



ДЕРЖАВНА СЛУЖБА
ІНТЕЛЕКТУАЛЬНОЇ
ВЛАСНОСТІ
УКРАЇНИ

УКРАЇНА

(19) **UA** (11) **86735** (13) **U**
(51) МПК (2013.01)
H03M 13/00

(12) ОПИС ДО ПАТЕНТУ НА КОРИСНУ МОДЕЛЬ

(21) Номер заявки:	u 2013 08386	(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 ШИФРУВАННЯ ІНФОРМАЦІЇ З ВІДКРИТИМ КЛЮЧЕМ У ВИГЛЯДІ ЕЛЕКТРОННОГО КОДУ НА ОСНОВІ РЕКУРЕНТНИХ ПОСЛІДОВНОСТЕЙ

(57) Реферат:

Спосіб шифрування інформації з відкритим ключем у вигляді електронного коду на основі рекурентних послідовностей, що включає відкритий канал передавання інформації у вигляді електронного коду, відправника, який шифрує відкрите повідомлення у вигляді електронного коду, та одержувача, який відновлює відкрите повідомлення із зашифрованого, секретний ключ одержувача у вигляді електронного коду та обчислений на його основі відкритий ключ, який відрізняється тим, що для шифрування інформації у вигляді електронного коду використовують обчислення елементів рекурентних послідовностей з заданим індексом.

UA 86735 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 шифрування інформації з відкритим ключем у вигляді електронного коду, що базується на використанні операції піднесення до степеня великих чисел за модулем [ElGamal T.A public key cryptosystem and a signature scheme based on discrete logarithms // IEEE Intern. Symp. Informat. Theory. V.IT-31. - 1985. - № 4. - P. 469-472].

Суть способу полягає в тому, що спочатку на попередньому етапі центр довіри (або приймач) вибирає і відкрито публікує просте число p та ціле число g , $g < p$. Потім він вибирає випадкове число a , $1 \leq a \leq p-2$, як секретний ключ та обчислює відкритий ключ $g^a \bmod p$, який передається разом з параметрами одержувачу. Після цього шифрування інформації відбувається таким чином.

Коли передавач хоче зашифрувати повідомлення M і надіслати його одержувачу, він спочатку генерує випадкове число b , $1 \leq b \leq p-2$, обчислює $g^b \bmod p$, потім отримує зашифроване повідомлення M' як $M' = M \oplus (g^a)^b \bmod p$, де \oplus позначає порозрядне виключне АБО, та передає отримані значення $g^b \bmod p$ та M' одержувачу.

Отримавши ці значення, одержувач дешифрує повідомлення M' , обчислюючи відкрите повідомлення M як $M = M' \oplus (g^b)^a \bmod p$.

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 способу необхідно виконати чотири таких операцій - по два на кожному боці.

Відомий спосіб шифрування інформації з відкритим ключем у вигляді електронного коду, що базується на використанні математичного апарату рекурентних послідовностей (P. Smith, M. Lennon, LUC: A new public-key system, Proceedings of the IFIP TCII, Ninth International Conference on Information Security: Computer Security, Toronto, May 12-14, 1993, P. 103-117).

Суть способу (його іноді називають LUCELG PK) полягає у використанні рекурентної функції Люка і заміні піднесення до степеня за модулем, як це робиться в способі Ель-Гамала, 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 $V_0 = 2$, і $V_1 = P$.

Ця послідовність залежить 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:

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

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

Згідно способу на попередньому етапі шифрування центр довір або одержувач генерує та публікує просте число p , при цьому $p+1$ не повинно бути складеним лише з малих простих чисел, використовуючи такий генератор, для якого $V_{(p+1)/t}(\lambda, 1) \neq 2 \bmod p$ для кожного $t > 1$, що ділить $(p+1)$. Потім він вибирає випадкове число $x < p$ як секретний ключ та отримує відкритий ключ y як $y \equiv V_x(\lambda, 1) \bmod p$, який публікує. Після цього шифрування інформації реалізується таким чином.

Коли відправник бажає зашифрувати повідомлення M , $0 < M < p$ або поділене на блоки такого розміру, і передати його одержувачу, він спочатку вибирає випадковим чином своє секретне число k , $0 < k < p$, для кожного повідомлення M або блоку повідомлення та обчислює G як $G \equiv V_k(y, 1) \bmod p$. Потім обчислюються дві частини криптограми як $d_1 \equiv V_k(\lambda, 1) \bmod p$ та $d_2 \equiv GM \bmod p$.

