- радиогерметизирующим уплотнителям из различных материалов;
- исключению взаимного влияния ЭМИ устройств ПК.

На основании вышеизложенного разрабатываются технические требования по защите информации в конкретном составе ПК. Практика выполненных опытно-конструкторских работ показала, что реализация таких конструкторско-технологических решений удовлетворяет техническим требованиям и нормативной документации по предотвращению утечки информации.

В рамках настоящей статьи не представляется возможным представить в полном объёме работы, выполняемые ООО «ЕПОС» по обеспечению безопасности информации. Приведём только направления, по которым проводятся научно-исследовательские и опытно-конструкторские работы (НИОКР):

- предотвращение утечки информации в цепях электропитания и заземления;
- защита от НСД к ПК;
- защита от НСД к информационным ресурсам ПК;
- восстановление и стирание информации на НЖМД;
- обеспечение безопасности информации в сетях.

В заключение необходимо отметить, что желание обеспечить высокоэффективную систему безопасности информации вполне оправдано, но это требует значительных финансовых затрат. Вместе с тем чрезмерные затраты на защиту не всегда адекватны гарантированной степени надежности защиты. Чтобы избежать «саморазорения» от чрезмерных затрат на обеспечение безопасности информации следует придерживаться принципа необходимой достаточности, т.е. стоимость защиты не должна превышать риска ущерба от негативного воздействия на информационные ресурсы.

Список литературы:

1. Волеводз А.Г. Проект Европейской Конвенции о киберпреступности, «Конфидент» №5, №6, 2001г.
2. Гриняев С.Н. Национальная информационная стратегия как основа внешней и внутренней политики США в XXI веке, «Конфидент» №5, №6, 2001г.
3. www.pole.ru/spk.htm
4. Бурлаков Г.Н. «Безопасность работы на компьютере» М.: «Финансы и стастика» 1998г.

Ключевые слова:
Информационная безопасность, каналы утечки информации, методы предотвращения утечки информации, типовые конструкторско-технологические решения.

Поступила 10.01.2002

УДК 621.391.7

Яремчук Ю.Є.

ВИКОРИСТАННЯ РЕКУРЕНТНИХ ПОСЛІДОВНОСТЕЙ В ЗАДАЧАХ КРИПТОГРАФІЧНОГО ЗАХИСТУ ІНФОРМАЦІЇ

Вступ

Існує багато методів та засобів забезпечення безпеки інформації. Криптографічні методи [1] застосовуються для вирішення проблем захисту інформації в комп'ютерних системах. Історично криптографія виникла як наука про шифрування інформації [2],

оскільки в класичній моделі Шенона [3] обидва учасники зв'язку 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].

Розрізняють методи шифрування з секретним та відкритим ключем [1, 2]. Основними перевагами методів з секретним ключем є те, що при шифруванні вони використовують більш короткий ключ та мають при апаратній реалізації на декілька порядків більшу швидкість шифрування. Однак, слабким місцем при їх практичній реалізації є необхідність вирішення задачі розповсюдження секретних ключів. В цьому зв'язку методи шифрування з відкритим ключем мають суттєву перевагу, оскільки при такому шифруванні відкритий ключ публікується і доступний будь-кому, хто бажає послати повідомлення адресату.

Розвиток комп'ютерних систем та мереж призвів до широкого впровадження електронних банківських платежів та обігу різного роду електронних документів. В зв'язку з цим у споживача виникають обгрунтовані сумніви відносно того, що отримана ним інформація створена потрібним джерелом, причому в такому вигляді, в якому вона дійшла до нього. Тобто необхідна гарантія, що повідомлення надійшло з достовірного джерела та в неперекрученому вигляді. Така гарантія отримала назву забезпечення цілісності інформації [2] і складає другу задачу криптографії.

Якщо задача конфіденційності вирішується за допомогою криптосистем, то для забезпечення цілісності інформації розробляються криптографічні протоколи [2]. Розрізняють криптографічні протоколи аутентифікації та цифрового підпису [2]. Протоколи аутентифікації використовуються для встановлення авторства (або ідентифікації), а протоколи цифрового підпису забезпечують аутентифікацію повідомлень, тобто гарантують, що повідомлення прийшло від достовірного відправника та в неперекрученому вигляді.

