



ДЕРЖАВНА СЛУЖБА
ІНТЕЛЕКТУАЛЬНОЇ
ВЛАСНОСТІ
УКРАЇНИ

УКРАЇНА

(19) **UA** (11) **86734** (13) **U**
(51) МПК (2013.01)
H03M 13/00

(12) ОПИС ДО ПАТЕНТУ НА КОРИСНУ МОДЕЛЬ

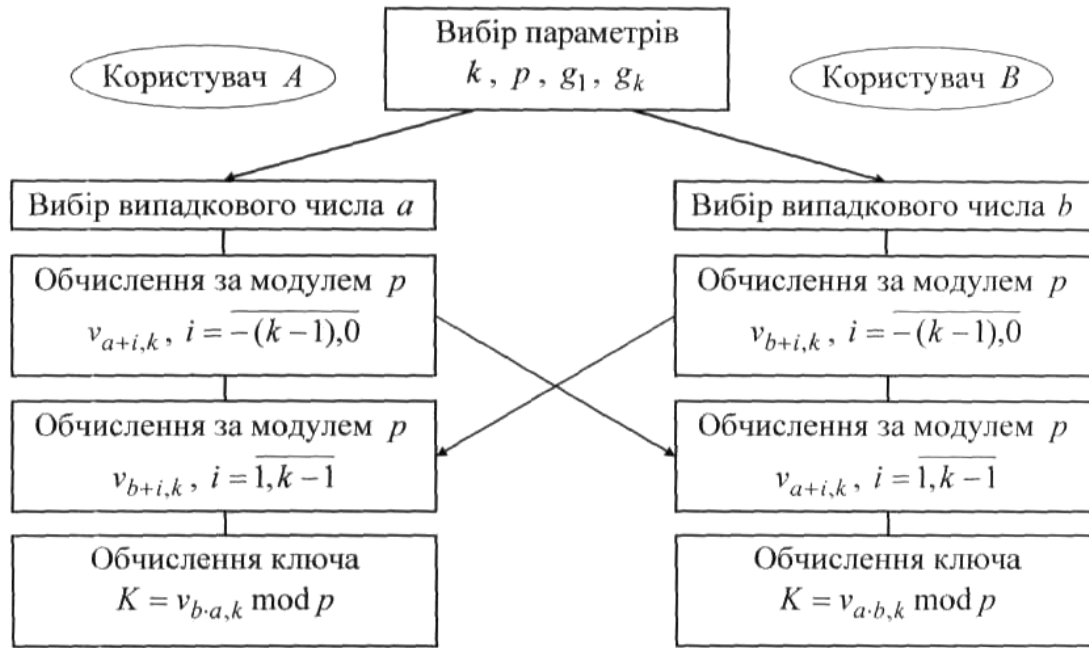
(21) Номер заявки:	u 2013 08385	(72) Винахідник(и):	Яремчук Юрій Євгенович (UA)
(22) Дата подання заявки:	04.07.2013	(73) Власник(и):	Яремчук Юрій Євгенович,
(24) Дата, з якої є чинними права на корисну модель:	10.01.2014		вул. Воїнів-Інтернаціоналістів, 9-а/ 63, м. Вінниця, 21021 (UA)
(46) Публікація відомостей про видачу патенту:	10.01.2014, Бюл.№ 1		

(54) СПОСІБ ВІДКРИТОГО РОЗПОДІЛУ СЕКРЕТНИХ КЛЮЧІВ У ВИГЛЯДІ ЕЛЕКТРОННОГО КОДУ НА ОСНОВІ РЕКУРЕНТНИХ ПОСЛІДОВНОСТЕЙ

(57) Реферат:

