УДК 621.391.7

Ю.Є. Яремчук,
кандидат технічних наук, доцент

МЕТОД АСИМЕТРИЧНОГО ШИФРУВАННЯ ІНФОРМАЦІЇ НА ОСНОВІ РЕКУРЕНТНИХ ПОСЛІДОВНОСТЕЙ

У роботі розглянуто метод асиметричного шифрування інформації 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, рекурентні послідовності.*

В работе рассмотрен метод ассиметричного шифрования информации 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, рекуррентные последовательности.*

Paper considers the method of an asymmetric encryption of the information, based on the recurrent V_k^+ *and* U_k*-sequences and their relations. Method of the computational complexity and cryptologic reliability has been presented.*

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

На сьогодні проблема забезпечення інформаційної безпеки в комп'ютерних системах і мережах успішно вирішується завдяки використанню криптографічних методів в інформаційно-комунікаційних системах. При цьому вирішення завдання забезпечення конфіденційності інформації здійснюється за допомогою шифрування. Основною перевагою асиметричного шифрування [1, 2] перед симетричним [3, 4] є відсутність необхідності фізичного розподілу ключів секретним каналом зв'язку або наявності третьої сторони для реалізації цього.

Наявні на сьогодні методи асиметричного шифрування базуються на певному класі необоротних функцій, найбільш відомими з яких є обчислення логарифму в скінченному полі, розкладання великих чисел на прості множники, обчислення коренів алгебраїчних рівнянь, дискретне логарифмування на еліптичних кривих [5]. Стійкість методів базується на складності вирішення цих проблем для великих чисел. Однак необхідність виконувати обчислення з великими числами створює певні проблеми і для санкціонованого користувачу методу, вимагаючи при практичній його реалізації високого рівня обчислювальної техніки.

З огляду на це, актуальною є побудова асиметричних методів шифрування 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 асиметричних методів, що базуються на його основі.

Так, в роботі [7] запропоновано використовувати рекурентні послідовності Люка за модулем простого числа замість піднесення до степеня за модулем як це робили Діффі та Хеллман. У роботі [8] було вказано на певну слабкість такого підходу щодо криптографічної стійкості. Однак, незважаючи на це, актуальним залишається питання пошуку та дослідження таких послідовностей, які могли б стати основою математичного апарату, а також розробки більш стійких асиметричних методів на його основі.

Математичний апарат на основі рекурентних послідовностей для розробки методу шифрування

Рекурентні послідовності у 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_0, u_1, ... , 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 $n=l$. 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

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

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

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

З наведених аналітичних залежностей V_k^+-послідовності видно, що для довільного додатного номера 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 доцільним є використання саме великих значень індексу елементу послідовності. Виникає необхідність у більш швидкому методі обчислення елементу $v_{n,k}$.

У зв'язку з цим, пропонується спосіб обчислення $v_{n,k}$, який базується на тій самій ідеї, що і бінарний метод [9] піднесення до степеня. Скористаємось цим методом для отримання адитивного ланцюжка

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

Якщо записати n у 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 $c_t = n$.

Звідси, обчислення $v_{n,k}$ буде зводитись до послідовного обчислення $v_{c_i,k} = v_{2c_{i-1}+1,k}$ або $v_{c_i,k} = v_{2c_{i-1},k}$.

Обчислення $v_{c_i,k} = v_{2c_{i-1},k}$ будемо здійснювати за формулою (4), а $v_{c_i,k} = v_{2c_{i-1}+1,k}$ будемо отримувати, обчислюючи спочатку $v_{2c_{i-1},k}$, а потім $v_{2c_{i-1}+1,k}$ за формулою (1).

З (4) видно, що для отримання елементу $v_{2n,k}$ використовуються елементи $v_{n+k-2,k}, \ldots, v_{n-(k-2),k}, v_{n-(k-2),k}$. Тобто на кожному кроці необхідно визначати та зберігати набір з $2k - 2$ елементів. Розглянемо обчислення цих елементів.

Елементи $v_{2n,k}, v_{2n-1,k}, \ldots, v_{2n-(k-3),k}, v_{2n-(k-2),k}$ можуть бути обчислені за формулою (3) відповідно як $v_{n+n,k}, v_{n+(n-1),k}, \ldots, v_{n+(n-(k-3)),k}, v_{n+(n-(k-2)),k}$.

Елемент $v_{2n-(k-1),k}$ не може бути обчислений за формулою (3), оскільки для його обчислення, окрім елементів, які є в наведеному вище наборі, потрібен елемент $v_{n-k,k}$. Розширення цього набору елементів елементом $v_{n-k,k}$ не бажано, тому що для обчислення $v_{2n-k,k}$ буде потрібен елемент $v_{2n-(k+1),k}$. Щоб усунути цей недолік будемо обчислювати елемент $v_{2n-(k+1),k}$ за формулою (2).