Стійкість більшості відомих методів криптографічного захисту до зламу базується на великій складності розв'язання певних математичних задач, найбільш відомими з яких є задачі розкладання великого числа на прості множники та дискретного піднесення до степеня великого числа. Однак, при практичній реалізації методів криптографічного захисту виникає проблема виконання складних обчислень над числами великої розрядності, що нерозривно пов'язує ці методи з високим рівнем обчислювальної техніки.

Виходячи з вищесказаного, актуальними є дослідження, що спрямовані на спрощення обчислень та підвищення криптостійкості методів криптографічного захисту. В зв'язку з цим інтерес викликають нетрадиційні підходи до вирішення цієї проблеми. Одним з таких підходів є підхід, що базується на використанні рекурентних послідовностей.

Так, в роботах [4, 5] представлені модифікації відомих методів криптографічного захисту інформації, а саме шифрування інформації з відкритим ключем (метод LUCRSA), розповсюдження секретних ключів (метод LUCDIF) та цифрового підпису (метод LUCELG). В цих методах дискретне піднесення до степеня замінюється обчисленням елементів узагальненої рекурентної послідовності Люка. Запропонований рекурентний підхід забезпечує спрощення обчислень, однак в роботах [6, 7] було показано, що даний підхід забезпечує не достатньо високий рівень криптостійкості для деяких застосувань.

Метою даної роботи є усунення вказаного недоліку шляхом використання спеціального класу рекурентних послідовностей

Рекурентні V_k та U_k-послідовності

Рекурентні послідовності в загальному вигляді породжується таким співвідношенням [8]

$$u_n = a_1 \cdot u_{n-1} + a_2 \cdot u_{n-2} + \ldots + a_k \cdot u_{n-k},$$

де $a_1, a_2, \ldots, a_k$ – коефіцієнти,

k – порядок послідовності,

виходячи з початкових елементів $u_0, u_1, \ldots, u_{k-1}$.

Складність обчислення елементів такої послідовності залежить від кількості ненульових коефіцієнтів a_1, a_2, ... , a_k та від порядку k рекурентного співвідношення.

Відомими прикладами вказаної послідовності є послідовність Фібоначчі [9] та послідовність Хорадама [10]. В усіх цих послідовностях початкові елементи – довільні числа, які не пов'язані з коефіцієнтами.

Запропоновані в [4, 5] узагальнені послідовності Люка відносяться до класу послідовностей, в яких початкові елементи пов'язані з коефіцієнтами. Найпростішим прикладом такого класу послідовностей є послідовність, елементи якої обчислюються за формулою:

$$u_n = a_1 \cdot u_{n-1}.$$

Якщо $u_1 = q$, $a_1 = q$, то $u_n = q^n$. Тобто, в цьому випадку, рекурентне співвідношення породжує послідовність степенів числа q.

Наступним за складністю є випадок, коли два коефіцієнти відрізняються від нуля. В цьому випадку елементи послідовності обчислюються за такою формулою:

$$u_n = a_1 \cdot u_{n-1} + a_k \cdot u_{n-k}.$$

Послідовності Люка, що лежать в основі представлених в [4, 5] модифікованих методів шифрування інформації, породжуються таким співвідношенням

$$u_n = a \cdot u_{n-1} - u_{n-2},$$

виходячи з початкових елементів $u_0 = 2$, $u_1 = a$.

Очевидно, що ці послідовності є лише окремим випадком більш узагальнених рекурентних послідовностей.

В роботах [11, 12] запропоновані та досліджені рекурентні послідовності, які є більш узагальненими, ніж послідовності Люка.