Спосіб відкритого розподілу секретних ключів у вигляді електронних кодів на основі рекурентних послідовностей включає відкритий канал передавання інформації у вигляді електронних кодів двох користувачів, вибір параметру k , вибір параметру p та $p > 2$, вибір g_1, g_k , публікацію параметрів, вибір користувачем А випадкового числа a , $1 < a < p$, а користувачем В випадкового числа b , $1 < b < p$, користувачем А обчислюється за модулем p $v_{a+i,k}$, $i = \overline{-(k-1), 0}$, а користувачу В обчислити за модулем p $v_{b+i,k}$, $i = \overline{-(k-1), 0}$, використовуючи спосіб прискореного обчислення елементів $v_{n,k}$ для додатних значень n , після чого передати один одному обчислені елементи, користувачем А обчислюється за модулем p $v_{b+i,k}$, $i = \overline{1, k-1}$, користувачем В обчислюється за модулем p $v_{a+i,k}$, $i = \overline{1, k-1}$, використовуючи формулу $v_{n,k} = g_k v_{n-1,k} + g_1 v_{n-k,k}$, користувачами А і В обчислюється спільний ключ K відповідно як $K = v_{b \cdot a, k} \bmod p$ та $K = v_{a \cdot b, k} \bmod p$, використовуючи спосіб прискореного обчислення елементів $v_{n \cdot m, k}$.

UA 86734 U



Корисна модель належить до техніки криптографічного захисту інформації і може використовуватися в системах захисту інформації, комп'ютерних мережах, банківських та електронних платіжних системах, системах стільникового зв'язку та інших інформаційно-обчислювальних і телекомунікаційних системах.

Відомий спосіб відкритого розподілу секретних ключів у вигляді електронних кодів, що базується на використанні операції піднесення до степеня великих чисел за модулем (W. Diffie, M.E. Hellman. New directions in cryptography // IEEE Transactions on Information Theory. - № 22, 1976. - P. 644-654).

Суть способу полягає в тому, що спочатку центр довіри (або користувач А чи користувач В) вибирає і відкрито публікує просте число p та ціле число g , $2 \leq g \leq p-2$. Під час безпосереднього розподілу ключів користувач А вибирає випадкове число a , $1 \leq a \leq p-2$, а користувач В вибирає випадкове число b , $1 \leq b \leq p-2$. Потім користувач А обчислює $g^a \bmod p$ і передає його користувачу В, а користувач В обчислює $g^b \bmod p$ і передає його користувачу А. Після цього користувачі А і В отримують спільний секретний ключ K відповідно як $K = (g^b)^a \bmod p$ та $K = (g^a)^b \bmod p$.

Стійкість способу базується на складності вирішення задачі дискретного логарифмування. Обчислювальна складність способу в основному визначається складністю виконання операцій піднесення до степеня великого числа за модулем. Всього, згідно зі способом, необхідно виконати чотири таких операції - по два на кожному боці.

Відомий спосіб відкритого розподілу секретних ключів у вигляді електронних кодів, що базується на використанні математичного апарату рекурентних послідовностей (P. Smith, M. Lennon, LUC: A new public-key system, Proceedings of the IFIP TC11, Nintli International Conference on Information Security: Computer Security, Toronto, May, 12-14, 1993. - P. 103-117).

Суть способу (його іноді називають LUCDIF) полягає у використанні рекурентної функції Люка і заміні піднесення до степеня за модулем, як це робиться в способі Діффі-Хеллмана, на обчислення елемента рекурентної послідовності Люка за модулем простого числа p з певним індексом.

В способі використовуються рекурентні послідовності $\{T_n\}$, що отримуються з лінійного рекурентного співвідношення другого порядку такого вигляду.

$$T_n = P \cdot T_{n-1} - Q \cdot T_{n-2} \quad (1)$$

де P і Q взаємно прості числа.

Серед набору послідовностей $\{T_n\}$, що породжуються рекурентним співвідношенням (1), виділяють послідовності $\{c_1 \alpha^n + c_2 \beta^n\}$, де c_1 і c_2 - будь-які числа, із значеннями початкових елементів $T_0 = c_1 + c_2$ та $T_1 = c_1 \alpha + c_2 \beta$.

