УДК 621.391.7

Ю.Є.Яремчук,
кандидат технічних наук, доцент

ШИФРУВАННЯ ІНФОРМАЦІЇ БЕЗ ПОПЕРЕДНЬОГО РОЗПОДІЛУ КЛЮЧІВ НА ОСНОВІ РЕКУРЕНТНИХ ПОСЛІДОВНОСТЕЙ

У роботі розглянуто метод шифрування інформації без попереднього розподілу ключів на основі рекурентних V_k^+ *та* U_k*-послідовностей та їх залежностей. Проведено дослідження представленого методу щодо обчислювальної складності та криптостійкості.*

Ключові слова*: інформація, захист інформації, криптографія, шифрування, розподіл ключів, рекурентні послідовності.*

В работе рассмотрен метод шифрования информации без предварительного распределения ключей на основе рекуррентных V_k^+ *и* U_k*-последовательностей и их зависимостей. Проведено исследование представленного метода по вычислительной сложности и криптостойкости.*

Ключевые слова*: информация, защита информации, криптография, шифрование, распределение ключей, рекуррентные последовательности.*

The paper considers the method of information encryption without preliminary key distribution based on recurrent V_k^+ *and* U_k*-sequences and their relations. A research of the presented method on computational complexity and cryptologic reliability has been conducted.*

Keywords: *information, information security, cryptography, encryption, key distribution, recurrent sequence.*

Збільшення кола користувачів систем і розподіл завдань, що виконуються за допомогою мереж, призвели до усвідомлення першочергової важливості проблем, пов'язаних із забезпеченням інформаційної безпеки при міжмережевій взаємодії, перш за все, з використанням відкритих каналів передавання даних, які створюють потенційну можливість для дій зловмисника. При цьому безпечне передавання ключів стає не менш важливим, ніж безпечне передавання інформації.

Особливо гостро проблема розподілу ключів постає в симетричних криптосистемах [1, 2], оскільки виникає необхідність обміну секретними ключами перед безпосереднім шифруванням інформації, причому таким чином, щоб ключ обміну став відомий лише учасникам обміну. В асиметричних системах [1–4] ця проблема по суті є винятком, оскільки розповсюдженню підлягає лише відкритий ключ, який є доступним будь-кому, хто бажає послати повідомлення адресату, але і в цьому випадку сама необхідність попереднього передавання ключів залишається.

Під час реалізації криптографічних систем виникають випадки, коли необхідно здійснювати шифрування інформації без попереднього розповсюдження ключів [1, 2]. В таких випадках застосовують протоколи шифрування без попереднього

розподілу ключів. Вперше такий протокол був запропонований Шаміром [5] і має назву трьохетапний протокол Шаміра. В протоколі передавач і приймач виконують обчислення над даними по два рази на кожному боці, здійснюючи при цьому три передавання даних: два від передавача до приймача і одне від приймача до передавача. З точки зору обчислювальної складності метод є недостатньо ефективним, оскільки крім необхідності виконання трьохетапної процедури передавання, ще необхідно під час обчислень здійснювати піднесення до ступеня над числами великої розрядності.

З огляду на це, актуальним є побудова методів шифрування без попереднього розподілу ключів на основі таких математичних апаратів, які б могли забезпечувати спрощення обчислень. У зв'язку з цим, певний інтерес викликає апарат на основі рекурентних послідовностей [6], який дозволяє за певних умов спрощувати обчислення в криптографічних застосуваннях, що базуються на його основі.

Так у роботах [7, 8] показано можливість використання рекурентних V_k^+ + та U_k-послідовностей для побудови криптографічних методів, що базуються на технології відкритого ключа, зокрема методів розподілу ключів та шифрування інформації.

У статті пропонується метод шифрування інформації без попереднього розподілу ключів на основі математичного апарату, що базується на цих рекурентних послідовностях.

