.5 рази перевищує відсоток проходження тестів послідовностями для методу Діффі–Хеллмана при найжорсткішому порозі проходження (проходженням 99% послідовностей тестів для $\alpha = 0.01$).

Порівняємо коди з рівнем значимості $\alpha = 0.01$ до оцінки за приведеною методикою. В таблиці 3 наведено результати порівняння для різних довжин ключів.

Таблиця 3.

Відсотки проходження кожного з 11 тестів для $\alpha = 0.01$ та різних довжин ключів

№ тесту	Назва статистичного тесту	1024 бітів			2048 бітів			4096 бітів		
		Д-Х	U_k	V_k	Д-Х	U_k	V_k	Д-Х	U_k	V_k
1	Частотний (монобітний) тест	100%	100%	100%	100%	100%	100%	99%	99%	100%
2	Частотний тест всередині блоку	98%	99%	99%	100%	100%	98%	100%	99%	100%
3	Послідовний тест	97%	99%	97%	96%	99%	100%	99%	98%	99%
4	Перевірка максимальної довжини серії в блоці	100%	100%	99%	98%	99%	99%	98%	100%	98%
5	Перевірка рангу двійкової матриці	100%	95%	97%	99%	98%	100%	100%	99%	98%
6	Спектральний тест на основі дискретного перетворення Фур'є	100%	98%	100%	95%	98%	96%	100%	99%	99%
7	Перевірка шаблонів, які не перекриваються	96%	96%	95%	96%	97%	97%	97%	98%	98%
8	Перевірка лінійної складності	94%	93%	97%	94%	98%	95%	95%	99%	100%
9	Перевірка серій	99%	98%	98%	99%	99%	100%	97%	99%	100%
10	Ентропійний тест	96%	100%	98%	97%	100%	100%	100%	98%	98%
11	Перевірка накоплених сум	100%	100%	100%	100%	100%	100%	100%	100%	100%

Як видно з результатів табл. 3, найкращі показники знову отримав метод на основі V_k –послідовностей. Найслабкішим метод виявився у тестах на перевірку лінійної складності, спектральному тесті на основі дискретного перетворення Фур'є та тесті перевірці шаблонів, які не перекриваються. В останніх тестах метод Діффі-Хеллмана має ще нижчі показники (94–97%) порівняно з методами на основі U_k (93–100%) та V_k (95–100%) – послідовностей, хоча при розмірі ключа 2048 бітів метод на основі U_k –послідовностей показав найгірші (93%) показники в тесті перевірки

лінійної складності, що свідчить про те, що отриманий в результаті тестування розподіл відрізняється від очікуваного.

Отримано також результати проходження тестів і для $\alpha = 0.001$, які показали більші відсотки проходження тестів. Проведено також порівняння, яке показало, що метод Діффі-Хеллмана має нижчі показники (94–99%) порівняно з методами на основі U_k (99–100%) та V_k (99–100%) – послідовностей у тестах на перевірку шаблонів, що не перекриваються та перевірку лінійної складності. Хоча, при розмірі ключа 4096 біт, 100% проходження усіх тестів отримав саме метод на основі V_k –послідовностей, що говорить про його кращу статистичну безпеку.

Узагальнимо результати тестування, показавши частку проходження для кожного тесту із статистичного пакету NIST. На рисунках 1–3 показані графіки з узагальненими результатами тестування по кожному тесту для кожного методу та довжини ключа.