Спосіб базується на математичному апараті конкретного представника цієї послідовності, який позначається $\{V_n\}$ і визначається таким чином:

$$V_n = \alpha^n + \beta^n, \text{ відповідно } c_1 = 1 = c_2.$$

Це є послідовність цілих чисел, оскільки її початкові елементи приймають такі значення $V_0 = 2$, $V_1 = P$.

Ці послідовності залежать тільки від цілих чисел P і Q , а функції, що їм відповідають, називають функціями Лука P і Q . Іноді їх записують як $V_n(P, Q)$, щоб підкреслити їхню залежність від P і Q .

Для цієї послідовності отримано таку аналітичну залежність:

$$V_{n \cdot k}(P, 1) = V_n(V_k(P, 1), 1) \quad (2)$$

Основу способу складає залежність (2), яка дозволяє обчислювати елементи $V_n(P, Q)$ - послідовності різними шляхами.

Згідно зі способом, на основі даного математичного апарату спочатку центр довіри (або один із користувачів) вибирає та відкрито публікує просте число p , а також число g , що задовольняє такий властивості.

$$\left(\frac{g}{p}\right) = -1 \text{ and } k/(p+1), \quad V_k(g, 1) \equiv 2 \bmod p \Rightarrow k = p+1$$

Під час безпосереднього розподілу ключів користувачі вибирають випадкові числа a і b , обчислюють відповідно $V_a(g, 1) \bmod p$ та $V_b(g, 1) \bmod p$ та передають ці значення один одному. Після цього вони обчислюють кожен на своєму боці спільний ключ K , використовуючи залежність (2), як

$$K = V_b(V_a(g, 1) \bmod p, 1) \bmod p = V_a(V_b(g, 1) \bmod p, 1) \bmod p.$$

Стійкість способу базується на складності обчислення індексу рекурентної $V_n(P, Q)$ - послідовності з обчисленого елемента цієї послідовності. Ця задача за обчислювальною складністю є аналогом задачі дискретного логарифмування, тому спосіб має схожі характеристики із способом Діффі-Хеллмана. Перевагою способу може бути те, що його стійкість не залежить від спроб криптоаналізу, які існують в задачах дискретного логарифмування.

Відомий спосіб відкритого розподілу секретних ключів у вигляді електронних кодів, в основі якого використовується математичний апарат рекурентних послідовностей, що базуються на співвідношеннях, в яких початкові елементи пов'язані з коефіцієнтами (Яремчук Ю.Є. Використання рекурентних послідовностей для побудови криптографічних методів з відкритим ключем // Захист інформації. - №4, 2012. - С. 120-127). (найближчий аналог).

Суть способу полягає у використанні залежностей рекурентних послідовностей і заміні піднесення до степеня за модулем, як це робиться в способі Діффі-Хеллмана, на обчислення елемента рекурентної U_k - послідовності з певним індексом.

U_k - послідовність визначається рекурентним співвідношенням.

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

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

Елементи U_k - послідовності можуть обчислюватись через елементи V_k^+ - послідовності, яка визначається таким рекурентним співвідношенням.

$$V_{n,k} = g_k V_{n-1,k} + g_1 V_{n-1,k} \quad (4)$$

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

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

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

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.

$$U_{n,k} = g_k \cdot v_{n-1,k} + g_1 \cdot \sum_{i=1}^{k-1} g_i \cdot v_{n-i-1,k} \quad (6)$$

Спосіб відкритого розподілу ключів базується на використанні аналітичної залежності (5), яка дозволяє обчислити елемент $u_{n+m,k}$ використовуючи елементи V_k^+ та U_k - послідовностей, причому 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 $u_{m-i,k}, i = \overline{0, k-1}$.