Математичний апарат на основі рекурентних послідовностей для розробки методу шифрування без необхідності розподілу ключів

Рекурентні послідовності в загальному вигляді породжуються таким співвідношенням [6]

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

де a_1, a_2, . . . a_k, – коефіцієнти, k – порядок послідовності, з огляду на початкові елементи u_1, u_2, . . . , u_k.

Назвемо 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^+-послідовністю.

Формула (1) дозволяє отримувати значення для зростаючих n, починаючи з n=0. Можлива і зворотна процедура, коли елементи послідовності обчислюються для спадних n, починаючи з деякого значення n=1. Обчислення елементів такої послідовності 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

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

В окремому випадку, коли залежність (3) буде мати такий вигляд

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

З наведених аналітичних залежностей V_k^+-послідовності видно, що для довільного додатного номеру n обчислення елементу $v_{n,k}$ може здійснюватись за формулою (1). Однак безпосереднє обчислення $v_{n,k}$ за цією формулою є повільним, а тому не може бути використано для великих значень n. Це створює проблему, оскільки при розробці методу шифрування без попереднього розподілу ключів доцільним є використання саме великих значень індексу елементу послідовності. Для вирішення цієї проблеми в роботі [7] розглянуто спосіб прискореного обчислення елементу $v_{n,k}$ для додатних n, який базується на тій самій ідеї, що і бінарний метод [9] піднесення до ступеня.

Обчислення за формулою (2) може продовжуватись і для $n < 0$, тобто існує два види послідовностей. Перший вид послідовностей формується для n – додатних за формулою (1). Другий вид послідовностей формується для n – від'ємних за формулою (2).

Назвемо V_k^--послідовністю 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 $k = 2$; $v_{-1,k} = 0$, $v_{-2,k} = g_1^{-1}$, $v_{-3,k} = v_{-4,k} = \ldots = v_{-k,k} = 0$ для $k > 2$.

Тоді послідовність чисел, яка складається з V_k^+-послідовності та V_k^--послідовності, назвемо V_k-послідовністю.

Для будь-яких цілих додатних n і m, таких що $1 \le m < n$ та будь-якого цілого додатного k, отримано таку аналітичну залежність

$$v_{n-m,k} = v_{-m+(k-2),k} \cdot v_{n,k} + g_1 \cdot \sum_{i=1}^{k-1} v_{-m+(k-2)-i,k} \cdot v_{n-k+i,k}. \quad (5)$$

З наведених формул та отриманих залежностей для V_k-послідовності видно, що обчислення елементів $v_{n,k}$ для від'ємних значень n безпосередньо за формулою (2) є неприйнятним з тієї ж причини, що і для додатних n, коли вони приймають великі значення. Тому розглянемо алгоритм прискореного обчислення елементу $v_{n,k}$ для від'ємних n. Розробку алгоритму проведено аналогічно, як і для додатних n, включаючи використання бінарного методу.

Скористаємось бінарним методом [1, 9] для отримання адитивного ланцюжка

$$1 = c_0, c_1, c_2, \ldots, c_t = n.$$

Якщо записати n в двійковій системі числення як $n = \sum_{i=0}^{t} \alpha_{t-i} 2^{t-i}$, то для кожного $i = \overline{1,t}$ правило отримання адитивного ланцюжка, починаючи з c_1, буде таким

– якщо значення α_{t-i} дорівнює 0, то $c_i = 2c_{i-1}$;

– якщо значення розряду α_{t-i} дорівнює 1, то $c_i = 2c_{i-1}+1$.

Як наслідок, дійшовши до крайнього правого розряду n отримаємо $c_t=n$.