Запропоновані такі рекурентні послідовності

– V_k^+–послідовність – 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 $k = 2$; $v_{0,k} = v_{1,k} = \ldots = v_{k-3,k} = 0$, $v_{k-2,k} = 1$, $v_{k-1,k} = g_k$ для $k > 2$; де g_1, g_k – цілі числа; n і k – цілі додатні;

– V_k^-–послідовність – послідовність чисел, що обчислюються за формулою

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

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

– U_k–послідовність – послідовність чисел, що обчислюються за формулою

$$u_{n,k} = g_k u_{n-1,k} + g_1 u_{n-k,k} \qquad (3)$$

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

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

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

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

Виходячи з формули (3) вираз для обчислення елементів $u_{n,k}$ для спадних n, починаючи з деякого $n = l$, має такий вигляд

$$u_{n,k} = \frac{u_{n+k,k} - g_k u_{n+k-1,k}}{g_1} . \qquad (6)$$

Для будь-яких цілих додатних n і m, таких що $1 \leq m < n$ та будь-якого цілого додатного k має місце така формула

$$u_{n-m,k} = v_{-m+(k-2),k} \cdot u_{n,k} + g_1 \cdot \sum_{i=1}^{k-1} v_{-m+(k-2)-i,k} \cdot u_{n-k+i,k} . \qquad (7)$$

Метод розповсюдження секретних ключів на основі U_k □послідовності

Задача розповсюдження секретних ключів може бути розв'язана на основі властивості (4), яка дозволяє обчислити елемент $u_{n+m,k}$, використовуючи елементи V_k^+ та U_k –послідовностей, причому елемент $u_{n+m,k}$ може бути обчислений 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 $u_{m-i,k}$, $i = \overline{0, k-1}$.

Тоді, якщо один користувач для будь-якого вибраного їм випадкового числа a обчислить $u_{a-i,k}$, $i = \overline{0, k-1}$, а другий користувач аналогічним чином обчислить $u_{b-i,k}$, $i = \overline{0, k-1}$, то, обмінявшись обчисленими значеннями, кожен з них зможе отримати $u_{a+b,k}$, продовжуючи обчислення на свому боці за формулою (4), використовуючи відповідно свої числа a або b. В цьому випадку $u_{a+b,k}$ буде ключем обміну, а числа a і b секретним ключем кожного користувача. Причому, a і b - це частини секретного ключа кожного користувача, оскільки попереднє отримання ключа обміну будь-яким користувачем не можливе без отримання відповідної інформації від іншого користувача.

Виходячи з цього процедура обміну ключами має вигляд, представлений на рис.1.

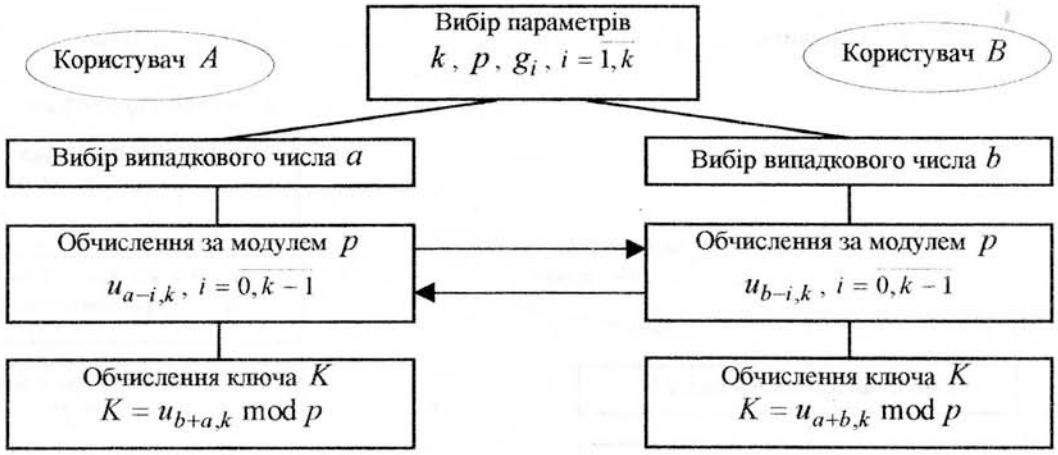

Рис. 1. Схема розповсюдження ключів на основі елементів U_k – послідовностей

Дослідження представленого методу розповсюдження ключів показало, що з точки зору теоретичної криптостійкості метод є стійким, і в той же час, з точки зору складності обчислень, в порівнянні з відомим методом ключового обміну Діффі-Хеллмана запропонований метод забезпечує для кожного користувача майже вдвічі меншу складність обчислень.

