УДК 681.3.067

МОЖЛИВІСТЬ АВТЕНТИФІКАЦІЇ СТОРІН ВЗАЄМОДІЇ НА ОСНОВІ РЕКУРЕНТНИХ ПОСЛІДОВНОСТЕЙ

Юрій Яремчук

На сьогодні для вирішення задачі забезпечення цілісності широкого використання отримали протоколи автентифікації та цифрового підписування, серед яких важливе місце займають протоколи автентифікації сторін взаємодії, коли здійснюється перевірка однією з сторін того, що взаємодіюча з нею сторона – саме та, за яку себе видає. Існуючи методи автентифікації в основному базуються на операції піднесенні до степеня, яка вимагає виконання досить складних обчислень, що впливає на швидкість роботи методу при його практичній реалізації. В роботі розглянуто можливість побудови методу автентифікації сторін взаємодії на основі математичного апарату рекурентних послідовностей, що базуються на співвідношеннях, в яких початкові елементи пов'язані з коефіцієнтами. Розроблено протокол реалізації методу. Запропонований метод, у порівнянні з відомим аналогом, дозволив підвищити криптографічну стійкість процесу автентифікації, а також можливість змінювати стійкість методу залежно від порядку послідовності. Представленні розробки дали можливість розширити галузь використання методів автентифікації, у першу чергу, в системах захисту з підвищеним рівнем секретності.

***Ключові слова**: захист інформації, криптографія, автентифікація, рекурентні послідовності.*

Вступ. На сьогодні широке застосування сучасних інформаційних технологій та систем електронного документообігу спричинило необхідність забезпечення захисту інформації не лише на рівні держави, але й у комерційній, фінансовій, банківській та інших сферах людської діяльності. При цьому виникає проблема забезпечення цілісності та автентичності даних [2] представлених в електронному вигляді, і ця проблема є не менш актуальною, ніж забезпечення конфіденційності [1–4]. Вирішення задачі автентифікації даних та джерел повідомлень здійснюється за допомогою криптографічних протоколів [1–4, 7, 8, 10], які бувають двох типів – автентифікації та цифрового підписування [1, 8].

В схемі автентифікації учасників взаємодії [1] існує з одного боку претендент – той, хто повинен довести свою автентичність, а з другого боку – перевіряльник – той, хто цю автентичність повинен перевірити. Претендент має два ключа – загальнодоступний K_1 та секретний K_2. При доведенні автентичності з нульовим розголошенням знання претенденту необхідно довести, що він знає K_2, причому зробити це таким чином, щоб це доведення можна було б перевірити знаючи лише K_1.

Теоретичні основи схем автентифікації були закладені в роботі Сіммонса [9]. Найбільш відомими методами автентифікації є методи Фейге-Фіата-Шаміра, Гіллоу-Куіскуотера та Шнорра [1, 3, 4, 8]. Дані методи базуються на операції піднесенні до степеня, яка вимагає виконання досить складних обчислень, що впливає на швидкість роботи методу при його практичній реалізації.

Виходячи з цього, у роботі [6] запропоновано метод автентифікації сторін взаємодії, в основі якого використовується математичний апарат рекурентних V_k^+ та U_k–послідовностей [5], що базуються на співвідношеннях, в яких початкові елементи пов'язані з коефіцієнтами. Суть методу полягає у заміні піднесення до степеня за модулем на обчислення елементу рекурентної U_k–послідовності з певним індексом. Запропонований метод, у порівнянні з відомими аналогами забезпечує значне спрощення обчислень і при цьому забезпечує достатній рівень криптографічної стійкості.

Однак існують задачі, в яких дуже важливим є забезпечення високого рівня стійкості криптографічних перетворень під час автентифікації, причому це може бути навіть більш важливим, ніж підвищення швидкості процесу автентифікації, в першу чергу, це стосується систем захисту з підвищеним рівнем секретності. В цьому зв'язку, метод автентифікації на основі U_k–послідовностей [6], хоч і забезпечує достатній рівень криптографічної стійкості, але має потенційні можливості підвищення стійкості для відповідних систем захисту, оскільки в ньому код автентифікації отримується як елемент U_k - послідовності, обчислений за адитивним, а не мультиплікативним способом зміни індексу, що могло б значно підвищити стійкість цього коду.

