надійний зв'язок. – М.: Сов. радіо, 1974. – 720 с. 14. Leung-Yan-Cheong S. K. On a Special Class of Wire-tap Channels // IEEE Trans. on Inform. Theory. – Vol. 24. – 1978. – № 4. – P. 268–275.

УДК 621.391.7

АВТЕНТИФІКАЦІЯ НА ОСНОВІ РЕКУРЕНТНИХ ПОСЛІДОВНОСТЕЙ

Юрій Яремчук
Вінницький державний технічний університет

Анотація: **Пропонується метод автентифікації, в основі якого лежить використання властивостей класу рекурентних послідовностей, для обчислення елементів яких використовуються рекурентні співвідношення з коефіцієнтами, що пов'язані з початковими елементами послідовностей.**
Summary: **The method of authentication is offered, in which base use of properties of the class recurrent of sequences lays, at calculation of which elements the recurrences with coefficients coupled to initial elements of sequences are used.**
Ключові слова: **Захист інформації, криптографія, автентифікація, рекурентні послідовності.**

I Вступ

В сучасному світі поняття "інформація" відіграє важливу роль. У різних своїх формах та проявах інформація стала товаром, який створюється, зберігається та передається користувачам, споживачам. Кожна інформація має свою ціну, а отже може продаватися та купуватися, старіти та пошкоджуватися і т. і. Найпоширенішими на сьогодні засобами для зберігання, обробки та передавання інформації є комп'ютерні системи, в яких інформація представляється в цифровому вигляді. Протягом всього циклу існування інформації однією з основних проблем для споживача є проблема її захисту від небажаного втручання та впливу з боку зловмисника. Для вирішення цієї проблеми в комп'ютерних системах застосовують криптографічні методи захисту інформації [1].

Історично криптографія виникла як наука про шифрування інформації, тобто як наука про криптосистеми [2]. В класичній шенонівській моделі [3] системи секретного зв'язку мають двох учасників, які повністю довіряють один одному і передають між собою інформацію, що не призначена для сторонніх осіб. Таку інформацію називають секретною або конфіденційною, а задачу, яка тут виникає, називають задачею забезпечення конфіденційності або секретності від зовнішнього противника [3]. Традиційно ця задача розв'язується за допомогою криптосистем.

Швидкі темпи розвитку засобів зв'язку та комп'ютерних мереж привели до широкого впровадження електронних банківських платежів та можливості обміну різного роду електронними документами. В зв'язку з цим у споживача можуть виникнути обґрунтовані сумніви відносно того, що отримана ним інформація створена потрібним джерелом, причому в такому вигляді, в якому вона дійшла до нього. Тобто необхідна гарантія того, що повідомлення надійшло з достовірного джерела та в неперекрученому вигляді. Така гарантія отримала назву забезпечення цілісності інформації [4] і складає другу задачу криптографії.

Якщо задача конфіденційності вирішується за допомогою криптосистем, то для забезпечення цілісності інформації розробляються криптографічні протоколи [2]. Найбільш розповсюдженими є два типи криптографічних протоколів: схеми автентифікації та цифрового підпису [4].

Схеми автентифікації використовуються для встановлення авторства (або ідентифікації). На цей час актуальність задачі автентифікації має не менше, а в деяких випадках і більше, значення, ніж задача конфіденційності інформації.

II Постановка задачі

В загальному вигляді в схемі автентифікації [2] існує два учасника. Передавач, який має довести свою автентичність, та Приймач, який цю автентичність має перевірити. Передавач має два ключа – загальнодоступний K_1 та секретний K_2. Передавачу необхідно довести, що він знає K_2, причому зробити це таким чином, щоб це доведення можна було б перевірити, знаючи лише K_1.

Найбільш відомими методами автентифікації з точки зору встановлення авторства повідомлення є методи Фейге-Фіата-Шаміра, Гіллу-Кіскатра та Шнорра [2]. Ці методи базуються на операції піднесення до степеня, яка вимагає виконання досить складних обчислень, що впливає на швидкість роботи методу при його

практичній реалізації. Крім того, в цих методах, окрім передавання параметрів та відкритого ключа, необхідно виконувати триетапне передавання інформації, що також створює певні труднощі.
Далі пропонується метод автентифікації, який в певній мірі усуває вказані труднощі.