Згідно зі способом, під час безпосереднього розподілу ключів один користувач для будь-якого вибраного ним випадкового числа a обчислює $u_{a-i,k} \bmod p, i = \overline{0, k-1}$, а другий користувач аналогічним чином обчислює $u_{b-i,k} \bmod p, i = \overline{0, k-1}$, і, обмінявшись обчисленими значеннями, кожен з них отримує ключ K як $u_{b+a,k} \bmod p$ та $u_{a+b,k} \bmod p$, продовжуючи обчислення на своєму боці за формулою (5), використовуючи відповідно свої числа a та b . При цьому значення ключа K є ключем розподілу, а числа a і b секретним ключем кожного користувача, причому a і b - це частини секретного ключа кожного користувача, оскільки попереднє отримання ключа розподілу будь-яким користувачем не можливе без отримання відповідної інформації від іншого користувача.

Стійкість способу базується на складності вирішення задачі отримання індексу елемента рекурентної послідовності, обчисленого за модулем. Ця задача за рівнем складності

знаходиться приблизно на тому ж рівні, що і задача отримання числа степеня з результату модулярного піднесення до степеня, на якій базується стійкість способу Діффі-Хеллмана.

Обчислювальна складність способу в основному визначається складністю обчислення за модулем елементу U_k - послідовності із заданим індексом. Рівень складності цих обчислень є приблизно таким же, що і рівень складності операції піднесення до степеня за модулем, на якому базується спосіб Діффі-Хеллмана.

Виходячи з цього, спосіб розподілу ключів на основі U_k - послідовностей майже у два рази є більш швидким, ніж спосіб Діффі-Хеллмана, оскільки згідно першого способу необхідно виконувати два складних обчислення (по одному на кожному боці) елементу U_k - послідовності для заданих індексів, що представляються великими числами, замість чотирьох піднесення до степеня великого числа згідно способу Діффі-Хеллмана.

Також перевагою способу на основі U_k - послідовностей є те, що в ньому забезпечується можливість збільшення стійкості пропорційно порядку k рекурентних послідовностей, що лежать в основі ключового розподілу, а також спрощення процедури завдання параметрів.

Однак існують задачі, в яких дуже важливою є проблема забезпечення високого рівня стійкості криптографічних перетворень під час розподілу ключів. Це може бути навіть більш актуальним, ніж вирішення проблеми підвищення швидкості процедури розподілу ключів. В першу чергу, це стосується задач в системах захисту з підвищеним рівнем секретності. В цьому зв'язку, спосіб розподілу ключів на основі U_k - послідовностей, хоч і забезпечує достатній рівень криптографічної стійкості, але має потенційні можливості підвищення стійкості для відповідних систем захисту, оскільки отримання спільного ключа K на завершальному етапі розподілу здійснюється за допомогою аналітичної залежності обчислення елементу послідовності з адитивною, а не мультиплікативною зміною індексу, що могло б значно підвищити стійкість криптографічних перетворень під час розподілу ключів.

В основу корисної моделі поставлено задачу створення способу відкритого розподілу секретних ключів у вигляді електронних кодів, в якому за рахунок використання в основі розподілу ключів математичного апарату тільки рекурентних V_k^+ - послідовностей та їх залежностей, досягається можливість підвищення стійкості криптографічних перетворень під час розподілу ключів.

Поставлена задача вирішується тим, що використання для розподілу ключів математичного апарату тільки на основі рекурентних V_k^+ - послідовностей забезпечує можливість користувачам на завершальному етапі розподілу обчислювати спільний ключ як результат обчислень елементу цієї послідовності за мультиплікативним способом зміни індексу. Оскільки отримання зловмисником складових частин індексу елемента послідовності обчисленого таким чином є більш складним, ніж отримання складових індексу елемента послідовності обчисленого за адитивним способом зміни індексу, це дасть можливість підвищити стійкість перетворень розподілу ключів.