У такому випадку необхідним є елемент $v_{2n+1,k}$. Цей елемент може бути обчислений за формулою (3). При цьому набір необхідних елементів буде розширений елементом $v_{n+k-1,k}$.

Елементи $v_{2n+k-1,k}, \ldots, v_{2n+3,k}, v_{2n+2,k}$ можуть бути отримані на основі вже обчислених елементів $v_{2n+k-1,k}, v_{2n,k}, \ldots, v_{2n-(k-3),k}, v_{2n-(k-2),k}$ за формулою (1).

Таким чином, для обчислення елементу $v_{2n,k}$ на кожному кроці необхідно визначати та зберігати набір з $2k - 1$ елементів.

Слід також відзначити, що в 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 асиметричного шифрування обчислення будуть виконуватись над числами великої розрядності.

Позначивши l як поточне значення індексу елементу V_k^+-послідовності, маємо такий алгоритм прискореного обчислення елементів цієї послідовності для додатних n.

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

П. 2. $i \leftarrow i-1$.

П. 3. $l \leftarrow 2l$.

П. 4. Обчислити нові значення $v_{l+1,k}$, $v_{l,k}$, ... , $v_{l-(k-3),k}$, $v_{l-(k-2),k}$ за модулем p, використовуючи (3).

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

П. 6. Якщо $k > 2$, то обчислити елементи $v_{l+k-1,k}$, $v_{l+k-2,k}$, ... , $v_{l+3,k}$, $v_{l+2,k}$ за модулем p, використовуючи (1).

П. 7. Якщо $\alpha_i = 0$, то перейти до п. 10.

П. 8. $l \leftarrow l+1$.

П. 9. Обчислити нові значення $v_{l+k-1,k}$, ... , $v_{l-(k-2),k}$, $v_{l-(k-1),k}$ шляхом присвоювання кожному попередньому елементу значення наступного за ним елементу та обчислення за модулем p останнього елементу $v_{l+k-1,k}$ за формулою (1), використовуючи тільки-но обчислені елементи.

П. 10. Якщо $i-1 \neq 0$, то перейти до п. 3, інакше завершити роботу алгоритму.

Таким чином, представлено, а також отримано аналітичні залежності та алгоритми 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

$$u_{n,k} = g_k u_{n-1,k} + g_1 u_{n-k,k} \tag{5}$$

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 $g_1, g_2, g_3, \dots, g_k$ – цілі числа; n і k – цілі додатні числа – U_k-послідовністю.

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

$$u_{n+m,k} = v_{m+(k-2),k} \cdot u_{n,k} + g_1 \cdot \sum_{i=1}^{k-1} v_{m+(k-2)-i,k} \cdot u_{n-k+i,k}. \tag{6}$$

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

$$u_{n,k} = g_k \cdot v_{n-1,k} + g_1 \cdot \sum_{i=1}^{k-1} g_i \cdot v_{n-i-1,k}. \tag{7}$$

Представлені рекурентні послідовності, а також отримані залежності дозволяють розробити метод асиметричного шифрування інформації на їх основі.

Метод шифрування інформації на основі рекурентних V_k^+ та U_k-послідовностей

Розглянемо метод шифрування, в якому для забезпечення необоротності перетворень пропонується використовувати аналітичну залежність (6). Необоротність згідно цієї залежності базується на тому, що 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 практично неможливо, тобто це є обчислювально складною задачею.

При цьому залежність (6), яка забезпечує можливість обчислення елементу $u_{n+m,k}$ використовуючи елементи V_k^+ та U_k-послідовностей, дозволяє зробити це 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 $u_{m-i,k}$, $i=\overline{0,k-1}$. Завдяки цьому можна розробити такий метод асиметричного 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.

З огляду на це, процедура асиметричного шифрування інформації може мати такий вигляд (рис. 1).

