УДК 621.391.7

Яремчук Ю.Є.

ОСОБЛИВОСТІ РОЗРОБЛЕННЯ ПРОГРАМНИХ ЗАСОБІВ РЕАЛІЗАЦІЇ ПРОТОКОЛІВ ШИФРУВАННЯ БЕЗ ПОПЕРЕДНЬОГО РОЗПОДІЛУ КЛЮЧІВ НА ОСНОВІ РЕКУРЕНТНИХ ПОСЛІДОВНОСТЕЙ

Розглянуто метод шифрування інформації без попереднього розподілу ключів на основі математичного апарату рекурентних V_k та U_k - послідовностей. Розроблено структуру програми шифрування, яка дозволяє реалізувати запропонований метод у вигляді набору модулів, що виконують певні обчислювальні процедури. Наведено структури програм шифрування / дешифрування головного модуля. З метою спрощення криптографічних перетворень розглянуто особливості програмної реалізації запропонованого методу, можливість реалізації певних модулів на низькому програмному рівні, а також наведено рекомендації щодо вибору параметрів.

Ключові слова: захист інформації, криптографія, шифрування, розподіл ключів, рекурентні послідовності, програмні засоби.

Вступ. В роботі [1] показано можливість використання рекурентних V_k^+ та U_k - послідовностей для побудови криптографічних методів, що базуються на технології відкритого ключа. Запропонований підхід дозволяє за певних умов спрощувати обчислення криптографічних перетворень.

В роботі [2] розглянуто метод шифрування інформації без попереднього розподілу ключів на основі рекурентних V_k і U_k - послідовностей та їх аналітичних залежностей. Метод забезпечує значне спрощення обчислень у порівнянні з відомим методом Шаміра [3] при забезпеченні достатнього рівня криптостійкості.

V_k - послідовністю називається послідовність чисел, яка складається з V_k^+ - послідовності та V_k^- - послідовності [2].

V_k^+ послідовністю називається 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 $k = 2$; $v_{0,k} = v_{1,k} = ... = v_{k-3,k} = 0$, $v_{k-2,k} = 1$, $v_{k-1,k} = g_k$ 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

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

V_k^- - послідовністю називається послідовність чисел, що обчислюються за формулою (2) для n - від'ємних при початкових значеннях $v_{-1,k} = 0$, $v_{-2,k} = g_1^{-1}$ для $k = 2$; $v_{-1,k} = 0$, $v_{-2,k} = g_1^{-1}$, $v_{-3,k} = v_{-4,k} = ... = v_{-k,k} = 0$ для $k > 2$.

U_k - послідовністю [1] називається 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 [1]

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

Для будь-яких цілих додатних n та k, таких що $n \geq k$, в [1] представлено залежність, яка дозволяє обчислювати елементи U_k - послідовності тільки на основі елементів V_k^+ - послідовності

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

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

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

Для будь-яких цілих додатних n і m, таких що $1 \leq m < n$ та будь-якого цілого додатного k [2]

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

На основі даного математичного апарату в [2] представлено метод шифрування інформації без попереднього розподілу ключів. Програмна чи апаратна реалізація криптографічних методів на основі технології відкритого ключа має ряд особливостей. Одна з них - необхідність виконувати обчислення над числами великої розрядності (1024 - 4096 двійкових розрядів). З урахуванням цих особливостей в [2] розроблено принципи побудови спеціалізованих процесорів шифрування / дешифрування інформації без попереднього розподілу ключів на основі рекурентних V_k та U_k -послідовностей.

Однак апаратна реалізація не в усіх випадках є прийнятною і можливою. Тому розглядається можливість розроблення програмних засобів шифрування та дешифрування інформації без попереднього розподілу ключів на основі рекурентних послідовностей з урахуванням усіх особливостей та можливості прискорювати процеси криптографічних перетворень.

Розроблення пакету програм шифрування інформації без попереднього розподілу ключів. Ідея методу шифрування інформації без попереднього розподілу ключів [2] базується на послідовному використанні спочатку аналітичної залежності (4) обчислення елементу $u_{n+m,k}$, а потім залежності (7) обчислення елементу $u_{n-m,k}$. Таким чином, якщо порівнювати з відомим методом Шаміра, здійснюється заміна модулярного піднесення до степеня обчисленням за модулем елементу U_k послідовності з певним індексом.