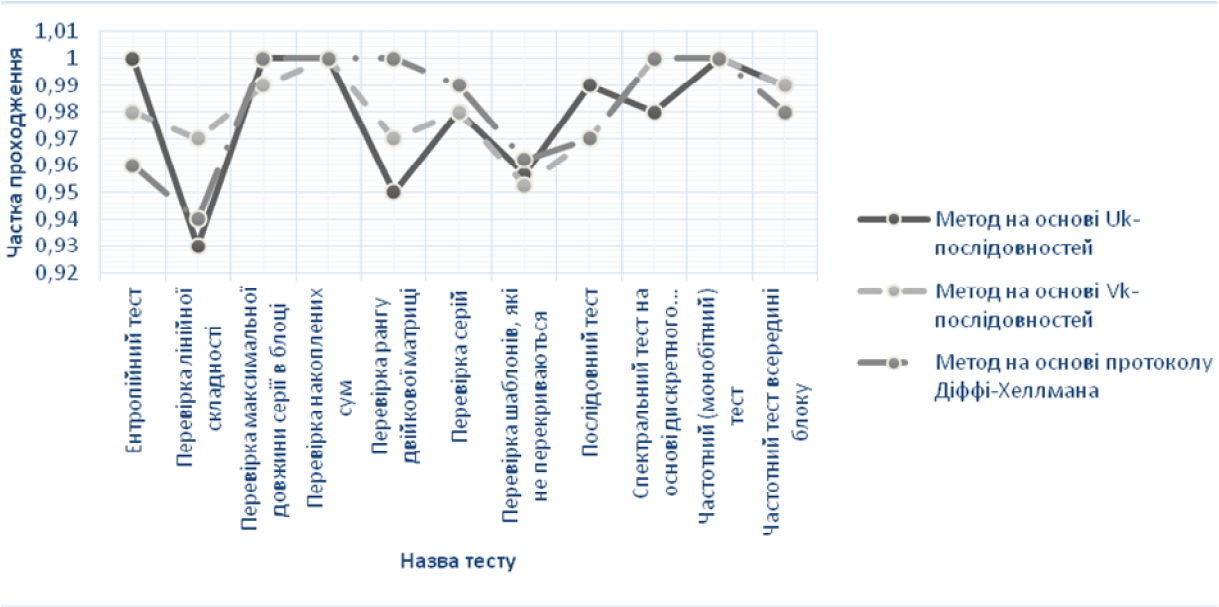

Рис. 1. Частка проходження тестів для послідовностей з розміром ключа 1024 біти

Як видно з графіку рис. 1, методи на основі U_k та V_k –послідовностей для довжини ключа 1024 бітів показали кращі результати в усіх тестах окрім тесту на перевірку рангу двійкової матриці. В усіх інших тестах отримані результати кращі, або на такому ж рівні, як і в методі Діффі-Хеллмана. Найгірше себе показав метод на основі U_k –послідовностей у тесті на перевірку лінійної складності та перевірку рангу двійкової матриці, а метод на основі V_k –послідовностей в усіх тестах мав показники або найвищі, або такі, що мали незначно менше значення за найвищий показник. Тобто метод розподілу секретних ключів на основі V_k –послідовностей для довжини ключа у 1024 бітів має найкращі показники як генератора ПВП.