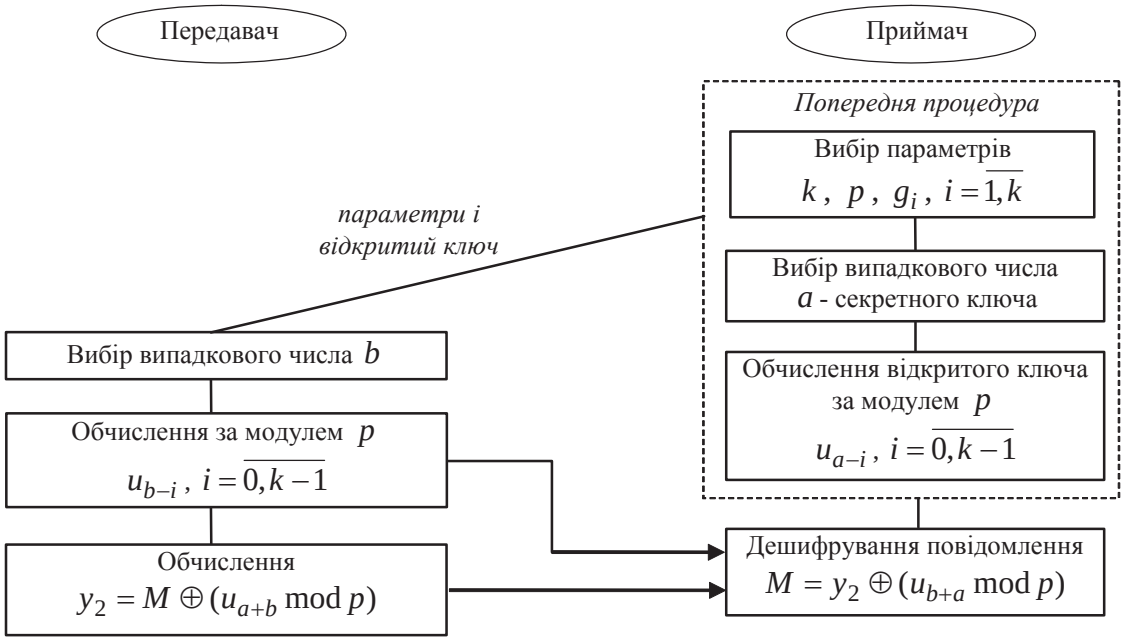

Рис. 1. Процедура асиметричного шифрування на основі елементів U_k-послідовностей

Операція за модулем в процедурі шифрування використовується для обмеження розрядності чисел, які використовуються в арифметичних операціях цієї процедури.

Обчислення елементів u_{a-i} та $i=\overline{0,k-1}$ для здійснюється за формулою (7) на основі елементів $v_{a+i,k}$ та $v_{b+i,k}$ для $i=\overline{-(k-1),k-2}$. Обчислення останніх може

здійснюватись за розглянутим вище алгоритмом прискореного обчислення елементів V_k^+-послідовності.

Визначивши необхідні залежності, процедуру та алгоритм обчислення елементів рекурентних послідовностей, протокол асиметричного шифрування інформації 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. Приймачу вибрати випадкове число a-секретний ключ.

П. 6. Приймачу обчислити $v_{a+i,k}$, $i = \overline{-(k-1), k-2}$, за модулем p, використовуючи алгоритм прискореного обчислення елементів V_k^+-послідовності.

П. 7. Приймачу обчислити $v_{a+i,k}$, $i = \overline{-2k+1, -k}$, за модулем p, використовуючи залежність (2) та дані отримані в п. 6.

П. 8. Приймачу обчислити відкритий ключ $u_{a-i,k}$, $i = \overline{0, k-1}$, за модулем p, використовуючи залежність (7) та дані, отримані в пп. 6, 7.

П. 9. Приймачу опублікувати відкритий ключ.

П. 10. Передавачу вибрати випадкове число b − секретний ключ.

П. 11. Передавачу обчислити $v_{b+i,k}$, $i = \overline{-(k-1), k-2}$, за модулем p, використовуючи алгоритм прискореного обчислення елементів V_k^+-послідовності.

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

П. 13. Передавачу обчислити $u_{b-i,k}$, $i = \overline{0, k-1}$, за модулем p, використовуючи залежність (7) та дані, отримані в пп. 11, 12.

П. 14. Передавачу зашифрувати повідомлення M за формулою

$$y_2 = M \oplus (u_{a+b,k} \bmod p),$$

де $u_{a+b,k}$ обчислюється, використовуючи залежність (6).

П. 15. Передавачу передати обчислені $u_{b-i,k}$, $i = \overline{0, k-1}$, а також y_2 Приймачу.

П. 16. Приймачу дешифрувати повідомлення M за формулою

$$M = y_2 \oplus (u_{b+a,k} \bmod p),$$

де $u_{b+a,k}$ обчислюється, використовуючи залежність (6).

У п. 2 протоколу 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 протоколу відбувається вибір параметрів g_i, $i = \overline{1, k}$. 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.

Параметр k, крім того, що визначає кількість початкових елементів рекурентних V_k^+ та U_k-послідовностей, ще й впливає на складність обчислень згідно аналітичної залежності (3) в алгоритмі прискореного обчислення елементів V_k^+-послідовності та згідно залежностей (6), (7) в методі асиметричного

шифрування інформації. Вплив відбувається таким чином, що чим більше параметр k, тим більше складність обчислень за цим методом.

Визначимо тепер обчислювальну складність представленого протоколу асиметричного шифрування інформації.