Для того, щоб обчислити за бінарним методом елемент $v_{n,k}$ необхідно, в першу чергу, мати формулу для обчислення елементу $v_{2n,k}$. Якщо для будь-якого додатного r прийняти $n=-r$, $m=r$, то з аналітичної залежності (5) отримаємо таку залежність для обчислення елементу $v_{-2r,k}$:

$$v_{-2r,k} = v_{-r+(k-2),k} \cdot v_{-r,k} + g_1 \cdot \sum_{i=1}^{k-1} v_{-r+(k-2)-i,k} \cdot v_{-r-k+i,k} \ . \qquad (6)$$

Аналіз аналітичної залежності (6) показує, що для отримання елементу $v_{-2r,k}$ використовуються елементи $v_{-r+k-2,k}$, ... , $v_{-r-(k-2),k}$, $v_{-r-(k-1),k}$. Обчислення елементу $v_{n,k}$ для великих від'ємних значень n потребує багатократного використання залежності (6). Тому на кожному кроці обчислень елементу $v_{n,k}$, як мінімум потрібно мати всі елементи, що використовуються в залежності (6).

Елементи $v_{-2r+k-2,k}$, ... , $v_{-2r,k}$, $v_{-2r-1,k}$ обчислимо згідно з залежністю (5) відповідно, як $v_{(-r+k-2)-r,k}$, ... , $v_{-r-r,k}$, $v_{(-r-1)-r,k}$. При цьому необхідно мати елементи $v_{-r+k-2,k}$, ... , $v_{-r-(k-1),k}$, $v_{-r-k,k}$, з яких визначеними вже, з точки зору обчислень, є лише елементи $v_{-r+k-2,k}$, ... , $v_{-r,k}$, $v_{-r-1,k}$. Обчислення ж елементів $v_{-2r-2,k}$, ... , $v_{-2r-(k-1),k}$, $v_{-2r-k,k}$ здійснимо за формулою (2), використовуючи вже обчислені елементи $v_{-2r+k-2,k}$, ... , $v_{-2r,k}$, $v_{-2r-1,k}$.

Таким чином, визначено всі елементи, які потрібні для обчислення елементу $v_{n,k}$ для від'ємних значень n за бінарним методом. Це елементи $v_{-r+k-2,k}$, ... , $v_{-r-(k-1),k}$, $v_{-r-k,k}$.

Слід також відзначити, що в прискореному алгоритмі, який розробляється, індекс n елементу V_k-послідовності буде приймати великі значення, тому доцільно одразу усі операції виконувати за модулем, тим більше, що і в методі шифрування без попереднього розподілу ключів обчислення будуть виконуватись над числами великої розрядності.

Позначивши l як поточне значення індексу елементу V_k-послідовності, маємо такий алгоритм прискореного обчислення елементу $v_{n,k}$ для від'ємних n.

П. 1. Провести початкову ініціалізацію: $i \leftarrow t$; $l \leftarrow 1$; присвоїти елементам $v_{-l+k-2,k}$, ... , $v_{-l-(k-1),k}$, $v_{-l-k,k}$ відповідні значення V_k-послідовності.

П. 2. $i \leftarrow i-1$.

П. 3. $l \leftarrow 2l$.

П. 4. Обчислити нові значення елементів $v_{-l+k-2,k}$, ... , $v_{-l,k}$, $v_{-l-1,k}$, за модулем p, використовуючи (6).

П. 5. Обчислити елементи $v_{-l-2,k}$, ... , $v_{-l-(k-1),k}$, $v_{-l-k,k}$, за модулем p, використовуючи (2).

П. 6. Якщо $\alpha_i = 0$, то перейти до п. 9.

П. 7. $l \leftarrow l+1$.

П. 8. Обчислити нові значення $v_{-l+k-2,k}$, ... , $v_{-l-(k-1),k}$, $v_{-l-k,k}$ шляхом присвоювання кожному елементу значення попереднього елементу та обчислення за модулем p першого з цього набору елементу $v_{-l-k,k}$ за формулою (2), використовуючи тільки-но обчислені елементи.

П. 9. Якщо $i-1 \neq 0$, то перейти до п. 3, інакше завершити роботу алгоритму.

Таким чином представлено, а також отримано аналітичні залежності та алгоритми прискореного обчислення елементів V_k-послідовності. Ця послідовність є окремим випадком більш узагальненої послідовності, оскільки значення більшості початкових елементів нульові. Якщо дозволити, щоб ці початкові елементи приймали будь-які значення, то отримаємо такий варіант узагальненої послідовності.