Під час дешифрування криптограм і отримання відкритого повідомлення M одержувач спочатку обчислює G як $G \equiv V_x(d_1, 1) \bmod p$, використовуючи аналітичну залежність (2) та свій секретний ключ x , а мультиплікативно обернене значення G , тобто G^{-1} , за модулем p одержувач може обчислити, використовуючи розширений алгоритм Евкліда, в результаті повідомлення M відновлюють за допомогою залежності (2) як $M \equiv d_2(G^{-1}) \bmod p$.

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

Відомий спосіб шифрування інформації з відкритим ключем у вигляді електронного коду, в основі якого використовується математичний апарат рекурентних послідовностей, що базуються на співвідношеннях, в яких початкові елементи пов'язані з коефіцієнтами (Яремчук Ю.Є. Криптографічні методи та засоби шифрування інформації на основі рекурентних послідовностей. Монографія. - Вінниця: "Книга-Вега". - 2002. - 136 с.). (найближчий аналог)

Суть способу полягає у використанні залежностей рекурентних послідовностей і заміні піднесення до степеня за модулем, як це робиться в способі Ель-Гамала, на обчислення елементу 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 $u_{0,k} = g_1$, $u_{1,k} = g_2$, $u_{2,k} = g_3$, ..., $u_{k-1,k} = g_k$; 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

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

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

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

- 5 Спосіб шифрування інформації з відкритим ключем у вигляді електронного коду 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 $u_{m-i,k}$, $i = \overline{0, k-1}$.
- 10 Згідно цього способу шифрування центр довіри або одержувач вибирає параметри: k - порядок послідовності, p - модуль, що використовується для обмеження великих чисел під час обчислень, а також коефіцієнти g_i , $i = \overline{1, k}$, рекурентного співвідношення. Потім він випадковим чином вибирає секретний ключ a і обчислює відкритий ключ $u_{a-i,k} \bmod p$, $i = \overline{0, k-1}$, який публікує.
- 15 Коли відправник бажає зашифрувати повідомлення M і передати його одержувачу, він спочатку вибирає випадкове число b та обчислює за модулем p $u_{b-i,k}$, $i = \overline{0, k-1}$. Потім він обчислює $u_{a+b,k} \bmod p$ за допомогою залежності (5) і отримує зашифроване повідомлення M' як результат виключного АБО $u_{a+b,k} \bmod p$ з відкритим повідомленням M , тобто $M' = M \oplus (u_{a+b,k} \bmod p)$, та передає одержувачу M' та $u_{b-i,k} \bmod p$, $i = \overline{0, k-1}$.
- 20 Під час дешифрування повідомлення M одержувач спочатку за допомогою свого секретного ключа a обчислює за модулем p $u_{b+a,k} \bmod p$, а потім дешифрує відкрите повідомлення, як результат виключного АБО $u_{b+a,k} \bmod p$ з M' , тобто $M = M' \oplus (u_{b+a,k} \bmod p)$.
- 25 Сстійкість 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 Ель-Гамала.
- 30 Обчислювальна складність способу в основному визначається складністю обчислення за модулем елемента 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 Ель-Гамала.
- 35 Аналіз обчислювальної складності способу шифрування з відкритим ключем у вигляді електронного коду на основі U_k -послідовності показує, що коли порядок послідовності $k=3$ він є більш складним, ніж спосіб Ель-Гамала. Однак, оскільки для $k=2$ мінімальна оцінка способу є на багато меншою, а максимальна оцінка складності майже збігається, то в цілому середня оцінка складності способу шифрування на основі U_k -послідовності для цього порядку буде меншою, ніж способу Ель-Гамала.
- Також перевагою способу на основі U_k -послідовностей є те, що в ньому забезпечується можливість збільшення стійкості пропорційно порядку послідовностей k , а також спрощення процедури завдання параметрів.
- 40 Однак існують задачі, в яких дуже важливою є проблема забезпечення високого рівня стійкості криптографічних перетворень під час шифрування. Це може бути навіть більш актуальним, ніж вирішення проблеми підвищення швидкості шифрування. В першу чергу, це стосується задач в системах захисту з підвищеним рівнем секретності. В цьому зв'язку, спосіб шифрування з відкритим ключем у вигляді електронного коду на основі U_k -послідовностей, хоч
- 45 і забезпечує достатній рівень криптографічної стійкості, але має потенційні можливості підвищення стійкості для відповідних систем захисту, оскільки безпосереднє обчислення зашифрованого повідомлення здійснюється шляхом поєднання відкритого повідомлення з

елементом U_k -послідовності, обчисленим за адитивним, а не мультиплікативним способом зміни індексу, що могло б значно підвищити стійкість зашифрованого повідомлення.