Постановка задач досліджень. Розробити метод автентифікації сторін взаємодії підвищеної стійкості на основі математичного апарату рекурентних послідовностей представленого в [5, 6] за рахунок отримання претендентом коду автентифікації у вигляді елементу послідовності, обчисленого за мультиплікативним способом зміни індексу.

Розробка методу автентифікації сторін взаємодії на основі рекурентних послідовностей. Для побудови методу автентифікації сторін взаємодії пропонується використовувати математичний апарат тільки на основі рекурентних V_k^+-послідовностей, що дасть можливість претенденту отримувати код автентифікації як результат обчислень елементу цієї послідовності за мультиплікативним способом зміни індексу.

V_k^+–послідовністю [5] називається послідовність чисел, що обчислюються за формулою

$$v_{n,k} = g_k v_{n-1,k} + g_1 v_{n-k,k} \qquad (1)$$

для початкових значень $v_{0,k} = 1$, $v_{1,k} = g_2$ для $k = 2$; $v_{0,k} = v_{1,k} = ... = v_{k-3,k} = 0$, $v_{k-2,k} = 1,$, $v_{k-1,k} = g_k$ для $k > 2$; де g_1, g_k – цілі числа; n і k – цілі додатні.

Обчислення елементів цієї послідовності для спадних n, починаючи з деякого значення $n = l$, буде здійснюватись таким чином

$$v_{n,k} = \frac{v_{n+k,k} - g_k \cdot v_{n+k-1,k}}{g_1}. \qquad (2)$$

Для будь-яких цілих додатних n, m та k отримано таку аналітичну залежність [5]

$$v_{n+m,k} = v_{m+(k-2),k} \cdot v_{n,k} + g_1 \cdot \sum_{i=1}^{k-1} v_{m+(k-2)-i,k} \cdot v_{n-k+i,k}. \qquad (3)$$

Суть методу автентифікації сторін взаємодії, що пропонується, базується на використанні властивості (3) V_k^+–послідовності, яка забезпечує можливість реалізувати процедури прискореного обчислення елементів V_k^+- послідовності для великих значень індексів, а саме процедури прискореного обчислення елементів $v_{n,k}$ та $v_{n\cdot m,k}$.

Спочатку претендент (або центр довіри) виконує попередню процедуру вибору параметрів та обчислення ключів. Для цього він вибирає і відкрито публікує параметри – ціле додатне число p ($p > 2$) та цілі числа g_1, g_k. Після цього він випадковим чином вибирає секретний ключ a, $1 < a < p$, та обчислює за модулем p і передає перевіряльнику відкритий ключ $v_{a+i,k}$, $i = \overline{-(k-1),0}$. Перевіряльник на своєму боці розширює набір елементів відкритого ключа, обчислюючи за модулем p елементи $v_{a+i,k}$, $i = \overline{1,k-1}$, за формулою (1).

Коли претендент хоче довести свою автентичність, він повідомляє про це перевіряльника, який вибирає випадкове число b, $1 < b < p$, обчислює за модулем p $v_{b+i,k}$, $i = \overline{-(k-1),0}$, і передає ці елементи претенденту. Претендент, прийнявши цей набір елементів, спочатку розширює його, обчислюючи за модулем p елементи $v_{b+i,k}$, $i = \overline{1,k-1}$, за формулою (1), а потім здійснює на основі всього набору елементів $v_{b+i,k} \bmod p$, $i = \overline{-(k-1),k-1}$, обчислення коду автентифікації $v_{b\cdot a,k} \bmod p$, використовуючи свій секретний ключ a, та передає отриманий код автентифікації перевіряльнику. В цей же час перевіряльник обчислює значення $v_{a\cdot b,k} \bmod p$ на основі отриманого ним раніше набору елементів $v_{a+i,k} \bmod p$, $i = \overline{-(k-1),k-1}$, та свого секретного значення b. На завершення, перевіряльник звіряє обчислене значення з отриманим від претендента кодом автентифікації, ідентифікуючи тим самим претендента.