Назвемо послідовність чисел, що обчислюються за формулою

$$u_{n,k} = g_k u_{n-1,k} + g_1 u_{n-k,k} \tag{7}$$

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 – U_k-послідовністю.

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

$$u_{n+m,k} = v_{m+(k-2),k} \cdot u_{n,k} + g_1 \cdot \sum_{i=1}^{k-1} v_{m+(k-2)-i,k} \cdot u_{n-k+i,k}\,. \tag{8}$$

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

$$u_{n,k} = g_k \cdot v_{n-1,k} + g_1 \cdot \sum_{i=1}^{k-1} g_i \cdot v_{n-i-1,k}\,. \tag{9}$$

Виходячи з формули (7), вираз для обчислення елементів $v_{n,k}$ для спадних n, починаючи з деякого $n=l$, має такий вигляд

$$u_{n,k} = \frac{u_{n+k,k} - g_k u_{n+k-1,k}}{g_1}\,. \tag{10}$$

Для будь-яких цілих додатних n і m, таких, що $1 \leq m < n$, та будь-якого цілого додатного k, отримано таку залежність

$$u_{n-m,k} = v_{-m+(k-2),k} \cdot u_{n,k} + g_1 \cdot \sum_{i=1}^{k-1} v_{-m+(k-2)-i,k} \cdot u_{n-k+i,k}\,. \tag{11}$$

В окремому випадку, коли $k = 2$, для будь-яких цілих додатних n та m, таких, що $1 < m < n$, додатково отримано таку аналітичну залежність

$$u_{n-m,2} = (-1)^m \cdot g_1^{-(m-1)} \cdot (v_{m-2,2} \cdot u_{n,2} - v_{m-1,2} \cdot u_{n-1,2})\,. \tag{12}$$

Метод шифрування інформації без попереднього розподілу ключів на основі рекурентних V_k та U_k-послідовностей

З метою прискорення обчислень пропонується ідея методу шифрування інформації без попереднього розподілу ключів, що базується на послідовному використанні спочатку аналітичної залежності (8) обчислення елементу $u_{n+m,k}$, а потім залежності (11) обчислення елементу $u_{n-m,k}$. Ідея в чомусь подібна з відомим методом Шаміра. Відмінність полягає в тому, що відбувається заміна модулярного піднесення до ступеня обчисленням за модулем елементу U_k-послідовності з певним індексом.

Передавач, використовуючи вибране ним випадкове число a, обчислює $u_{a-i,k}$, $i=\overline{0,k-1}$, та отримує зашифроване повідомлення, як результат об'єднання $u_{a-i,k}$, $i=\overline{0,k-1}$, з відкритим повідомленням M за допомогою операції множення. 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 $i=\overline{0,k-1}$ згідно залежності (8). 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 $M\cdot u_{(a+b)-a-i,k}$, $i=\overline{0,k-1}$ згідно залежності (11). Третій і заключний етап передавання здійснюється під час передавання отриманих даних до Приймача.

"Знявши" свій ключ b з отриманих даних згідно залежності (11), Приймач отримує значення $M\cdot u_{0,k}$, яке він дешифрує, виконуючи просту операцію ділення цього значення на $u_{0,k}$, або множення на g_1^{-1}, оскільки g_1 є значенням 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 операції в усіх використаних залежностях та формулах значення M виноситься за дужки, не змінюючи при цьому правильність формул.

Загальна процедура шифрування інформації без попереднього розподілу ключів згідно представленого методу представлена на рис.1.