Загальна процедура шифрування даних без попереднього розподілу ключів згідно даного методу представлена на рис. 1.

Згідно представленого методу шифрування основні обчислення виконуються згідно залежностей (4) і (7). Для обчислення елементів $u_{n+m-i,k}$, $i = \overline{0,k-1}$ згідно залежності (4) потрібні елементи $v_{m+i,k}$, $i = \overline{-k,k-2}$ та елементи $u_{n-i,k}$, $i = \overline{0,k-1}$, а для обчислення елементів $u_{n-m-i,k}$, $i = \overline{0,k-1}$ згідно залежності (7) потрібні елементи $v_{-m+i,k}$, $i = \overline{-k,k-2}$ та елементи $u_{n-i,k}$, $i = \overline{0,k-1}$. Обчислення елементів $u_{n-i,k}$, $i = \overline{0,k-1}$ здійснюється Передавачем за формулою (5). При цьому потрібно мати елементи $v_{n+i,k}$, $i = \overline{-2k+1,-1}$.

Звідси виходить, що всього для обчислення елементу $u_{n+m,k}$ згідно залежності (4) та елементу $u_{n-i,k}$, $i = \overline{0,k-1}$, за формулою (5) потрібно мати елементи $v_{n+i,k}$, $i = \overline{-2k+1,k-2}$, V_k послідовності. Частину елементів цього набору для $i = \overline{-(k-1),k-2}$ отримаємо за алгоритмом прискореного обчислення елементів V_k^+ - послідовності [1]. Іншу частину, для $i = \overline{-2k+1,-k}$, отримаємо за формулою (2), використовуючи дані отримані в цьому

алгоритмі. Елементи $v_{-m+i,k}$, $i=\overline{-k,k-2}$, що використовуються в залежності (7), обчислимо за алгоритмом прискореного обчислення елементів $v_{n,k}$ для від'ємних значень n [4].

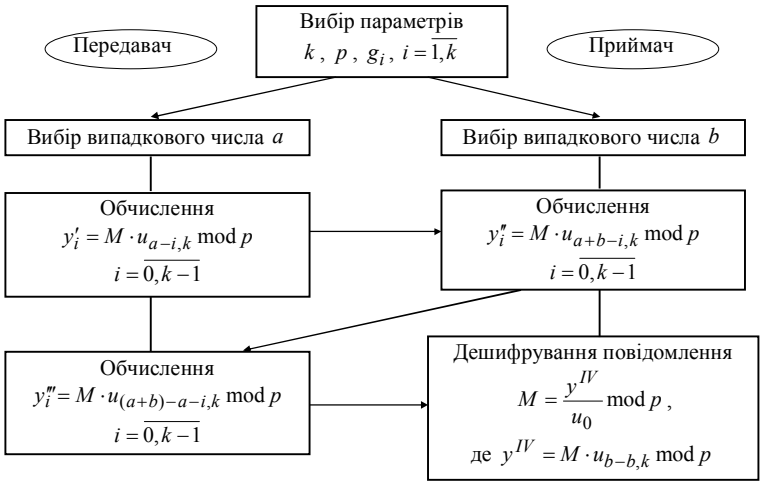

Рис. 1. Процедура шифрування даних без попереднього розподілу ключів на основі елементів U_k - послідовності

Розглянемо особливості розроблення пакету програм, що реалізують процедури шифрування та дешифрування інформації згідно з представленим методом шифрування інформації без попереднього розподілу ключів.

Розроблення пакету програм пропонується розпочати з визначення його складових програмних модулів. Для цього пропонується виділити такі програмні модулі:

- головний модуль реалізації методу шифрування інформації без попереднього розподілу ключів на основі V_k - та U_k - послідовностей;
- модуль задавання та вибору параметрів;
- модуль генерування випадкових чисел, у т.ч. простих, у заданому діапазоні;
- модуль обчислення елементів V_k - та U_k - послідовностей;
- модуль виконання арифметичних операцій з великими числами.

На рис. 2 представлена узагальнена структура програмної реалізації протоколу шифрування без попереднього розподілу ключів з відображенням зв'язків між її компонентами.