Виходячи з цього схема автентифікації сторін взаємодії за даним методом буде мати вигляд, що представлено на рис. 1.

Операція за модулем в схемі автентифікації використовується для обмеження розрядності чисел під час виконання арифметичних операцій.

Вибір числа b та обчислення за модулем p елементів $v_{b+i,k}$, $i = \overline{-(k-1),0}$, можуть бути виконані перевіряльником попередньо, заздалегідь до безпосередньої автентифікації. Так само попередньо перевіряльник обчислює за модулем p елементи $v_{a+i,k}$, $i = \overline{1,k-1}$, за формулою (1), розширюючи набір елементів відкритого ключа. Можливість попередніх обчислень з боку перевіряльника дає можливість зменшити майже у два рази обчислювальну складність процедури перевірки автентичності безпосередньо під час автентифікації.

В запропонованому методі автентифікації сторін взаємодії основні обчислення виконуються згідно залежності (3). Обчислення елементу $v_{n+m,k}$ згідно цієї залежності здійснюється на основі елементів $v_{n+i,k}$, $i = \overline{-(k-1),0}$, та елементів $v_{m+i,k}$, $i = \overline{-1,k-2}$.

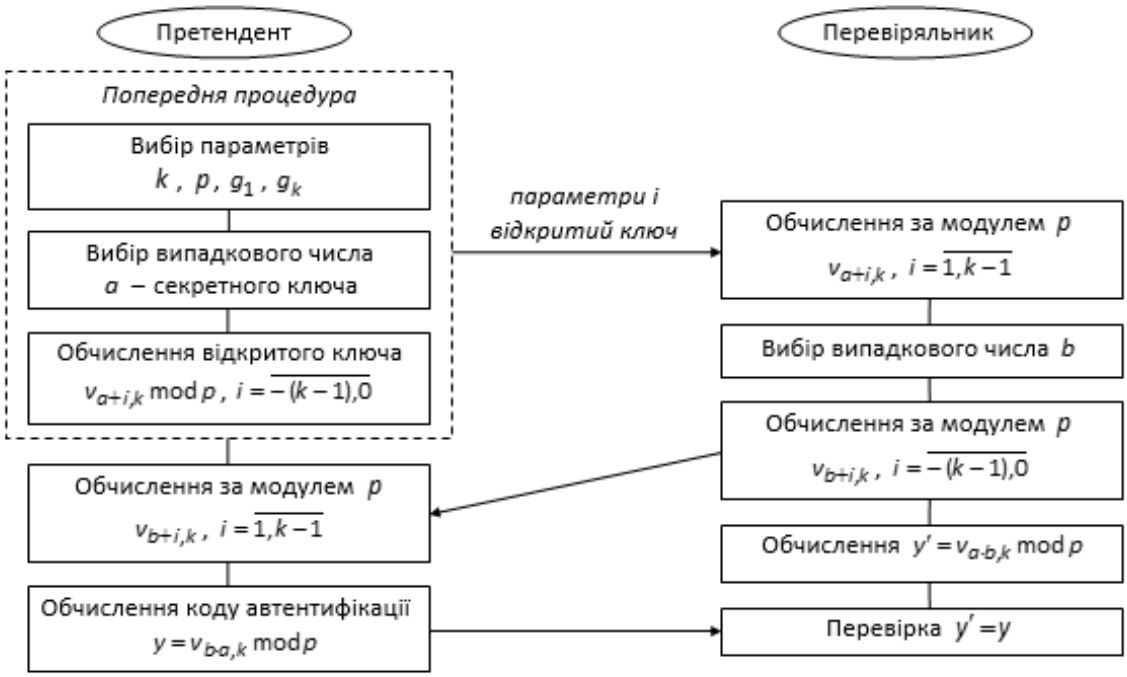

Рис. 1. Схема автентифікації сторін взаємодії на основі елементів V_k^+ –послідовності.