III Рекурентні V_k та U_k –послідовності

В роботах [5, 6] запропоновані такі рекурентні послідовності:

V_k^+ – послідовність чисел, що обчислюються за формулою

$$v_{n,k} = g_k v_{n-1,k} + g_1 v_{n-k,k}; \tag{1}$$

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

V_k^- – послідовність чисел, що обчислюються за формулою

$$v_{n,k} = \frac{v_{n+k,k} - g_k \cdot v_{n+k-1,k}}{g_1}, \tag{2}$$

для n – від'ємних з початковими значеннями $v_{-1,k} = 0$, $v_{-2,k} = g_1^{-1}$ для $k = 2$; $v_{-1,k} = 0$, $v_{-2,k} = g_1^{-1}$, $v_{-3,k} = v_{-4,k} = \ldots = v_{-k,k} = 0$ для $k > 2$;

V_k – послідовність чисел, яка складається з V_k^+ –послідовності та V_k^- –послідовності;

U_k – послідовність чисел, що обчислюються за формулою

$$u_{n,k} = g_k u_{n-1,k} + g_1 u_{n-k,k}, \tag{3}$$

для початкових значень $u_{0,k} = g_1$, $u_{1,k} = g_2$, $u_{2,k} = g_3$, ... $u_{k-1,k} = g_k$; де g_1, g_2, g_3, ..., g_k – цілі числа; n і k – цілі додатні числа.

Для будь-яких цілих додатних n, m та k отримана така властивість

$$u_{n+m,k} = v_{m+(k-2),k} \cdot u_{n,k} + g_1 \cdot \sum_{i=1}^{k-1} v_{m+(k-2)-i,k} \cdot u_{n-k+i,k}. \tag{4}$$

Для будь-яких цілих додатних n та k, таких що $n \geq k$, отримана властивість, яка дозволяє обчислювати елементи U_k – послідовності тільки на основі елементів V_k^+ – послідовності

$$u_{n,k} = g_k \cdot v_{n-1,k} + g_1 \cdot \sum_{i=1}^{k-1} g_i \cdot v_{n-i-1,k}. \tag{5}$$

IV Метод автентифікації

Суть методу автентифікації, що буде розглянуто, базується на властивості (4), яка дозволяє обчислити елемент $u_{n+m,k}$ двома шляхами: або використовуючи елементи $v_{m+i,k}$, $i = \overline{-1, k-2}$, та $u_{n-i,k}$, $i = \overline{0, k-1}$, або використовуючи елементи $v_{n+i,k}$, $i = \overline{-1, k-2}$, та $u_{m-i,k}$, $i = \overline{0, k-1}$. Це дає можливість створення такого методу автентифікації.

Спочатку Передавач виконує попередню процедуру обчислення ключів. Для цього він випадковим чином вибирає секретний ключ a, після чого обчислює і публікує відкритий ключ $u_{a-i,k}$, $i = \overline{0, k-1}$.

Коли Приймач бажає перевірити автентичність Передавача, він вибирає випадкове число b, обчислює $u_{b-i,k}$, $i = \overline{0, k-1}$ і передає отриманий набір елементів Передавачу. Передавач, прийнявши цей набір елементів, здійснює на їх основі обчислення $u_{a+b,k}$. В цей же час Приймач обчислює $u_{b+a,k}$. Потім

Передавач передає отримане значення $u_{a+b,k}$ Приймачу, який звіряє його зі значенням $u_{b+a,k}$, ідентифікуючи таким чином Передавача.

Схема автентифікації за даним методом представлена на рис. 1.