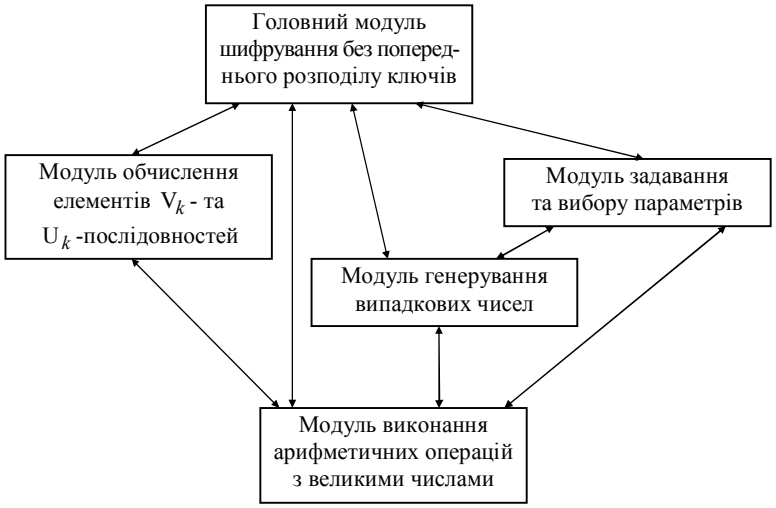

Рис. 2. Узагальнена структура програмної реалізації методу шифрування без попереднього розподілу ключів на основі елементів U_k -послідовностей

Розглянемо реалізацію кожного програмного модуля.

Головний модуль містить програмні процедури реалізації дій, що виконують окремо Передавач та Приймач за представленим методом шифрування без попереднього розподілу ключів.

Алгоритми реалізації цих процедур представлені на рис. 3, 4.