Протокол автентифікації сторін взаємодії згідно запропонованого методу буде мати такий вигляд.

П.1. Задати параметр k.

П.2. Вибрати p, $p > 2$.

П.3. Вибрати g_1, g_k.

П.4. Претенденту передати параметри Перевіряльнику.

П.5. Претенденту як секретний ключ вибрати випадкове число a, $1 < a < p$.

П.6. Претенденту обчислити відкритий ключ за модулем p $v_{a+i,k}$, $i = \overline{-(k-1),0}$, використовуючи спосіб прискореного обчислення елементів $v_{n,k}$ для додатних значень n, та передати його Перевіряльнику.

П.7. Перевіряльнику обчислити за модулем p елементи $v_{a+i,k}$, $i = \overline{1,k-1}$, використовуючи формулу (1).

П.8. Перевіряльнику вибрати випадкове число b, $1 < b < p$.

П.9. Перевіряльнику обчислити за модулем p $v_{b+i,k}$, $i = \overline{-(k-1),0}$, використовуючи спосіб прискореного обчислення елементів $v_{n,k}$ для додатних значень n, і передати ці елементи Претенденту.

П.10. Претенденту обчислити за модулем p елементи $v_{b+i,k}$, $i = \overline{1,k-1}$, використовуючи формулу (1).

П.11. Претенденту обчислити код автентифікації $y = v_{b\cdot a,k} \bmod p$, а Перевіряльнику обчислити значення $y' = v_{a\cdot b,k} \bmod p$, використовуючи спосіб прискореного обчислення елементів $v_{n\cdot m,k}$.

П.12. Претенденту передати код автентифікації y Перевіряльнику.

П.13. Перевіряльнику перевірити обчислене у п.11 значення y' з отриманим кодом автентифікації y, тобто $y' \overset{?}{=} y$.

У п.2 проводиться вибір параметру p, який є модулем при обчисленнях в представленому протоколі та визначає верхню межу діапазону чисел, що отримуються під час цих обчислень.

У п.3 відбувається вибір параметрів g_1, g_k. Оскільки значення будь-якого числа в розробленому протоколі обмежується параметром p, вказані параметри слід вибирати в діапазоні $[1, p-1]$. При цьому вибір можна здійснювати за допомогою будь-якого генератора випадкових чисел у вказаному діапазоні.

В протоколі автентифікації сторін взаємодії претенденту в п.6 необхідно здійснювати обчислення за модулем p елементів $v_{a+i,k}$, $i = \overline{-(k-1),0}$, а перевіряльнику в п.9 – елементів $v_{b+i,k}$, $i = \overline{-(k-1),0}$, причому індекси цих елементів

приймають великі значення. Проблема обчислення елементу $v_{n,k}$ для великих значень n полягає в тому, що обчислення цього елементу за формулою (1) є неприйнятним, тому обчислення елементу $v_{n,k}$ для додатних n може здійснюватись за алгоритмом прискореного обчислення елементів V_k^+–послідовності [5], який реалізовано на основі відомого бінарного методу піднесення до степеня [8].

У п.11 протоколу претенденту необхідно обчислювати значення елементу $v_{b\cdot a,k} \bmod p$, а перевіряльнику – значення елементу $v_{a\cdot b,k} \bmod p$ для великих значень індексів цих елементів. Це можна здійснювати за алгоритмом обчислення елементу $v_{m\cdot n,k}$, який можна реалізувати по аналогії з обчисленням елементу $v_{n,k}$ для додатних n згідно алгоритму прискореного обчислення цих елементів представленого у роботі [5], але починати обчислення не з елементів $v_{1+i,k}$, $i = \overline{-(k-1), k-1}$, а з елементів $v_{m+i,k}$ для тих же значень i.