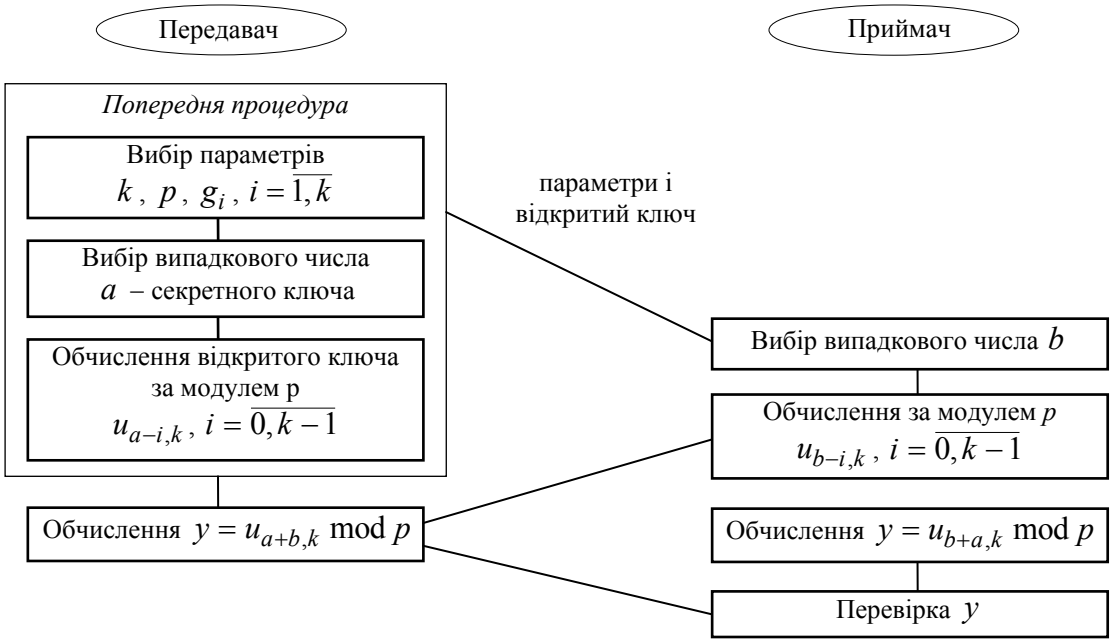

Рисунок 1 – Схема автентифікації на основі елементів U_k –послідовності

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

Відповідно до запропонованого методу автентифікації основні обчислення виконуються за формулою (4). Для обчислення елементу $u_{n+m,k}$ за цією формулою потрібні елементи $v_{m+i,k}$, $i = \overline{-1,k-2}$, та елементи $u_{n-i,k}$, $i = \overline{0,k-1}$. Обчислення останнього набору елементів здійснюється за формулою (5), для чого необхідно мати елементи $v_{n+i,k}$, $i = \overline{-2k+1,-1}$. Звідси виходить, що всього для обчислення елементу $u_{n+m,k}$ за формулою (4) потрібно мати елементи $v_{n+i,k}$, $i = \overline{-2k+1,k-2}$ V_k –послідовності. Для отримання останнього набору елементів достатньо обчислити будь-які k послідовних елементів з цього набору, оскільки інші можуть бути обчислені на їх основі за формулами (1) або (2).

Визначивши обчислення за усіма формулами, що використовуються в методі автентифікації, отримаємо такий алгоритм автентифікації.

Алгоритм 1.

П. 1. Задати параметр k.

П. 2. Вибрати p.

П. 3. Вибрати $g_1, g_2, \ldots, g_k$.

П. 4. Опублікувати параметри.

П. 5. Передавачу вибрати випадкове число a – секретний ключ.

П. 6. Передавачу обчислити за модулем p $v_{a+i,k}$, $i = \overline{-(k-1),k-2}$.

П. 7. Передавачу обчислити за модулем p $v_{a+i,k}$, $i = \overline{-2k+1,-k}$, за формулою (2).

П. 8. Передавачу обчислити відкритий ключ за модулем p $u_{a-i,k}$, $i = \overline{0,k-1}$, за формулою (5).

П. 9. Передавачу опублікувати відкритий ключ.

П. 10. Приймачу вибрати випадкове число b.

П. 11 Приймачу обчислити за модулем p $v_{b+i,k}$, $i = \overline{-(k-1), k-2}$.

П. 12. Приймачу обчислити за модулем p $v_{b+i,k}$, $i = \overline{-2k+1, -k}$, за формулою (2).