В основу корисної моделі поставлено задачу створення способу шифрування з відкритим ключем у вигляді електронного коду, в якому за рахунок використання при шифруванні математичного апарату тільки рекурентних V_k^+ -послідовностей та їх залежностей, досягається можливість підвищення стійкості криптографічних перетворень під час шифрування.

Поставлена задача вирішується тим, що використання для шифрування інформації у вигляді електронного коду математичного апарату тільки на основі рекурентних V_k^+ -послідовностей забезпечує можливість безпосереднє обчислення зашифрованого повідомлення здійснювати шляхом поєднання відкритого повідомлення з елементом V_k^+ -послідовності, обчисленим 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 під час шифрування.

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 шифрування інформації з відкритим ключем, 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 $v_{n \cdot m,k}$.

Спочатку центр довіри або одержувач вибирає і відкрито публікує ціле додатне число p ($p > 2$) та цілі числа g_1, g_k . Потім він випадковим чином вибирає секретний ключ a і обчислює відкритий ключ $v_{a+i,k} \bmod p$, $i = \overline{-(k-1), 0}$, і публікує його.

Відправник на основі отриманого відкритого ключа продовжує на своєму боці обчислення за модулем p елементів $v_{a+i,k}$, $i = \overline{1, k-1}$, використовуючи формулу (4).

Коли відправник бажає зашифрувати повідомлення M , яке представляється як $0 < M < p$ або поділене на блоки такого розміру, і передати його одержувачу, він спочатку вибирає випадкове число b та обчислює за модулем p $v_{b+i,k}$, $i = \overline{-(k-1), 0}$. Потім він, використовуючи своє секретне число b , обчислює $v_{a \cdot b,k} \bmod p$, зашифровує відкрите повідомлення M за допомогою операції виключного АБО з обчисленим значенням як $M' = M \oplus (v_{a \cdot b,k} \bmod p)$ та передає одержувачу зашифроване повідомлення M' разом з елементами $v_{b+i,k} \bmod p$, $i = \overline{-(k-1), 0}$.

Під час дешифрування одержувач спочатку обчислює за модулем p $v_{b+i,k}$, $i = \overline{1, k-1}$, а потім обчислює $v_{b \cdot a,k} \bmod p$, використовуючи свій секретний ключ a . Після цього одержувач дешифрує відкрите повідомлення M як результат виключного АБО M' з $v_{b \cdot a,k} \bmod p$, тобто $M = M' \oplus (v_{b \cdot a,k} \bmod p)$.

Загальна схема способу шифрування інформації з відкритим ключем у вигляді електронного коду на основі математичного апарату рекурентних V_k^+ -послідовностей, що пропонується, буде мати вигляд представлений на кресленні.

Алгоритм шифрування інформації у вигляді електронного коду згідно цього способу буде мати такий вигляд.

Крок 1. Задати параметр k .

Крок 2. Вибрати p , $p > 2$.

5 Крок 3. Вибрати g_1, g_k .

Крок 4. Опублікувати параметри.

Крок 5. Одержувачу вибрати випадкове число a , $1 < a < p$, як секретний ключ.

Крок 6. Одержувачу обчислити за модулем p відкритий ключ $v_{a+i,k}$, $i = \overline{-(k-1), 0}$, використовуючи спосіб прискореного обчислення елементів $v_{n,k}$ для додатних значень n , та опублікувати відкритий ключ.

Крок 7. Відправнику обчислити за модулем p $v_{a+i,k}$, $i = \overline{1, k-1}$, за формулою (4).

Крок 8. Відправнику вибрати випадкове число b , $1 < b < p$.

Крок 9. Відправнику 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 .

15 Крок 10. Відправнику обчислити $v_{a \cdot b, k} \bmod p$, використовуючи спосіб прискореного обчислення елементів $v_{n \cdot m, k}$, та зашифрувати відкрите повідомлення M , отримуючи зашифроване повідомлення M' як $M' = M \oplus (v_{a \cdot b, k} \bmod p)$.

Крок 11. Відправнику передати обчислені елементи $v_{b+i,k} \bmod p$, $i = \overline{-(k-1), 0}$, разом з M' одержувачу.

