2 Забезпечення комп'ютерної безпеки в інформаційних системах

УДК 621.391.7

СПЕЦІАЛІЗОВАНІ ПРОЦЕСОРИ АСИМЕТРИЧНОГО ШИФРУВАННЯ ІНФОРМАЦІЇ НА ОСНОВІ РЕКУРЕНТНИХ ПОСЛІДОВНОСТЕЙ

Юрій Яремчук
Вінницький національний технічний університет

Анотація: **Розглянуто математичний апарат рекурентних послідовностей, а також можливість побудови методу асиметричного шифрування інформації на його основі. Для запропонованого методу розроблено принципи побудови спеціалізованих процесорів шифрування та дешифрування інформації. Порівняння швидкості роботи розроблених процесорів з відомими аналогами показало, що вони забезпечують приблизно однаковий час шифрування-дешифрування, але при цьому запропонований метод забезпечує можливість встановлювати необхідний рівень криптостійкості залежно від порядку послідовності. Спеціалізовані процесори, побудовані за цим методом, мають перспективи використання в задачах іншого криптографічного призначення на основі відкритого ключа.**

Summary: **In this paper a mathematical apparatus of recurrent sequences, as well as a possibility of constructing a method of asymmetric information encryption, based on it, was considered. For the proposed method, principles of constructing specialized processors of information encryption and decryption were developed. A comparison of the speed of the developed processors with the known analogues showed that they provide about the same time for encryption-decryption, but simultaneously the proposed method provides a possibility of setting required levels of cryptographic reliability depending on the sequence order. Also the specialized processors, built under this method, can be used in other cryptographic tasks based on the public key.**

Ключові слова: **Інформація, захист інформації, криптографія, шифрування, асиметричне шифрування, рекурентні послідовності, спеціалізовані процесори.**

I Вступ

Важливе місце при вирішенні проблеми захисту інформації займають криптографічні методи шифрування інформації, які поділяють на симетричні та асиметричні [1 – 4]. Основною перевагою асиметричних криптосистем [3, 4] є відсутність необхідності фізичного розподілу ключів секретним каналом зв'язку або третьої сторони (посередника) для реалізації цього. Однак, при практичній реалізації методів асиметричного криптографічного захисту виникає проблема виконання складних обчислень над числами великої розрядності, що нерозривно пов'язує ці методи з високим рівнем обчислювальної техніки.

Виходячи з цього, актуальним є побудова асиметричних методів шифрування на основі таких математичних апаратів, які б могли забезпечувати спрощення обчислень. В цьому зв'язку певний інтерес викликає апарат на основі рекурентних послідовностей, який дозволяє за певних умов спрощувати обчислення асиметричних методів, що базуються на його основі.

Особливість методів асиметричного шифрування полягає в тому, що в них необхідно виконувати обчислення над числами великої розрядності (1024–4096 двійкових розрядів), тому програмна реалізація алгоритмів шифрування вимагає великого часу і для деяких застосувань є непридатною. Потрібна в цих випадках швидкість шифрування може бути досягнута за рахунок апаратної реалізації методу шифрування. Тому розглядається можливість побудови спеціалізованих процесорів асиметричного шифрування та дешифрування інформації на основі рекурентних послідовностей.

Мета роботи – розробка принципів побудови швидкісних спеціалізованих процесорів асиметричного шифрування-дешифрування інформації на основі рекурентних послідовностей, які б забезпечували достатній рівень криптостійкості.

Постановка задач досліджень. Розглянути математичний апарат рекурентних послідовностей з точки зору побудови швидкісних методів асиметричного шифрування інформації та розробити принципи побудови спеціалізованих процесорів на їх основі. Дослідити запропоновані процесори щодо швидкості їх роботи і порівняти з відповідними процесорами, що реалізують відомі методи асиметричного шифрування.

II Асиметричне шифрування інформації на основі рекурентних послідовностей

Рекурентні послідовності в загальному вигляді породжуються таким співвідношенням [5]

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

де a_1, a_2, ..., a_k - коефіцієнти, k - порядок послідовності, виходячи з початкових елементів u_0, u_1, ..., u_k.

Назвемо послідовність чисел, що обчислюються за формулою

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

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

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

Назвемо 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 – U_k –послідовністю.

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

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

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

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

Ідея методу асиметричного шифрування інформації полягає в побудові односторонньої функції на основі властивості (4), оскільки 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 є практично неможливим для великих значень n. Крім того, елемент $u_{n+m,k}$ за формулою (4) може бути обчислений 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 $u_{m-i,k}$, $i = \overline{0,k-1}$.

Використовуючи вищенаведене маємо такий метод 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 (4) 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.

Процедура шифрування даних представлена на рис. 1.