П. 13. Приймачу обчислити за модулем p $u_{b-i,k}$, $i = \overline{0, k-1}$, за формулою (5).

П. 14. Приймачу передати Передавачу обчислені за модулем p $u_{b-i,k}$, $i = \overline{0, k-1}$.

П. 15. Передавачу обчислити $y = u_{b+a,k} \bmod p$, а Приймачу $y = u_{a+b,k} \bmod p$ за формулою (4).

П. 16. Передавачу передати значення y Приймачу.

П. 17. Приймачу звірити отримане від Передавача значення y з тим значенням, що він обчислив в п. 15.

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

В п. 3 відбувається вибір параметрів g_i, $i = \overline{1, k}$. Оскільки значення будь-якого числа в розробленому алгоритмі обмежується параметром p, вказані параметри слід вибирати в діапазоні $[1, p-1]$. При цьому вибір можна здійснювати у вказаному діапазоні за допомогою будь-якого генератора випадкових чисел.

V Оцінка складності виконання алгоритму автентифікації

Не важко помітити, що Передавач і Приймач виконують за алгоритмом 1 однакову кількість арифметичних операцій над великими числами. Тому для визначення складності обчислень за цим алгоритмом достатньо визначити складність обчислення з боку одного з них, а потім подвоїти отримане значення.

Складність обчислень за алгоритмом 1 з боку Передавача визначається складністю обчислень за модулем p елементів $v_{a+i,k}$, $i = \overline{-(k-1), k-2}$, елементів $v_{a+i,k}$, $i = \overline{-2k+1, -k}$ за формулою (2), елементів $u_{a-i,k}$, $i = \overline{0, k-1}$ за формулою (5), та елементу $u_{b+a,k}$ за формулою (4). Обчислення першого набору елементів може бути здійснено за методом обчислення елементів V_k – послідовності з розкладанням індексу, який представлений в роботі [7]. В тій же роботі визначено, що складність обчислень даного набору елементів складає приблизно $H^2 q \cdot [6H(k^2 + k) + 3(3k^2 + k)]$ операцій над машинними одиницями інформації, де H – кількість машинних одиниць інформації для зберігання великого числа, q – кількість розрядів машинної одиниці інформації.

Обчислення інших елементів V_k та U_k –послідовностей за модулем p за формулами (2), (4) та (5) потребує виконання приблизно $k^2 + 4k$ множень, k^2 додавань та k віднімань над машинними одиницями інформації. Враховуючи оцінки складності виконання арифметичних операцій за модулем над числами великої розрядності, що представлені в [7], складність обчислень за формулами (2), (4) та (5) буде складати приблизно $6H(H+1)(k^2 + 4k) + 2Hk^2(H+1) + 3Hk(H+1)$ операцій над машинними одиницями інформації. Виходячи з того, що при реалізації криптографічних методів в сучасних комп'ютерних системах оперують ключами, що мають розмір 1024 і більше розрядів ($Hq \geq 1024$), отримана оцінка буде значно меншою за оцінку складності обчислення набору елементів $v_{a+i,k}$, $i = \overline{-(k-1), k-2}$, а тому може не враховуватись в загальній оцінці складності всього алгоритму автентифікації.

Таким чином складність виконання запропонованого алгоритму автентифікації з боку Передавача або Приймача складає $H^2 q \cdot [6H(k^2 + k) + 3(3k^2 + k)]$ операцій над машинними одиницями інформації.

Порівнюючи запропонований метод автентифікації з відомими методами Фейге-Фіата-Шаміра, Гіллу-Кіскатра та Шнорра відносно складності виконання автентифікації слід відзначити таке. В запропонованому методі Передавачу і Приймачу необхідно виконувати обчислення певного елементу U_k –послідовності по одному разу, в той час як за відомими методами їм необхідно виконувати піднесення до степеня по два рази. В [7] показано, що складність обчислення певного елементу U_k –послідовності має той же порядок, що і складність піднесення до заданого степеня. Тому можна стверджувати, що представлений метод має

приблизно вдвічі меншу складність обчислень, ніж відомі методи автентифікації. Крім того запропонований метод має значно простішу процедуру завдання параметрів, оскільки їх вибір не потребує проведення складних обчислень над великими числами.