Основні обчислення в протоколі Приймач виконує у пп. 6–8, 16, а Передавач в пп. 11–14. При цьому, крім операцій додавання, віднімання та множення, Передавач і Приймач відповідно в пунктах 14 та 16 виконують операцію виключне АБО.

Складність виконання п. 6 з боку Приймача, як і п. 11 з боку Передавача, визначається складністю прискореного обчислення елементів $v_{n+i,k}$ для $i=\overline{-(k-1),k-2}$, для додатних значень n.

Оскільки повідомлення M зазвичай розбивають на певне число Q частин $M_1, M_2, ..., M_Q$ фіксованого розміру, кожна з яких шифрується окремо, то Передавач буде виконувати разів пункти 11–14, а Приймач – п. 16. Отже, в Q разів зросте і складність виконання вказаних пунктів.

Не важко помітити, що Передавач і Приймач виконують за алгоритмом прискореного обчислення елементів V_k^+-послідовності однакову кількість арифметичних операцій над великими числами. Складність обчислень за алгоритмом прискореного обчислення елементів V_k^+-послідовності на прикладі Приймача 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 (7), та елементу $u_{b+a,k}$ за формулою (6). Обчислення першого набору елементів буде складати приблизно $H^2q\cdot[6H(k^2+k)+3(3k^2+k)]$ 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), (6) та (7) 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, складність обчислень за формулами (2), (6) та (7) буде складати приблизно $6H(H+1)(k^2+4k)+2Hk^2(H+1)+3Hk(H+1)$ операцій над машинними одиницями інформації. З огляду на те, що під час 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 у загальній оцінці складності всього протоколу асиметричного шифрування.

Враховуючи вищесказане, отримано такі мінімальні та максимальні оцінки складності для розглянутого протоколу асиметричного шифрування, які представлено як кількість операцій над машинними одиницями інформації

$$S_{\min}=QH\cdot[12H(k^2+3k+1)+18k^2+39k+8]+3Hk\cdot[4H(k+2)+6k+7],$$
$$S_{\max}=QH^2q\cdot[6H(k^2+k)+3(3k^2+k)]+H^2q\cdot[6H(k^2+k)+3(3k^2+k)].$$

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

Для порівняння отриманих оцінок складності представленого протоколу асиметричного шифрування з аналогічними оцінками відомого протоколу асиметричного шифрування за аналог взято протокол шифрування Ель-Гамаля. При цьому для оцінювання відомого протоколу використовувались оцінки складності алгоритмів виконання арифметичних операцій з великими числами за модулем, що і для представленого протоколу шифрування. У результаті оцінки складності мають такий вигляд

$$S_{E\Gamma\min} = 18QH^2q(H+1) + 6H^2q(H+1),$$
$$S_{E\Gamma\max} = 36QH^2q(H+1) + 12H^2q(H+1).$$

Аналіз отриманих оцінок показує, що мінімальна оцінка складності представленого протоколу асиметричного шифрування для $Q > 100$ менша ніж для відомого приблизно у 10^2 разів. При цьому максимальна оцінка складності представленого протоколу для $Q > 100$ майже збігається з відомим для k=2 і більша ніж відомого приблизно у 300 разів для k=3. Оскільки для k=2 мінімальна оцінка набагато менша, а максимальна збігається, то можна очікувати, що середня оцінка представленого протоколу асиметричного шифрування буде меншою ніж для відомого для цього значення порядку послідовності.

Проведено дослідження криптостійкості представленого методу асиметричного шифрування на основі рекурентних послідовностей. Дослідження показало, що представлений метод має такий самий рівень криптостійкості, що й відомі аналоги і метод Ель-Гамаля зокрема.

Висновки

Розглянуто рекурентні V_k^+ та U_k-послідовності, а також отримано залежності для цих послідовностей, на основі яких запропоновано метод асиметричного шифрування інформації.

Проведено оцінювання складності обчислень за цим методом і його теоретичної криптостійкості, а також порівняння отриманих оцінок з відомим методом Ель-Гамаля. Показано, що розглянутий метод має за певних умов меншу складність обчислень у порівнянні з відомим методом і при цьому забезпечує такий самий рівень криптостійкості, як і відомий метод. Крім того, запропонований метод дозволяє встановлювати необхідну криптостійкість у залежності від параметру k, тобто існує можливість збільшення криптостійкості із збільшенням цього параметру.

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ

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

2. *Саломаа А.* Криптография с открытым ключом / А. Саломаа ; пер. с англ. – М. : Мир, 1995. – 318 с.

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

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

5. *Харин Ю.С.* Математические и компьютерные основы криптологии : учеб. пособ. / Ю.С. Харин, В.И. Берник, Г.В. Матвеев, С.В. Агиевич. – Мн. : Новое знание, 2003. – 382 с.

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

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

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

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

Отримано 10.12.2012