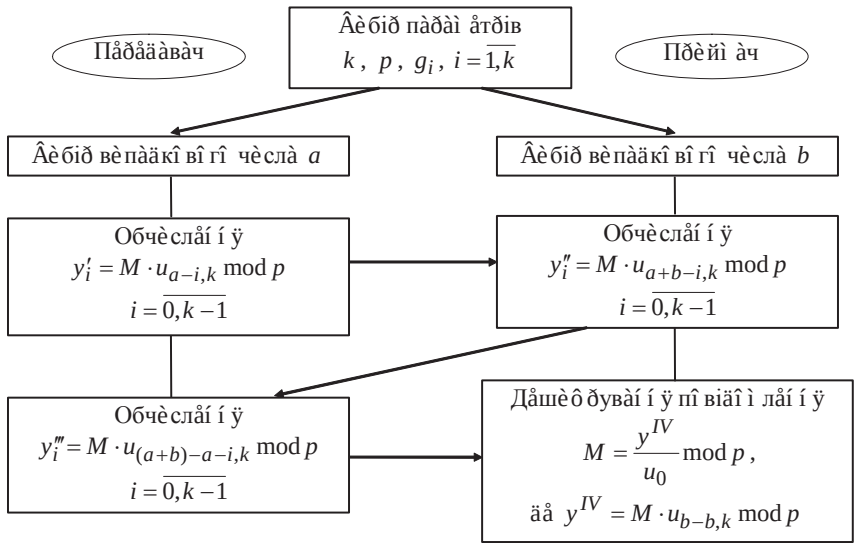

Рис. 1. Процедура шифрування інформації без попереднього розподілу ключів на основі елементів U_k - послідовності.

Операція за модулем в наведеній процедурі шифрування використовується для обмеження розрядності чисел, що використовуються при обчисленнях в процесі шифрування.

Згідно із запропонованим методом шифрування основні обчислення виконуються згідно залежностей (8) та (11). Для обчислення елементів $u_{n+m-i,k}$, $i=\overline{0,k-1}$ т згідно залежності (8) 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 (11) 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 згідно залежності (9). 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 (8) та елементу $u_{n-i,k}$, $i=\overline{0,k-1}$, згідно залежності (9) 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, який було розглянуто в роботі [7]. Іншу частину, для $i=\overline{-2k+1,-k}$, отримаємо за формулою (2), використовуючи дані, отримані в цьому алгоритмі. І, насамкінець, частина елементів $v_{-m+i,k}$, $i=\overline{-k,k-2}$, що використовуються в залежності (11), може бути обчислена за алгоритмом прискореного обчислення елементів $v_{n,k}$ для від'ємних значень n, який було представлено вище.

Тепер, коли визначено як проводити обчислення за усіма формулами, що використовуються в методі шифрування даних без попереднього розподілу ключів, алгоритм шифрування за цим методом набуває такого вигляду.

Визначивши необхідні аналітичні залежності та алгоритми прискореного обчислення елементів рекурентних послідовностей, протокол шифрування інформації без попереднього розподілу ключів згідно представленого методу буде мати такий вигляд.

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, а Приймачу вибрати випадкове число b.

П. 6. Передавачу обчислити $v_{a+i,k}$ за модулем p, а Приймачу обчислити $v_{b+i,k}$ за модулем p для $i=\overline{-(k-1),k-2}$, використовуючи алгоритм прискореного обчислення елементів $v_{n,k}$ для додатних значень n.

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

П. 8. Передавачу обчислити $v_{-a+i,k}$ за модулем p, а Приймачу обчислити $v_{-b+i,k}$ за модулем p для $i=\overline{-k,k-2}$, використовуючи алгоритм прискореного обчислення елементів $v_{n,k}$ для від'ємних значень n.

П. 9. Передавачу обчислити $u_{a-i,k}$, $i=\overline{0,k-1}$, за модулем p, використовуючи (9).

П. 10. Передавачу обчислити

$$y_i' = M \cdot u_{a-i} \bmod p, \quad i=\overline{0,k-1}.$$

П. 11. Передавачу передати y_i', $i = \overline{0,k-1}$, Приймачу.

П. 12. Приймачу обчислити y_i'', $i = \overline{0,k-1}$, за модулем p, використовуючи (8).

П. 13. Приймачу передати y_i'', $i = \overline{0,k-1}$, Передавачу.