В основі способу пропонується використовувати таку аналітичну залежність V_k^+ - послідовності: для будь-яких цілих додатних n , m та k .

$$U_{n+m,k} = V_{m+(k-2),k} \cdot V_{n,k} + g_1 \cdot \sum_{i=1}^{k-1} V_{m+(k-2)-i,k} \cdot V_{n-k+i,k} \quad (7)$$

Залежність (7) дозволяє обчислювати елемент $v_{n+m,k}$ на основі двох наборів елементів V_k^+ - послідовності: $v_{n+i,k}$, $i = \overline{(k-1),0}$ та $v_{m+i,k}$, $i = \overline{-1,k-2}$.

Суть способу відкритого розподілу секретних ключів у вигляді електронних кодів, що пропонується, базується на використанні властивості (7) V_k^+ - послідовності, яка забезпечує можливість організувати процедури прискореного обчислення елементів V_k^+ - послідовності для великих значень індексів, а саме процедури прискореного обчислення елементів $v_{n,k}$ та $v_{n+m,k}$.

Спочатку центр довіри (або користувач А чи користувач В) вибирає і відкрито публікує ціле додатне число p ($p > 2$) та цілі числа g_1 , g_k .

Під час безпосереднього розподілу ключів користувач А вибирає випадкове число a , $1 < a < p$, а користувач В вибирає випадкове число b , $1 < b < p$, Потім користувач А обчислює за модулем p ; $v_{a+i,k}$, $i = \overline{-(k-1),0}$, а користувач В - за модулем p $v_{b+i,k}$, $i = \overline{-(k-1),0}$, після чого вони обмінюються

обчисленими значеннями. Далі користувачі А і В розширюють отриманий один від одного набір елементів, використовуючи формулу (4), обчислюючи за модулем p відповідно набори елементів $v_{h+i, k}$, $i = \overline{1, k-1}$, та $v_{a+i, k}$, $i = \overline{1, k-1}$. Після цього вони обчислюють спільний ключ K відповідно як $K = v_{b \cdot a, k} \bmod p$ та $K = v_{a \cdot b, k} \bmod p$, використовуючи свої секретні числа a і b .

5 Загальна схема способу відкритого розподілу секретних ключів у вигляді електронних кодів

на основі математичного апарату рекурентних v_k^+ - послідовностей, що пропонується, буде мати вигляд представлений на фігурі 1.

Протокол розподілу секретних ключів у вигляді електронних кодів згідно з цим способом буде мати такий вигляд.

10 Крок 1. Задати параметр k .

Крок 2. Вибрати p , $p > 2$.

Крок 3. Вибрати g_1 , g_k .

Крок 4. Опублікувати параметри.

15 Крок 5. Користувачу А вибрати випадкове число a , $1 < a < p$, а користувачу В вибрати випадкове число b , $1 < b < p$.

Крок 6. Користувачу А обчислити за модулем p $v_{a+i, k}$, $i = \overline{-(k-1), 0}$, а користувачу В обчислити за модулем p $v_{b+i, k}$, $i = \overline{-(k-1), 0}$, використовуючи спосіб прискореного обчислення елементів $v_{n, k}$ для додатних значень n , після чого передати один одному обчислені елементи.

Крок 7. Користувачу А обчислити за модулем p $v_{h+i, k}$, $i = \overline{1, k-1}$, а користувачу В обчислити за модулем p $v_{a+i, k}$, $i = \overline{1, k-1}$, використовуючи формулу (4).

20 Крок 8. Користувачам А і В обчислити спільний ключ K відповідно як $K = v_{b \cdot a, k} \bmod p$ та $K = v_{a \cdot b, k}$, використовуючи спосіб прискореного обчислення елементів $v_{n \cdot m, k}$.

25 Технічний результат: підвищено стійкість та достовірність процедури відкритого розподілу секретних ключів, що дає можливість розширення галузі використання таких способів розподілу ключів, в першу чергу, в системах захисту з підвищеним рівнем секретності.