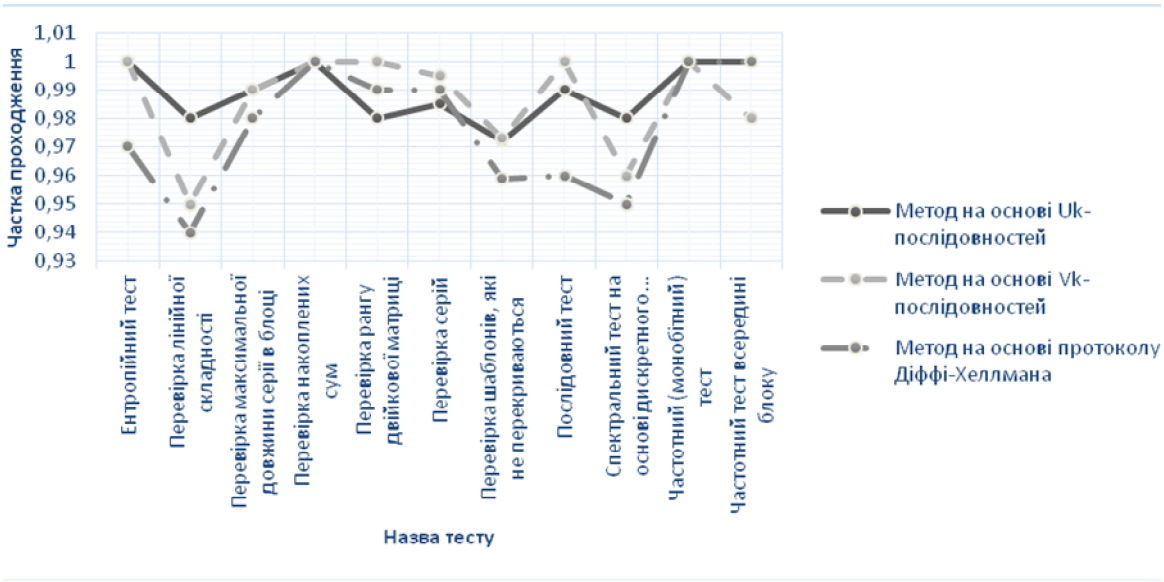

Рис. 2. Частка проходження тестів для послідовностей з розміром ключа 2048 біти

Як видно з рис. 2, при збільшені довжини ключа частка проходження усіх тестів збільшується, що є гарним показником, який свідчить про якісне збільшення статистичної безпеки створених ключів. При цьому метод Діффі-Хеллмана має найгірші (на 0.01 менші) показники вже з більшості тестів порівняно з попереднім розміром ключа у 1024 біти. В таких тестах як перевірка лінійної складності та спектральний тест на основі дискретного перетворення Фур'є найвищі показники (на 0.02–0.03 більше) показав метод на основі U_k–послідовностей. У більшості тестах частка проходження тестів послідовностями на основі V_k–послідовностей мають однакові з іншими або вищі (на 0.01) частки проходження тестів. В середньому, за рівномірною ламаною часток проходження можна прийняти рішення, що послідовності на основі V_k–послідовностей мають більш рівномірні характеристики, що є гарним показником як для генератора ПВП.

З рис. 3 видно, що послідовності за методом Діффі-Хеллмана продовжують програвати послідовностям за методами на основі U_k та V_k–послідовностей, показуючи найнижчу частку проходження у 0.95 не лише в одному тесті перевірки лінійної складності, а й усього графіка в цілому. Частки проходження тестів послідовностями за методом на основі U_k–послідовностей є рівномірними (0.98–1), проте місцями мають найгірші результати (послідовний тест і частотний тест в середині блоку). В більшості тестах частка проходження тестів послідовностями за методом на основі V_k–послідовностей також коливається у діапазоні 0.98–1, проте найгірший результат присутній тільки в одному тесті, а саме перевірці рангу бінарної матриці. В усіх інших результатах метод на основі V_k–послідовностей показує або однакові або кращі показники, що свідчить про високий рівень статистичної безпеки.

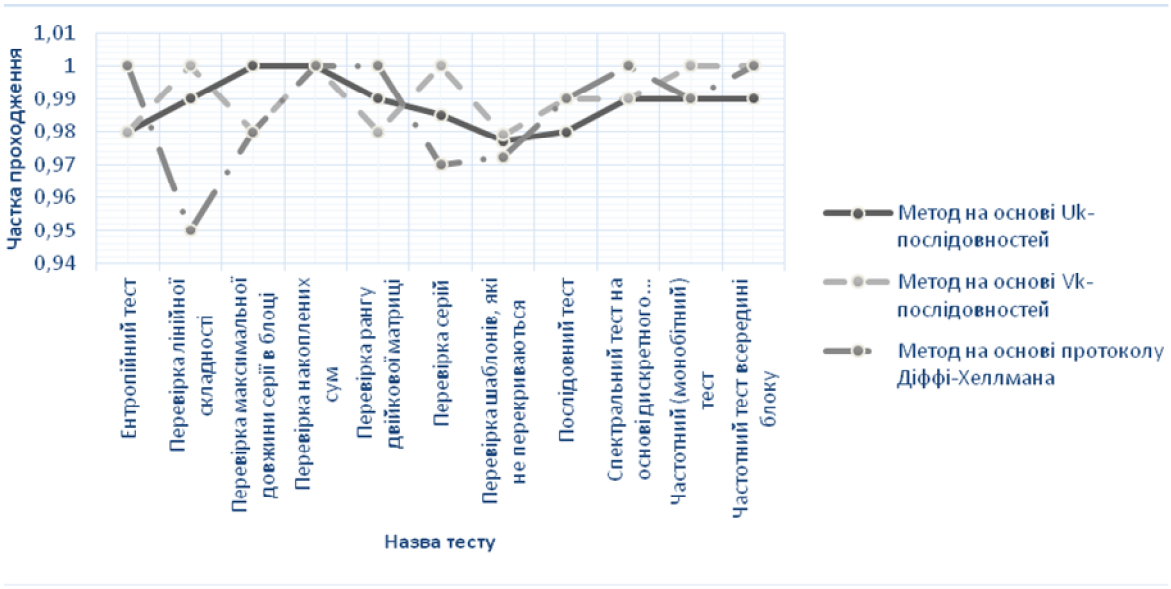

Рис. 3. Частка проходження тестів для послідовностей з розміром ключа 4096 біти

Висновки

Дослідження показало, що зі збільшенням довжини ключа в методах на основі V_k та U_k –послідовностей суттєво збільшується і статистична безпека отриманих послідовностей. Так, якщо при довжині ключа у 1024 біти послідовності успішно пройшли лише 6 (3.77%) та 5 (3.14%) тестів відповідно, то при ключі у 2048 біти ці показники зросли у 2.5 рази і вже становили 15 (9.43%) в обох випадках. При тестуванні з більш жорстким рівнем значимості $\alpha = 0.01$ та рівнем проходження тестів у 99% метод розподілу секретних ключів на основі V_k –послідовностей з довжиною ключа 4096 бітів пройшов 24 тести з 159 тестів, в той час як метод на основі протоколу Діффі-Хеллмана лише 12, що вдвічі перевищує рівень статистичної безпеки відомого аналогу. При цьому метод на основі U_k –послідовностей показав нижчі результати порівняно з методом на основі V_k –послідовностей (18 з 159 тестів), проте і вони кращі за результати тестування методу Діффі-Хеллмана, що робить методи на основі V_k та U_k –послідовностей одними з кращих аналогів щодо стійкості серед існуючих методів розподілу секретних ключів.