Порівнюючи запропонований метод автентифікації сторін взаємодії на основі V_k^+–послідовності з методом автентифікації на основі V_k^+ та U_k –послідовностей, представленого в роботі [6], слід відзначити, що запропонований метод на основі V_k^+–послідовності має вищу складність обчислень, однак при цьому він забезпечує вищу криптографічну стійкість процесу автентифікації, оскільки в ньому код автентифікації отримується як результат обчислень елементу $v_{n\cdot m,k}$ V_k^+–послідовності, тобто за мультиплікативним способом зміни індексу, а не за адитивним способом зміни індексу при обчисленні елементу $u_{n+m,k}$ U_k–послідовності, як це робиться згідно методу представленого в роботі [6].

Висновки. На основі математичного апарату рекурентних V_k^+–послідовностей запропоновано метод автентифікації сторін взаємодії, в якому відбувається заміна піднесення до степеня обчисленням елементу рекурентної послідовності з певним індексом. Представлено протокол реалізації методу, а також показано можливість реалізації цього протоколу. Запропонований метод дозволяє змінювати стійкість методу залежно від параметру k –порядку послідовності.

У порівнянні з відомим аналогом на основі V_k^+ та U_k–послідовностей запропонований метод дозволяє підвищити криптографічну стійкість процесу автентифікації, що дає можливість розширення галузі його використання, у першу чергу, в системах захисту з підвищеним рівнем секретності.

ЛІТЕРАТУРА

[1]. Введение в криптографию [Текст] / под общ. ред. В.Б. Ященко. – М.: МЦНМО: «ЧеРо», 2000. – 236 с.

[2]. Основы криптографии [Текст] / А. П. Алферов, А. Ю. Зубов, А. С. Кузьмин, А. В. Черемушкин. – М: Гелиос АРВ, 2001. – 480 с.

[3]. Петров, А. А. Компьютерная безопасность. Криптографические методы защиты [Текст] / А. А. Петров. – М.: ДМК, 2000. – 448 с.

[4]. Романец, Ю. В. Защита информации в компьютерных системах и сетях [Текст] / Ю. В. Романец, П. А. Тимофеева, В. Ф. Шаньгин. – М.: Радио и связь, 2001. – 376 с.

[5]. Яремчук, Ю. Є. Використання рекурентних послідовностей для побудови криптографічних методів з відкритим ключем [Текст] / Ю. Є. Яремчук // Захист інформації. – 2012. – №4. – С. 120–127.

[6]. Яремчук, Ю. Є. Метод автентифікації сторін взаємодії на основі рекурентних послідовностей [Текст] / Ю.Є. Яремчук // Сучасний захист інформації. – 2013. – №1. – С. 4–10.

[7]. Brassard, G. Modern Cryptology: A Tutorial [Текст] / G. Brassard. – Springer-Verlag, 1988. – 107 p.

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

[9]. Simmons, G. J. Authentication theory/coding theory [Текст] / G. J. Simmons // Proc. CRYPTO'84, Lect. Notes in Comput. Sci. – 1985. – V. 196. – Pp. 411-431.

[10]. Van Tilborg, Henk C.A. Fundamentals of cryptology. A Professional Reference and Interactive Tutorial [Текст] / Henk C.A. van Tilborg. – Kluwer Academic Publishers, 2000. – 512 p.

REFERENCES

[1]. Yaschenko, V.B. (ed.) (2000) Introduction to cryptography. Moscow: MCNMO.

[2]. Alferov, A.P. et al. (2001) Cryptography basics. Moscow: Gelios ARV.

[3]. Petrov, A.A. (2000) Computer safety. Cryptographic methods of protection. Moscow: DMK.

[4]. Romanets, Yu.V. and Timofeeva, P.A. Information security in computer systems and networks. Moscow: Radio and Communications.