Слід також відмітити те, що у відомих методах автентифікації, крім передавання параметрів, необхідно виконувати три передавання інформації: два від Передавача до Приймача і одне від Приймача до Передавача, в той час як за представленим методом достатнім є лише два передавання: по одному з кожного боку.

VI Криптостійкість методу автентифікації

Визначимо теоретичну криптостійкість запропонованого методу автентифікації за допомогою теоретико-складносного підходу. Для цього зазначимо, по-перше, що запропонований метод використовує фіксовані значення параметрів k, q, H, наприклад $k = 3$, $q = 16$, $H = 32$, а параметр безпеки – будь-яке натуральне число. По-друге, будемо вважати, що противнику відома така інформація: алгоритм автентифікації; параметри алгоритму k, p, g_i, $i = \overline{1,k}$; відкритий ключ $u_{a-i,k} \bmod p$, $i = \overline{0,k-1}$; вся інформація, що передається від Передавача до Приймача та навпаки в процесі автентифікації, тобто $u_{b-i,k} \bmod p$, $i = \overline{0,k-1}$, та $u_{a+b,k} \bmod p$. По-третє, об'єм обчислень будемо вважати "практично нездійсненим", якщо найкращий алгоритм, який буде використовувати противник для зламу, буде виконуватись не за поліноміальний час. Доведемо, що не існує поліноміальних алгоритмів для зламу запропонованого методу.

Перше, що може спробувати противник, – отримати секретний ключ a шляхом послідовних обчислень за модулем p за формулою (3), доки не буде отримано значення $u_{a,k} \bmod p$. Аналіз показує, що такі обчислення потребують виконання $3aH(4H+5)$ операцій над машинними одиницями інформації. Тобто, якщо продуктивність комп'ютера дорівнює 2^{34} операцій за секунду, для представлення a використовують 1024 розряди, $H = 32$, то для виконання цих операцій потрібно приблизно 2^{979} років, що є практично нездійсненим.

Для отримання значення $u_{a,k} \bmod p$ або набору елементів $v_{a+i,k}$, $i = \overline{-(k-1),k-2}$, противник може застосовувати формули безпосереднього обчислення елементів відповідно U_k або V_k –послідовностей через початкові елементи. Такі формули наведені відповідно в роботах [6] та [5]. Аналіз цих формул показує, що вони є більш складними за кількістю виконуваних операцій, ніж формула (3), тобто дана спроба теж є практично нездійсненною.

Оскільки елементи $u_{a-i,k} \bmod p$, $i = \overline{0,k-1}$, відомі, то можлива спроба знаходження елементів $v_{a+i,k}$, $i = \overline{-(k-1),k-2}$, використовуючи формулу (5). Реалізація цієї спроби зводиться до розв'язання системи з k рівнянь з $k+1$ невідомими. Математична задача розв'язання такої системи рівнянь, враховуючи велику розрядність коефіцієнтів та невідомих, на цей день не має ефективного поліноміального алгоритму, а отже є практично нездійсненою.

Проведений аналіз криптостійкості показує, що запропонований метод автентифікації теоретично є криптостійким.

VII Висновки

Запропоновано метод автентифікації, який базується на властивостях рекурентних V_k та U_k –послідовностей. В порівнянні з відомими методами Фейге-Фіата-Шаміра, Гіллу-Кіскатра та Шнорра цей метод має простішу процедуру завдання параметрів та приблизно вдвічі меншу складність обчислень. Крім того, у відомих методах, окрім передавання параметрів, безпосередньо під час автентифікації необхідно виконувати три етапи передавання інформації, в той час як у представленому методі лише два. Запропонований метод з точки зору теоретичної криптостійкості є стійким.

Література: 1. Жельников В. Криптография от папируса до компьютера. М.: ABF, 1997.– 335 с. 2. Manazes A., van Oorschot, S. Vanstone. Handbook of Applied Cryptography.– CRC Press, 1996.– 782 p. 3. Shannon C. E. Communication Theory of Secrecy Systems // Bell System Tech. Jour.– 1949.– V. 28. № 11. 4. Симмонс Г.