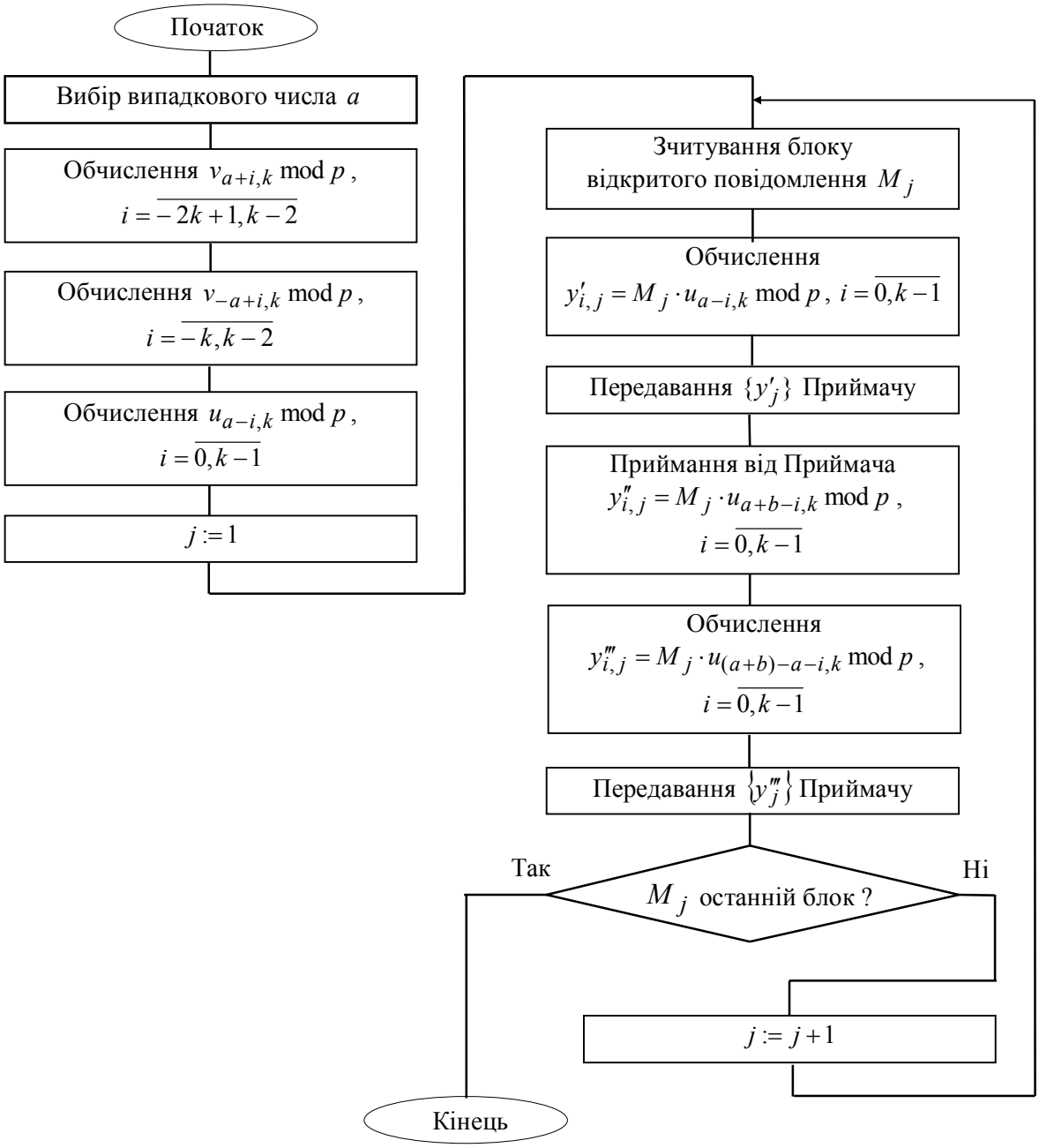

Рис. 3. Структура програми шифрування без попереднього розподілу ключів на основі елементів U_k-послідовностей з боку Передавача

Шифрування інформації в розглянутому протоколі шифрування проводиться не для всього відкритого повідомлення M, а для окремих його частин M_j. Розмір однієї частини визначається параметром p. Тобто зашифровані повідомлення y'_i, y''_i, y'''_i, $i = \overline{0, k-1}$, в протоколі шифрування без попереднього розподілу ключів складаються з окремих частин.