Метод шифрування інформації на основі U_k □послідовності

В задачі шифрування інформації в системах з відкритим ключем одностороння функція може бути побудована на основі властивості (4), оскільки обчислити елемент $u_{n+m,k}$, знаючи елементи $u_{n-i,k}$ або $u_{m-i,k}$ для $i = \overline{0,k-1}$ без знання відповідно m або n є практично неможливим для великих значень n. Крім того, як вже було відмічено вище, елемент $u_{n+m,k}$ за формулою (4) може бути обчислений 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 $u_{m-i,k}$, $i = \overline{0,k-1}$.

Використовуючи вищенаведене маємо такий метод шифрування. Приймач випадковим чином вибирає секретний ключ a і обчислює відкритий ключ $u_{a-i,k}$, $i = \overline{0,k-1}$, який передає Передавачу.

Передавач спочатку вибирає випадкове число b та обчислює $u_{b-i,k}$, $i = \overline{0,k-1}$. Потім він обчислює $u_{a+b,k}$ за формулою (6) і отримує зашифроване повідомлення y_2 як результат виключного АБО $u_{a+b,k}$ з відкритим повідомленням M.

Отримавши від Передавача $u_{b-i,k}$, $i = \overline{0,k-1}$ та y_2 Приймач спочатку за допомогою свого секретного ключа a обчислює $u_{b+a,k}$, а потім дешифрує відкрите повідомлення, як результат виключного АБО $u_{b+a,k}$ з y_2.

Процедура шифрування даних представлена на рис.2.

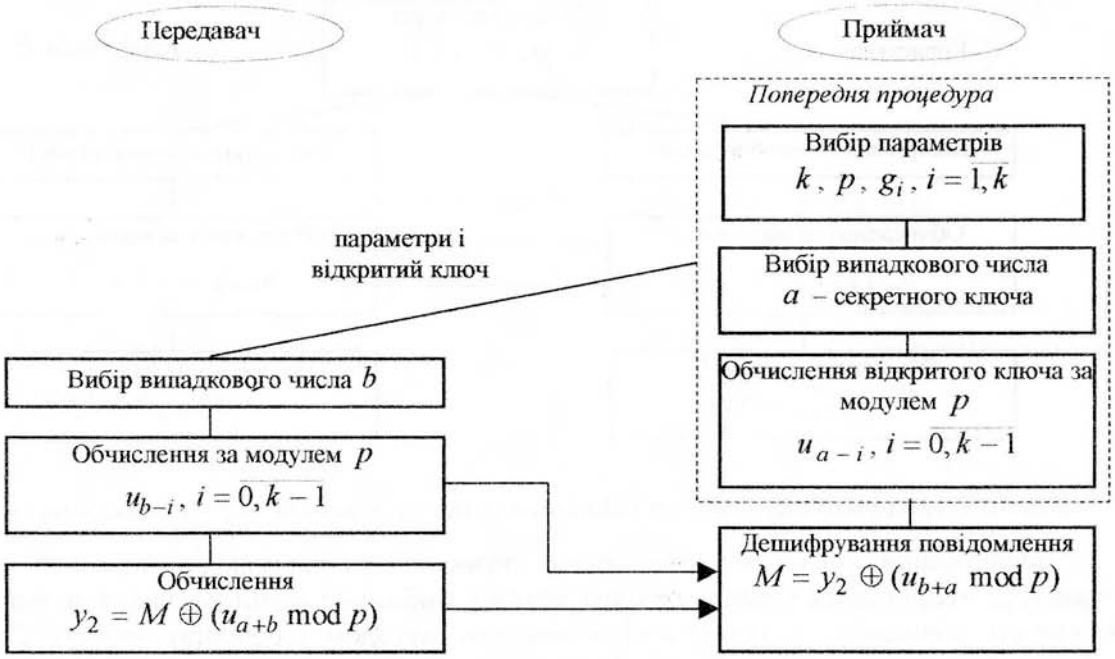

Рис. 2. Процедура шифрування на основі елементів U_k – послідовностей.