Дж. Обзор методов аутентификации информации // ТИИЭР. Т. 76.– 1988.– № 5.– С. 105–125. 5. Лужецький В. А., Яремчук Ю. Є. Рекурентні V_k –послідовності // Вісник ВПІ.– 1999.– № 6.– С. 53–59. 6. Лужецький В. А., Яремчук Ю. Є. Про один клас рекурентних послідовностей // Наукові праці Донецького державного технічного університету. Серія "Проблеми моделювання та автоматизації проектування динамічних систем".– 1999.– № 10.– С. 62–70. 7. Яремчук Ю. Є. Методи та засоби шифрування інформації на основі рекурентних послідовностей.– Дис. ... канд. техн. наук: 05.13.21 – К., 2000.– 179 с.

УДК 681.3.06

СРЕДСТВА ЗАЩИТЫ ИНФОРМАЦИИ ОТ НЕСАНКЦИОНИРОВАННОГО ДОСТУПА СЕМЕЙСТВА "ГРИФ"

Виктор Кондратюк, Дмитрий Корниенко
ООО «Институт компьютерных технологий»

Анотація: **Надано загальний опис можливостей комплексів засобів захисту від НСД родини "Гриф". Розглянуто проблеми оцінки таких комплексів на відповідність вимогам діючих в Україні критеріїв.**
Summary: **The brief description of functionality of unauthorized access protection systems from "Grif" family is given. Problems of such systems evaluation according to the Ukrainian criteria are discussed.**
Ключові слова: **Несанкціонований доступ, комплекс засобів захисту, критерії оцінки, криптографічний захист, централізоване керування.**

В статье рассмотрено две группы вопросов: во-первых, принципиальные отличительные функциональные характеристики прошедшей экспертную оценку первой версии комплекса средств защиты от несанкционированного доступа (КСЗ от НСД) "Гриф", которые выделяют его среди других аналогичных имеющихся на рынке систем; во-вторых, особенности второй версии КСЗ с централизованным удаленным администрированием. Ниже как синоним термина КСЗ иногда употребляется термин "система защиты".

Итак, краткая характеристика. Комплекс средств защиты от НСД "Гриф" предназначен для защиты обрабатываемой на ПЭВМ информации от несанкционированного ознакомления, модификации, удаления. КСЗ "Гриф" служит специализированной надстройкой над стандартной операционной системой (ОС) MS Windows 95/98 и дополняет ее функциями разграничения доступа. Комплекс позволяет создать защищенное автоматизированное рабочее место с ограниченным кругом пользователей, обладающих различными полномочиями по доступу к ресурсам.

Согласно выданному Департаментом специальных телекоммуникационных систем и защиты информации Службы безопасности Украины экспертному заключению (№ 10 от 18. 07. 2001 г.) совокупность реализованных в комплексе "Гриф" функций и механизмов защиты информации обеспечивает уровень защищенности информации, достаточный для обработки информации, составляющей государственную тайну.

КСЗ "Гриф" реализует следующие функции:

- *идентификацию и аутентификацию пользователей* при загрузке ПЭВМ до загрузки каких-либо программных средств с дисков на основании вводимого пароля и носимого идентификатора;
- *блокировку загрузки ОС с гибкого диска и CD-ROM*;
- *разграничение доступа пользователей к выбранным каталогам* и находящимся в них файлам;
- *управление потоками информации* и блокировку потоков информации, приводящих к снижению ее конфиденциальности;
- *гарантированное удаление конфиденциальной информации* путем затирания содержимого файлов при их удалении;
- *контроль за выводом информации на печать*;
- *контроль целостности прикладного программного обеспечения (ПО) и ПО КСЗ*, а также блокировку загрузки посторонних (незарегистрированных) программ и программ, целостность которых нарушена;
- *блокировку устройств интерфейса пользователя* (гашение экрана и блокировку клавиатуры и мыши) по выбранной комбинации клавиш или после определенного периода бездействия пользователя;