П. 14. Передавачу обчислити y_i''', $i = \overline{0,k-1}$, за модулем p, використовуючи (11).

П. 15. Передавачу передати y_i''', $i = \overline{0,k-1}$, Приймачу.

П. 16. Приймачу дешифрувати повідомлення M за формулою

$$M = \frac{y^{IV}}{u_{0,k}} \bmod p = (y^{IV} \cdot g_1^{-1}) \bmod p ,$$

де y^{IV} обчислюється за модулем p за формулою (11), використовуючи дані, отримані ним в п. 8, та дані, що передав Передавач у п. 15.

В окремому випадку, коли $k = 2$, можливий варіант алгоритму, якщо при обчислені елементу $u_{n-m,2}$ в пп. 15 та 17 замість залежності (11) використовувати залежність (12). Це дозволить уникнути обчислення елементу $v_{n,2}$ для від'ємних n в п. 8, тим самим виключивши взагалі його з алгоритму. Але складність алгоритму при цьому значно не зменшиться, оскільки замість обчислення елементу $v_{n,2}$ для від'ємних n необхідно виконувати згідно аналітичної залежності (12) піднесення до ступеня за основою g_1, а це майже однаково за складністю.

В представленому методі, як і у відомому методі Шаміра, Передавач і Приймач виконують обчислення над даними по два рази кожен на своєму боці та здійснюють три передавання даних.

Визначимо тепер обчислювальну складність представленого протоколу шифрування інформації без попереднього розподілу ключів.

Основні обчислення в протоколі Передавач проводить в пп. 6–10, 14, а Приймач в пп. 6–8, 12, 16. Складність обчислення елементів в п. 6 з боку Передавача, як і з боку Приймача визначається складністю алгоритму прискореного обчислення елементів $v_{n+i,k}$, $i = \overline{-(k-1),k-2}$, для додатних значень n. Так само для кожного, складність обчислення елементів в п. 8 визначається складністю алгоритму прискореного обчислення елементів $v_{n+i,k}$ для $i = \overline{-k,k-2}$, для від'ємних значень n.

Оскільки повідомлення M зазвичай розбивають на певну кількість Q частин $M_1, M_2, ..., M_Q$ фіксованого розміру, кожна з яких шифрується окремо, то Передавач буде виконувати пп. 10, 14 Q разів, а Приймач так само – пп. 12, 16. Отже в Q разів зросте і складність виконання вказаних пунктів.

Не важко пересвідчитись, що складність обчислень за алгоритмами прискореного обчислення елементів $v_{n,k}$ для додатних і для від'ємних значень n на рівні машинних одиниць інформації будуть однаковими. Визначено, що максимальна оцінка складності кожного з них не буде перевищувати $H^2 q \cdot [6H(k^2+3k)+9(k^2+2k)]$ операцій над машинними одиницями інформації, де H – кількість машинних одиниць інформації для зберігання великого числа, q – кількість розрядів машинної одиниці інформації.

Окрім того, Передавачу і Приймачу необхідно виконувати обчислення елементів V_k та U_k-послідовності згідно з формулою (2) і залежностями (8), (9) та (11). При цьому під час шифрування кожної частини повідомлення Передавачу необхідно виконати згідно цих залежностей приблизно $k^2 - k$ додавань та $k^2 + 2k$ множень,

а Приймачу k^2-1 додавань та k^2+2k+2 множень над машинними одиницями інформації.

Визначено, що складність обчислень додавання за модулем складає приблизно 3(H+2)операцій, а множення за модулем − 6H(H+1) операцій. Враховуючи те, що під час реалізації криптографічних методів в сучасних комп'ютерних системах оперують ключами, що мають розмір 1024 і більше розрядів ($Hq \geq 1024$) і тому певними незначними оцінками можна знехтувати, отримаємо такі мінімальні та максимальні оцінки складності в машинних одиницях інформації для розглянутого протоколу шифрування інформації без попереднього розподілу ключів

$$S_{\min} = QH \cdot [12H(k^2+2k+1)+3(6k^2+7k+3)] + H \cdot [6H(5k^2+7k+2)+15(3k^2+2k+1)],$$

$$S_{\max} = QH \cdot [12H(k^2+2k+1)+3(6k^2+7k+3)] + 4H^2q \cdot [6H(k^2+k)+3(3k^2+k)].$$

Аналіз складності обчислень показав, що обчислення певного елементу U_k-послідовності має той же порядок, що і складність піднесення до заданого ступеня.