Розглянутий метод є модифікацією відомого методу шифрування інформації Ель–Гамаля. Суть модифікації полягає в заміні піднесення до степеня обчисленням певного елементу U_k □послідовності.

Проведено дослідження теоретичної криптостійкості та складності обчислень за даним методом, а також порівняння з відомим методом Ель-Гамаля. Показано, що модифікований метод Ель-Гамаля має таку ж криптостійкість, як і відомий метод, але при цьому для $k = 2$ має меншу складність обчислень у порівнянні з відомим.

Метод шифрування даних без попереднього розподілу ключів на основі елементів U_k – послідовності

Найвідомішим методом розв'язання задачі шифрування даних без попереднього розподілу ключів є триетапний протокол Шаміра. Можна побудувати метод подібний протоколу Шаміра на основі послідовного використання спочатку властивості обчислення елементу $u_{n+m,k}$, а потім властивості обчислення елементу $u_{n-m,k}$.

Виходячи з цього маємо такий метод шифрування. Передавач, використовуючи вибране ним випадкове число a, отримує зашифроване повідомлення, як результат об'єднання $u_{a-i,k}$, $i = \overline{0,2k-2}$ з відкритим повідомленням M за допомогою операції множення. Необхідність обчислення елементів $u_{a-i,k}$ саме для $i = \overline{0,2k-2}$ пов'язана з тим, що саме такий набір елементів використовується в подальшому у властивостях обчислення $u_{n+m,k}$ та $u_{n-m,k}$. Отримані результати Передавач передає Приймачу, здійснюючи таким чином перший етап передавання.

Приймач за допомогою свого вибраного випадкового числа b продовжує обчислення над прийнятими від Передавача даними, отримуючи свої дані $M \cdot u_{a+b-i,k}$ для $i = \overline{0,k-1}$ за формулою (4), а потім і для $i = \overline{k,2k-2}$ за формулою (6), використовуючи тільки-но отримані дані. При передаванні цих даних до Передавача здійснюється другий етап передавання.

Потім Передавач «знімає» свій ключ a з отриманих від Приймача даних, обчислюючи таким чином нові дані $M \cdot u_{(a+b)-a-i,k}$, $i = \overline{0,k-1}$ за формулою (7). Третій і заключний етап передавання здійснюється під час передавання отриманих даних до Приймача.

«Знявши» свій ключ b з отриманих даних за формулою (7), Приймач отримує значення $M \cdot u_{0,k}$, яке він дешифрує, виконуючи просту операцію ділення цього значення на $u_{0,k}$, або на g_1, як значення початкового елементу $u_{0,k}$.

Зазначимо, що використання операції множення для об'єднання відкритого повідомлення M з даними, що отримуються пов'язано з тим, що саме завдяки цій