20 Крок 12. Одержувачу обчислити за модулем p $v_{b+i,k}$, $i = \overline{1, k-1}$, за формулою (4).

Крок 13. Одержувачу обчислити $v_{b \cdot a, k} \bmod p$, використовуючи спосіб прискореного обчислення елементів $v_{n \cdot m, k}$, та дешифрувати повідомлення M' , отримуючи відкрите повідомлення M як $M = M' \oplus (v_{b \cdot a, k} \bmod p)$.

25 Технічний результат: підвищено стійкість та достовірність шифрування інформації з відкритим ключем у вигляді електронного коду, що дає можливість розширення галузі використання таких способів шифрування, в першу чергу, в системах захисту з підвищеним рівнем секретності.

ФОРМУЛА КОРИСНОЇ МОДЕЛІ

30

Спосіб шифрування інформації з відкритим ключем у вигляді електронного коду на основі рекурентних послідовностей, що включає відкритий канал передавання інформації у вигляді електронного коду, відправника, який шифрує відкрите повідомлення у вигляді електронного коду, та одержувача, який відновлює відкрите повідомлення із зашифрованого, секретний ключ одержувача у вигляді електронного коду та обчислений на його основі відкритий ключ, який **відрізняється** тим, що для шифрування інформації 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

40 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 $v_{n+m,k}$ для будь-яких цілих додатних n та m розраховуються за формулою

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

45 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 $v_{n+m,k}$, при цьому шифрування інформації у вигляді електронного коду відбувається таким чином: спочатку центр довіри або одержувач вибирає і відкрито публікує параметри - ціле

додатне число p , $p > 2$, та цілі числа g_1 і g_k , потім він випадковим чином вибирає секретний ключ a , $1 < a < p$, який він використовує для обчислення відкритого ключа $v_{a+i,k} \bmod p$, $i = \overline{-(k-1), 0}$, за допомогою способу прискореного обчислення елементів $v_{n,k}$ з використанням бінарного способу розкладання індексу n та формули обчислення елементів $v_{n+m,k}$, і публікує
 5 обчислений відкритий ключ, після цього відправник на своєму боці розширює отриманий набір елементів відкритого ключа за допомогою формули, що визначає рекурентну V_k^+ -послідовність, обчислюючи за модулем p елементи $v_{a+i,k}$, $i = \overline{1, k-1}$, при шифруванні інформації у вигляді електронного коду відправник вибирає випадкове число b , $1 < b < p$, обчислює за модулем p $v_{b+i,k}$, $i = \overline{-(k-1), 0}$, за допомогою способу прискореного обчислення елементів $v_{n,k}$, обчислює
 10 елемент $v_{a,b,k} \bmod p$ за допомогою способу прискореного обчислення елементів $v_{n,m,k}$, на основі свого секретного числа b та отриманого і обчисленого за модулем p розширеного набору елементів відкритого ключа $v_{a+i,k}$, $i = \overline{-(k-1), k-1}$, після цього відправник зашифровує відкрите повідомлення M (або блок цього повідомлення), $0 < M < p$, за допомогою операції виключного АБО з обчисленим значенням $v_{a,b,k} \bmod p$, отримуючи зашифроване повідомлення
 15 M' у вигляді електронного коду як $M' = M \oplus (v_{a,b,k} \bmod p)$, та передає одержувачу зашифроване повідомлення M' разом з елементами $v_{b+i,k} \bmod p$, $i = \overline{-(k-1), 0}$, при відновленні відкритого повідомлення із зашифрованої інформації у вигляді електронного коду одержувач спочатку обчислює за модулем p $v_{b+i,k}$, $i = \overline{1, k-1}$, за допомогою формули, що визначає рекурентну V_k^+ -послідовність, на основі отриманих від відправника елементів $v_{b+i,k} \bmod p$, $i = \overline{-(k-1), 0}$,
 20 розширюючи тим самим цей набір, потім одержувач обчислює елемент $v_{b,a,k} \bmod p$ за допомогою способу прискореного обчислення елементів $v_{n,m,k}$ на основі свого секретного ключа a та отриманого і обчисленого за модулем p розширеного набору елементів $v_{b+i,k}$, $i = \overline{-(k-1), k-1}$, на завершення, одержувач відновлює відкрите повідомлення M у вигляді електронного коду як результат виключного АБО зашифрованого повідомлення M' з обчисленим значенням $v_{b,a,k} \bmod p$, тобто $M = M' \oplus (v_{b,a,k} \bmod p)$.
 25