При порівнянні результатів тестування з рівнем значимості $\alpha = 0.01$ найкращі показники показав метод на основі V_k –послідовностей. Найменшу статистичну стійкість має метод Діффі-Хеллмана з показниками (94–97%) порівняно з методами на основі U_k (93–100%) та V_k (95–100%) – послідовностей.

У цілому результати тестування показують, що запропоновані методи розподілу секретних ключів на основі V_k та U_k –послідовностей мають високі показники статистичної безпеки порівняно з відомим методом Діффі-Хеллмана. Найвищий рівень статистичної безпеки має метод на основі V_k –послідовностей, який пройшов удвічі більшу кількість тестів порівняно з методом Діффі-Хеллмана, при цьому метод на основі U_k –послідовностей пройшов у 1.5 рази більшу кількість тестів, що теж є гарним результатом.

Список літератури

1. Menezes, A.J. Handbook of Applied Cryptography / A.J. Menezes, P.C. van Oorschot, S.A. Vanstone – CRC Press, 2001. – 816 p.
2. Diffie, W. New directions in cryptography / W. Diffie, M.E. Hellman. // IEEE Transactions on Information Theory. – №22, 1976. – Pp. 644–654.
3. Яремчук, Ю.Є. Використання рекурентних послідовностей для побудови криптографічних методів з відкритим ключем / Ю.Є. Яремчук // Захист інформації. – №4, 2012. – С. 120–127.
4. Яремчук, Ю.Є. Метод відкритого розподілу секретних ключів на основі рекурентних послідовностей / Ю.Є. Яремчук // Інформаційна безпека. – №2, 2013. – С. 177–183.
5. NIST SP 800-22 Rev. 1a. A Statistical Test Suite for Random and Pseudorandom Number Generators for Cryptographic Applications / [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.

ИССЛЕДОВАНИИЕ СТАТИСТИЧЕСКОЙ БЕЗОПАСНОСТИ МЕТОДОВ ОТКРЫТОГО РАСПРЕДЕЛЕНИЯ СЕКРЕТНЫХ КЛЮЧЕЙ НА ОСНОВЕ РЕКУРРЕНТНЫХ ПОСЛЕДОВАТЕЛЬНОСТЕЙ

Ю.Е. Яремчук

Винницкий национальный технический университет,
ул. Хмельницкое шоссе, 95, Винница, 21021, Украина; e-mail: yurevyar@vntu.net

Проведены исследования статистической безопасности методов открытого распределения секретных ключей соответственно на основе рекуррентных U_k и V_k –последовательностей и осуществлено их сравнение с известным методом Диффи-Хеллмана. Результаты анализа показали, что наиболее высокий уровень статистической безопасности имеет метод на основе V_k –последовательностей, который прошёл вдвое большее количество тестов по сравнению с методом Диффи-Хеллмана, в то же время метод на основе U_k –последовательностей прошел в 1.5 раза большее количество тестов, чем известный аналог.

Ключевые слова: криптография, распределение секретных ключей, криптостойкость, статистическая безопасность, рекуррентные последовательности.

RESEARCH A STATISTICAL SECURITY METHODS OF PUBLIC DISTRIBUTION OF SECRET KEYS BASED ON RECURRENT SEQUENCES

Yuri E. Yaremchuk

Vinnytsia National Technical University,
95 Khmelnytske shose, Vinnytsia, 21021, Ukraine; e-mail: yurevyar@vntu.net

The research are conducted for statistical security of public distribution of secret keys based on recurrent U_k and V_k sequences and performed their comparison with the known method of Diffie-Hellman. The analysis showed that the highest level of security is a statistical method based on V_k sequences, having twice the number of tests compared with the Diffie-Hellman method, while at the same time, the method based on the U_k sequences was 1.5 times greater number of tests than the known analogue.

Keywords: cryptography, distribution of secret keys, cryptographic reliability, statistical security, recurrent sequences