ФОРМУЛА КОРИСНОЇ МОДЕЛІ

30 Спосіб відкритого розподілу секретних ключів у вигляді електронних кодів на основі рекурентних послідовностей, що включає відкритий канал передавання інформації у вигляді електронних кодів двох користувачів, які бажають отримати за допомогою відкритого каналу спільний секретний ключ у вигляді електронного коду на основі секретних частин у вигляді електронних кодів кожного користувача, який **відрізняється** тим, що для отримання спільного ключа у вигляді електронного коду використовують обчислення елементів рекурентних послідовностей з заданим індексом, а саме рекурентної v_k^+ - послідовності, яка визначається як послідовність чисел, що обчислюються за формулою $v_{n, k} = g_k v_{n-1, k} + g_1 v_{n-k, k}$ для початкових значень $v_{0, k} = 1$, $v_{1, k} = g_2$ для порядку послідовності $k = 2$; $v_{0, k} = v_{1, k} = \dots = v_{k-3, k} = 0$, $v_{k-2, k} = 1$, $v_{k-1, k} = g_k$ для $k > 2$; де g_1 , g_k - цілі числа, n і k - цілі додатні числа, елементи v_k^+ - послідовності $v_{n \cdot m, k}$ для будь-яких цілих додатних n та m розраховуються за формулою

40 $u_{n \cdot m, k} = v_{m \cdot (k-2), k} \cdot u_{n, k} + g_1 \cdot \sum_{i=1}^{k-1} v_{m \cdot (k+2)-i, k} \cdot u_{n-k+i, k}$, елементи v_k^+ - послідовності $v_{n \cdot m, k}$ для будь-яких

цілих n та m обчислюються за допомогою способу прискореного обчислення цих елементів з використанням бінарного способу розкладання індексу m та формули обчислення елементів $v_{n \cdot m, k}$, при цьому розподіл секретного ключа відкритим каналом у вигляді електронного коду відбувається таким чином: спочатку центр довіри (або користувач А чи користувач В) виконує попередню процедуру вибору параметрів, для цього він вибирає параметр p як ціле додатне число, $p > 2$, яке потім використовується як модуль під час обчислень елементів v_k^+ - послідовності, вибирає цілі числа g_1 , g_k і відкрито публікує їх разом з параметром p , під час безпосереднього розподілу ключа користувач А вибирає випадкове число a , $1 < a < p$, а користувач В вибирає випадкове число b , $1 < b < p$, потім користувач А обчислює за модулем p $v_{a+i, k}$, $i = \overline{-(k-1), 0}$, а користувач В обчислює за модулем p $v_{b+i, k}$, $i = \overline{-(k-1), 0}$, за допомогою способу прискореного обчислення елементів $v_{n, k}$ з використанням бінарного способу розкладання індексу n та формули обчислення елементів $v_{n \cdot m, k}$, після чого користувачі А і В

- передають один одному обчислені елементи і розширюють отриманий один від одного набір елементів за допомогою формули, що визначає рекурентну v_k^+ - послідовність, тобто користувач А таким чином обчислює за модулем p ; елементи $v_{h+i,k}$, $i = \overline{1, k-1}$, а користувач В обчислює за модулем p елементи $v_{a+i,k}$, $i = \overline{1, k-1}$ на завершення користувачі А і В обчислюють спільний ключ K у вигляді електронного коду відповідно як $K = v_{b \cdot a, k} \bmod p$ та $K = v_{a \cdot b, k} \bmod p$ за допомогою способу прискореного обчислення елементів $v_{n \cdot m, k}$ на основі відповідно своїх секретних чисел a і b та отриманих і обчислених за модулем p розширених наборів елементів відповідно $v_{h+i,k}$, $i = \overline{-(k-1), k-1}$, та $v_{a+i,k}$, $i = \overline{-(k-1), k-1}$.