[5]. Iaremchuk, I.E. (2012). Use of recurrent sequences to construct cryptographic methods with the public key. Information Security, No. 4, pp. 120-127.

[6]. Iaremchuk, I.E. (2013). The method of authentication of parties of interaction based on recurrent sequences. Modern Information Security, No. 1, pp. 4-10.
[7]. Brassard, G. (1988) Modern Cryptology: A Tutorial. Springer-Verlag.
[8]. Menezes, A.J., van Oorschot, P.C., Vanstone, S.A. (2001). Handbook of Applied Cryptography. CRC Press.
[9]. Simmons, G. J. (1985) Authentication theory/coding theory. Proceedings of CRYPTO'84, Lecture Notes in Computer Science, V. 196, pp. 411-431.
[10]. Van Tilborg, Henk C.A. (2000). Fundamentals of cryptology. A Professional Reference and Interactive Tutorial. Kluwer Academic Publishers.

ВОЗМОЖНОСТЬ АУТЕНТИФИКАЦИИ СТОРОН ВЗАИМОДЕЙСТВИЯ НА ОСНОВЕ РЕКУРРЕНТНЫХ ПОСЛЕДОВАТЕЛЬНОСТЕЙ

На сегодня для решения задачи обеспечения целостности широкое использование получили протоколы аутентификации и цифрового подписания, среди которых важное место занимают протоколы аутентификации сторон взаимодействия, когда осуществляется проверка одной из сторон того, что взаимодействующая с ней сторона - именно та, за которую себя выдаёт. Существующие методы аутентификации в основном базируются на операции возведения в степень, которая требует выполнения достаточно сложных вычислений, что влияет на скорость работы метода при его практической реализации. В работе рассмотрена возможность построения метода аутентификации сторон взаимодействия на основе математического аппарата рекуррентных последовательностей, базирующегося на соотношениях, в которых начальные элементы связаны с коэффициентами. Разработан протокол реализации метода. Предложенный метод, по сравнению с известным аналогом, позволил повысить криптографическую стойкость процесса аутентификации, а также возможность изменять стойкость метода в зависимости от порядка последовательности. Представленные разработки дали возможность расширить область использования методов аутентификации, в первую очередь, в системах защиты с повышенным уровнем секретности.

Ключевые слова: защита информации, криптография, аутентификация, рекуррентные последовательности.

POSSIBILITIES FOR AUTHENTICATION OF THE INTERACTION PARTIES BASED ON RECURRENT SEQUENCES

To date, for solving the integrity provision problem of broad utilization, we received protocols of authentication and digital signature. Amongst them, protocols of the parties to interaction hold an important place, when a checkup of the fact that the interacting party is the self-identified party, is conducted by one party. The existing authentication methods are based mainly on operations of exponentiation, requiring implementation of complex calculations, affecting the speed of the method at the stage of its practical implementation. We consider a possibility of creating an authentication method of the interaction parties based on the mathematical apparatus of recurrent sequences, based on the proportions in which the initial elements are associated with the coefficients. We have worked out a protocol implementing the method. The proposed method, compared with the known analogues, allowed to increase the cryptographic reliability of the authentication process, and the ability to change the reliability of the method depending on the sequence order. The presented developments made it possible to expand the use of authentication methods, especially in protection systems with high level of secrecy.

Keywords: information security, cryptography, authentication, recurrent sequence.

Яремчук Юрій Євгенович кандидат технічних наук, доцент, директор Центру інформаційних технологій і захисту інформації, професор кафедри менеджменту та безпеки інформаційних систем, Вінницький національний технічний університет.
E-mail: yurevyar@vntu.net
Яремчук Юрий Евгеньевич кандидат технических наук, доцент, директор Центра информационных технологий и защиты информации, профессор кафедры менеджмента и безопасности информационных систем, Винницкий национальный технический университет.
Iurii Iaremchuk, Ph.D., Director of IT and Information Security Center, Professor Department of Management and Security of Information Systems, Vinnytsia National Technical University.