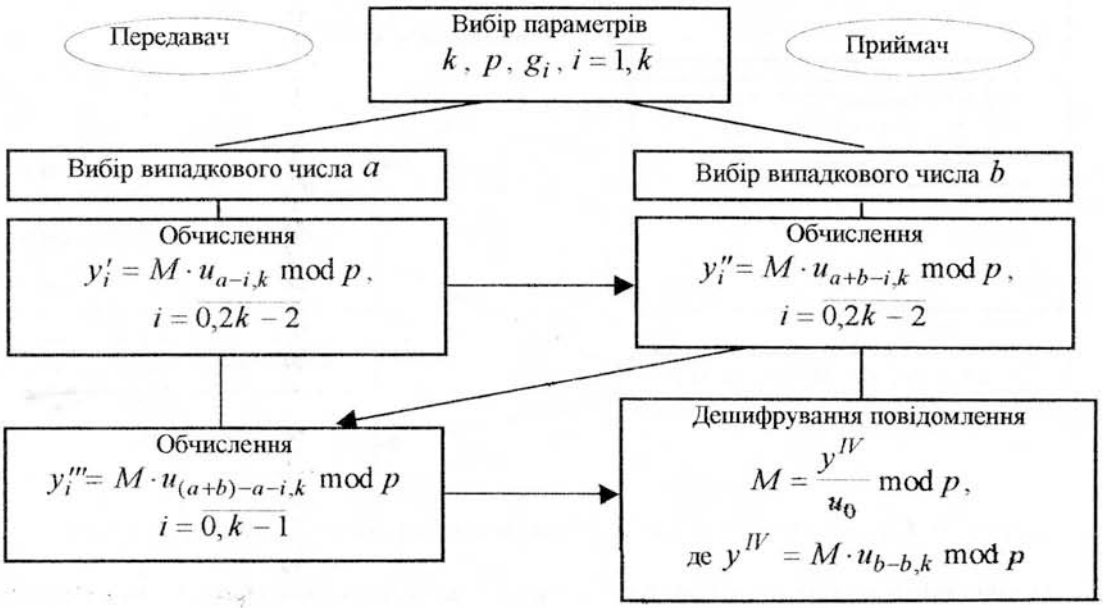

Рис. 3. Схема шифрування даних без попереднього розподілу ключів на основі елементів U_k – послідовності.

операції в усіх використаних формулах значення y_2 виноситься за дужки, не змінюючи при цьому правильність формул.

Загальна схема шифрування даних, при якому передавання даних здійснюється в три етапи представлена на рис.3.

Проведено дослідження теоретичної криптостійкості та складності обчислень за даним методом, а також порівняння з відомим методом Шаміра. Показано, що модифікований метод Шаміра має таку ж криптостійкість, як і відомий метод, але при цьому для будь-якого k має меншу складність обчислень у порівнянні з відомим, причому не менше ніж у 10^2 разів.

Метод аутентифікації на основі елементів U_k – послідовності

Задача встановлення авторства повідомлення може бути розв'язана з використанням властивості (4), яка, як вже розглядалось вище, дозволяє обчислювати елемент $u_{n+m,k}$ двома шляхами. Це дозволяє створити такий метод аутентифікації.

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 аутентичність 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 аутентифікації за даним методом представлена на рис.4.

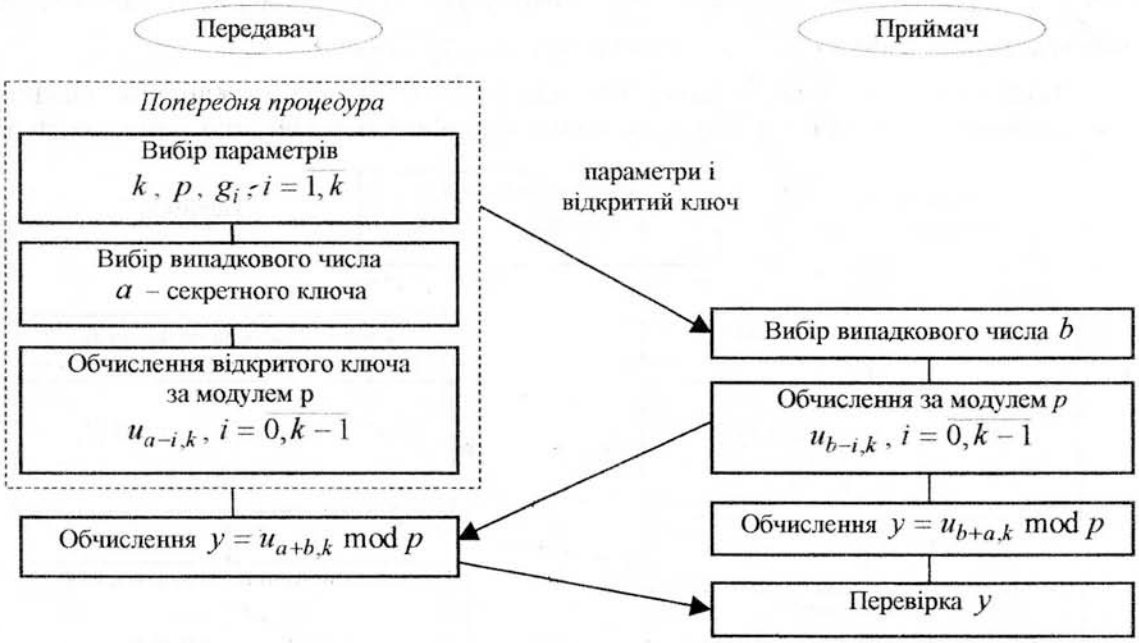

Рис. 4. Схема аутентифікації на основі елементів U_k □ послідовності.