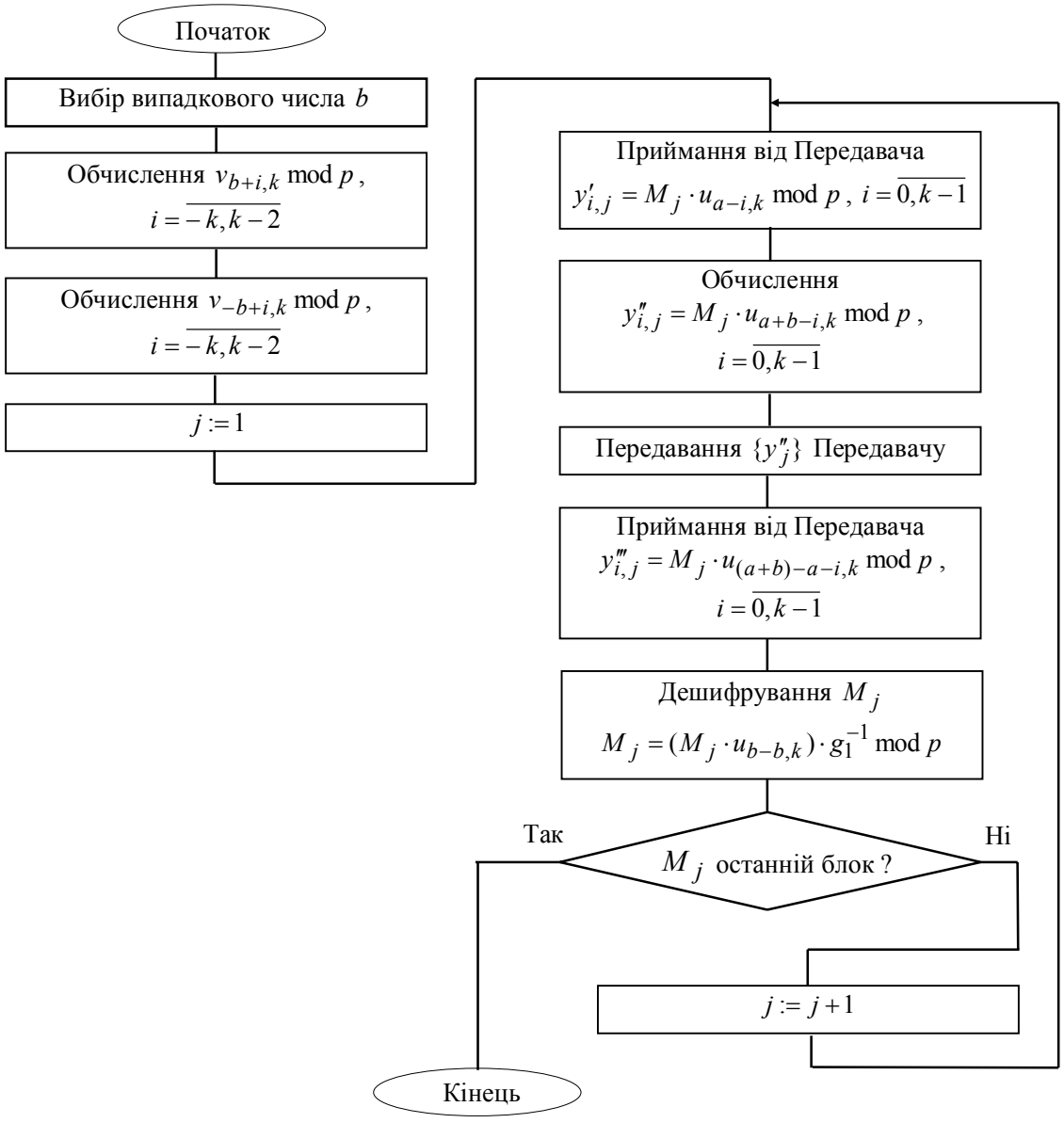

Рис. 4. Структура програми шифрування без попереднього розподілу ключів на основі елементів U_k-послідовностей з боку Приймача

Вибір параметру p здійснюється в програмному модулі задавання та вибору параметрів, де окрім нього задається параметр k та вибираються коефіцієнти рекурентного співвідношення g_i, $i = \overline{1, k}$.

При задаванні параметру k слід враховувати, що від цього параметру в прямій залежності знаходиться криптостійкість представленого методу шифрування без попереднього розподілу ключів, а також складність виконання, а, отже, і час виконання програм шифрування/дешифрування інформації.

Рекомендується вибирати параметр k, що дорівнює 2 або 3.

Параметр p вибирається як випадкове число, розрядність якого кратна розрядності машинної одиниці інформації й залежить від можливостей комп'ютера, на якому реалізується програма шифрування інформації. Для сучасних комп'ютерів цю розрядність слід вибирати 1024, 2048 або 4096.

В протоколі шифрування без попереднього розподілу ключів усі арифметичні операції виконуються з великими числами. Необхідність виділення окремого програмного модуля для виконання операцій з великими числами пов'язана із певними обмеженнями реалізації таких

операцій у відомих мовах програмування, які не завжди є прийнятними для реалізації криптографічних методів.

З метою прискорення криптографічних перетворень даний програмний модуль розроблено на низькому рівні програмної реалізації. Зокрема, реалізовані такі операції над числами великої розрядності, як цілочисельне додавання, віднімання та операції за модулем додавання, віднімання, обчислення мультиплікативно оберненої величини, лишку Монтгомері, множення за Монтгомері та обчислення величин, що необхідні для виконання прискореної операції піднесення до степеня за Монтгомері.

Зазначимо, що обчислення мультиплікативно оберненої величини за модулем виконується за умови $(p,b)=1$, а при обчисленні $g_1^{-1} \bmod p$ потрібно виконання умови $(g_1, p)=1$. Щоб задовольнити вказані умови, параметр p вибирається як просте число.

Коефіцієнти g_i, $i=\overline{1,k}$, вибираються як випадкові числа.

Оскільки параметр p є модулем при обчисленнях та визначає верхню границю усіх чисел, що використовуються в протоколі шифрування, вибір параметрів g_i, $i=\overline{1,k}$, здійснюється в діапазоні $[1, p]$.

Таким чином, для вибору параметрів алгоритмів шифрування/дешифрування потрібні генератори звичайних випадкових та простих випадкових чисел.

Тут зазначимо, що генератор випадкових чисел потрібен і для вибору сеансових секретних ключів a і b в алгоритмах шифрування/дешифрування без попереднього розподілу ключів.

Програмна реалізація генераторів випадкових чисел здійснюється в модулі генерування випадкових чисел.