Здійснено порівняння отриманих оцінок складності представленого протоколу шифрування без попереднього розподілу ключів з аналогічними оцінками відомого протоколу шифрування Шаміра. При цьому для оцінювання відомого протоколу, зокрема для визначення оцінки складності операції піднесення до ступеня, використовувались оцінки складності алгоритмів виконання арифметичних операцій з великими числами за модулем, що і для представленого протоколу шифрування. В результаті оцінки складності для протоколу Шаміра мають такий вигляд

$$S_{Ш\min} = 24QH^2q(H+1),$$

$$S_{Ш\max} = 48QH^2q(H+1).$$

Аналіз отриманих оцінок показав, що максимальна оцінка складності представленого протоколу шифрування на основі V_k та U_k-послідовностей для $Q > 100$ приблизно у 10^2 разів менша ніж для відомого, а мінімальна оцінка менша ніж для відомого приблизно у 10^2 для q=16 та у 10^3 для q=32.

Проведено дослідження криптостійкості представленого методу шифрування без попереднього розподілу ключів на основі рекурентних послідовностей. Дослідження показало, що представлений метод має принаймні не менший рівень криптостійкості, що й відомий метод Шаміра.

Запропонований метод також дозволяє за допомогою параметру k змінювати складність виконання методу, встановлюючи таким чином необхідний рівень криптостійкості.

Висновок

Розглянуто рекурентні V_k- та U_k-послідовності та їх аналітичні залежності як математичний апарат, на основі якого представлено метод шифрування інформації без попереднього розподілу ключів. В методі відбувається заміна піднесення до ступеня обчисленням певного елементу U_k-послідовності.

Проведено оцінювання складності обчислень за цим методом і його теоретичної криптостійкості, а також порівняння отриманих оцінок з відомим методом Шаміра. Показано, що розглянутий метод має меншу складність обчислень для будь-якого k не менше ніж у 10^2 разів у порівнянні з відомим методом і при цьому забезпечує принаймні не менший рівень криптостійкості, що і відомий метод.

Крім того, запропонований метод дозволяє встановлювати необхідну криптостійкість в залежності від параметру k, тобто існує можливість збільшення криптостійкості із збільшенням цього параметру.

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ

1. *Menezes A.J., van Oorschot P.C., Vanstone S.A.* Handbook of Applied Cryptography. – CRC Press, 2001. – 816 p.

2. *Шнайер Б.* Прикладная криптография. Протоколы, алгоритмы, исходные тексты на языке Си. – М. : Триумф, 2002. – 816 с.

3. *Молдовян Н.А., Молдовян А.А.* Введение в криптосистемы с открытым ключом. – СПб. : БХВ-Петербург, 2005. – 288 с.

4. *Саломаа А.* Криптография с открытым ключом. – М. : Мир. – 1995. – 318 с.

5. *Месси Д.Л.* Введение в современную криптологию // ТИИЭР. – Т. 76. – № 5. – 1988. – С. 24–42.

6. *Маркушевич А.И.* Возвратные последовательности. – М . : Наука, 1975. – 48 с.

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

8. *Яремчук Ю.Є.* Метод асиметричного шифрування інформації на основі рекурентних послідовностей // Сучасна спеціальна техніка. – 2012, № 4. – С. 79–87.

9. *Кнут Д.* Искусство программирования для ЭВМ, том 2. Получисленные алгоритмы. – М. : Вильямс, 2004. – 832 с.

Отримано 15.02.2013