Проведений аналіз криптостійкості такого методу аутентифікації показав, що він теоретично є криптостійким. Водночас, в порівнянні з відомими методами Фейге-Фіата-Шаміра, Гіллу-Кіскатра та Шнорра цей метод має простішу процедуру завдання параметрів, оскільки їх вибір не потребує проведення складних обчислень над великими числами, та приблизно вдвічі меншу складність обчислень. Слід також відзначити те, що у відомих методах аутентифікації, 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.

Висновок

В задачах криптографічного захисту інформації обчислення елементів U_k □ послідовності є альтернативою операції піднесення до степеня, оскільки забезпечує спрощення обчислень (від 2 до 10^2 разів). При цьому рівень крипостійкості не зменшується.

Список літератури:

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. Smith P. and Lennon M. LUC: A new public key system // Proceedings of the IFIP TC11 Ninth International Conference on Information Security. North-Holland. □ 1993. □ P.103–117.

5. Smith P. and Skinner C. A public-key cryptosystem and a digital signature system based on the Lucas function analogue to discrete logarithms // In Advances in Cryptology Asiacrypt '94, Springer-Verlag. □ 1995. □ P. 357□364.

6. Bleichenbacher D., Bosma W., and Lenstra A. Some remarks on Lucas-based cryptosystems // In Advances in Cryptology Crypto'95, Springer-Verlag. □ 1995. □ P.386 □□396.

7. Laih C.-S., Tu F.-K., and Tai W.-C. On the security of the Lucas function // Information Processing Letters. □ 1995. □ №53. P. 243–247.

8. Маркушевич А.И. Возвратные последовательности. □ М.: Наука, 1975. □ 48с.

9. Воробьев Н.Н. Числа Фибоначчи. □ М.: Наука, 1992. □ 192 с.

10. Horadam A.F. A generalized Fibonacci Sequence // Amer. Math. Monthly. □ 1961. □ Vol.68. □ P. 455 □□459.

11. Лужецький В.А., Яремчук Ю.Є. Рекурентні V_k -послідовності // Вісник ВПІ. - 1999. - №6. - С. 53 - 59.

12. 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.

Надійшла 31.01.2002

УДК 681.322

Гроздов Г.Г.

ИСПОЛЬЗОВАНИЕ СОВРЕМЕННЫХ КРИПТОАЛГОРИТМОВ В ПРОГРАММНЫХ СРЕСТВАХ ЗАЩИТЫ ИНФОРМАЦИИ

Рассмотрены возможности наиболее популярных современных программных средств защиты информации по использованию криптоалгоритмов. Приведены причины ненадежности этих средств, даны рекомендации для оптимального использования их возможностей.

Основным показателем, характеризующим развитие современных информационных технологий, является ежегодный рост числа компьютерных преступлений и связанных с ними хищений конфиденциальной и иной информации, а также материальных потерь.

Данная работа посвящена рассмотрению вопросов, связанных с методами криптографической защиты информации. Криптографические методы защиты информации являются неотъемлемой частью теории защиты информации. В современных вычислительных системах методы криптографии могут применяться для защиты информации, передаваемой по каналам связи, для аутентификации передаваемой информации или права на доступ к данным, для хранения данных на носителях в шифрованном виде и в других целях.

Выделим этапы развития криптографических методов защиты информации. Весь период с древних времен до 1949 года можно представить как период донаучной криптологии. Достижения этого периода были построены скорее на интуиции и вере, чем на научных доказательствах. Ситуация кардинально изменилась с выходом в 1949