Для генерування параметрів g_i, $i=\overline{1,k}$, може використовуватись один з відомих генераторів випадкових чисел [5, 6], наприклад, лінійний конгруентний генератор.

Для вибору секретних ключів рекомендується використовувати більш випадкові генератори. Наприклад, генератор, заснований на затримках між натисненнями клавіш клавіатури.

Для генерування простих випадкових чисел пропонується використовувати відомі тести на простоту [5], зокрема тест Міллера-Рабіна.

Розглянемо реалізацію модуля обчислення елементів V_k та U_k-послідовностей.

Аналіз алгоритмів, представлених на рис. 3, 4, показує, що в цих алгоритмах використовуються однакові блоки обчислення елементів V_k- та U_k-послідовностей тільки для різних значень індексу. Тому окремо слід виділити такі процедури:

- обчислення за модулем p $v_{n+i,k}$, $i=\overline{-2k+1,k-2}$ для додатних n;
- обчислення за модулем p $v_{n+i,k}$, $i=\overline{-k,k-2}$ для від'ємних n;
- обчислення за модулем p $u_{n-i,k}$, $i=\overline{0,k-1}$;
- обчислення за модулем p $u_{n+m-i,k}$, $i=\overline{0,k-1}$;
- обчислення за модулем p $u_{n-m-i,k}$, $i=\overline{0,k-1}$.

При реалізації процедури обчислення елементу $v_{n,k}$ за модулем p для додатних і для від'ємних значень n пропонується виділити окремо такі процедури:

- рискорене обчислення елементу $v_{n,k}$ для додатних n, наприклад, за алгоритмом, який наведено в роботі [1];
- прискорене обчислення елементу $v_{n,k}$ для від'ємних n, наприклад, за одним із алгоритмів, які наведено в [4];

- пряме обчислення елементу $v_{n,k}$ за формулою (1);
- зворотне обчислення елемента $v_{n,k}$ за формулою (2).

Таким чином визначена структура програми шифрування без попереднього розподілу ключів, а також визначено, як розробляти усі програмні модулі цієї структури.

Здійснено повну реалізацію на низькому рівні програмних модулів виконання арифметичних операцій з великими числами, вибору параметрів, обчислення елементів V_k- та U_k-послідовностей, а також головного модуля реалізації представленого методу шифрування інформації без попереднього розподілу ключів.

Розмір машинного коду розробленого пакету програм не перевищує 30 Кбайт.

Висновки. Розглянуто метод шифрування інформації на основі математичного апарату рекурентних V_k- і U_k-послідовностей та їх аналітичних залежностей. З метою прискорення обчислень розроблено узагальнену структуру програми шифрування інформації на основі елементів U_k-послідовностей, яка дозволяє реалізувати розглянутий метод у вигляді набору модулів, що виконують певні обчислювальні процедури. Найскладнішим з усіх модулів є модуль виконання арифметичних операцій з великими числами. Запропонована програмна реалізація повного набору арифметичних операцій за модулем.

Окремо розроблено структуру головного модуля - програм шифрування / дешифрування інформації без попереднього розподілу ключів згідно розглянутого методу. Також наведено особливості програмної реалізації методу та рекомендації щодо вибору параметрів з метою спрощення обчислень криптографічних перетворень.

ЛІТЕРАТУРА

1. Яремчук Ю.Є. Використання рекурентних послідовностей для побудови криптографічних методів з відкритим ключем // Захист інформації. - 2012.- №4. - С. 120-127.

2. Яремчук Ю.Є. Спеціалізовані процесори шифрування інформації без попереднього розподілу ключів на основі рекурентних послідовностей // Радіотехніка. - 2013. - Вип. 172. - С. 109-117.

3. Месси Д.Л. Введение в современную криптологию // ТИИЭР. - 1988. - Т.76№5. - С. 2442.

4. Яремчук Ю.Є. Оцінювання обчислювальної складності алгоритмів прискореного обчислення елементів рекурентних послідовностей // Вісник СНУ ім. В. Даля. - 2012. - №12 (183),Ч.2. - С. 113-121.

5. Menezes, A.J. Handbook of Applied Cryptography / A.J. Menezes, P.C. van Oorschot, S.A. Vanstone. - CRC Press, 2001. - 816 p.

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

Надійшла: 29.03.2013 р.

Рецензент: д.т.н., проф. Хорошко В.О.