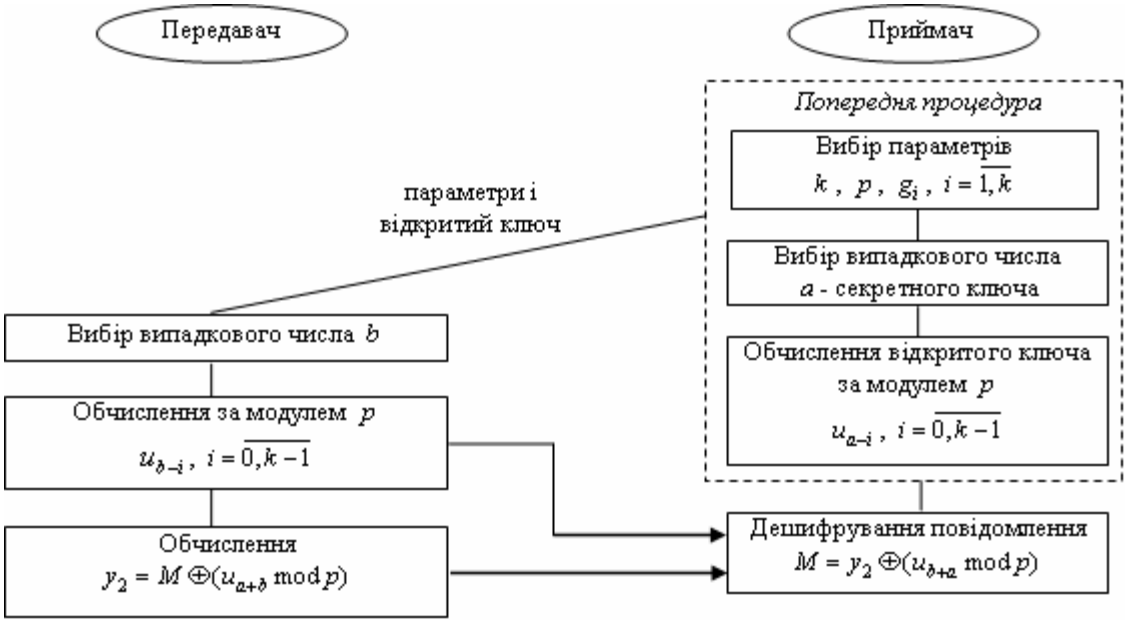

Рисунок 1 – Процедура шифрування з відкритим ключем на основі елементів U_k – послідовностей

Обчислення елементів u_{a-i} та u_{b-i} для $i = \overline{0,k-1}$ здійснюється за формулою (5) на основі елементів $v_{a+i,k}$ та $v_{b+i,k}$ для $i = \overline{-(k-1),k-2}$. Обчислення останніх може здійснюватись за алгоритмом прискореного обчислення елементів V_k^+ –послідовності, який може бути реалізований на основі відомого бінарного методу піднесення до степеня [6].

Проведено дослідження теоретичної криптостійкості та складності обчислень за даним методом, а також порівняння з відомим методом Ель-Гамаля. Показано, що розглянутий метод має таку ж криптостійкість, як і відомий метод, але за певних умов має меншу складність обчислень порівняно з відомим. Суттєвою перевагою запропонованого методу є те, що він дозволяє встановлювати необхідну криптостійкість залежно від параметру k. Тобто існує можливість збільшення криптостійкості зі збільшенням цього параметру.

III Розробка принципів побудови спеціалізованих процесорів асиметричного шифрування інформації

Розглянемо процесори, що реалізують процедури шифрування та дешифрування інформації представленого методу асиметричного шифрування інформації.

Для реалізації цього методу необхідні процедури для обчислення за модулем p елементів $v_{n+i,k}$, $i = \overline{-(k-1),k-2}$, а також елементів $u_{n-i,k}$, $i = \overline{0,k-1}$, та $u_{n+m,k}$. Всі ці обчислення пропонується здійснювати на одному пристрої обчислення елементів V_k^+ – та U_k –послідовностей. Роботу пристрою організуємо в п’яти режимах. В першому режимі будемо здійснювати обчислення елементів $v_{n+i,k}$, $i = \overline{-2k+1,k-2}$, для додатних значень *n*. Другий режим роботи пристрою буде забезпечувати обчислення елементів $v_{n+i,k}$, $i = \overline{-k,k-2}$, для від’ємних значень n. Третій, четвертий та п’ятий режими роботи пристрою будуть забезпечувати відповідно обчислення елементів $u_{n-i,k}$, $i = \overline{0,k-1}$, за формулою (5), $u_{n+m-i,k}$, $i = \overline{0,k-1}$, за формулою (4) та $u_{n-m-i,k}$, $i = \overline{0,k-1}$.

Для реалізації асиметричного шифрування (дешифрування) інформації Передавачем (Приймачем) за представленим методом пропонується схема процесора, що наведена на рис. 2.

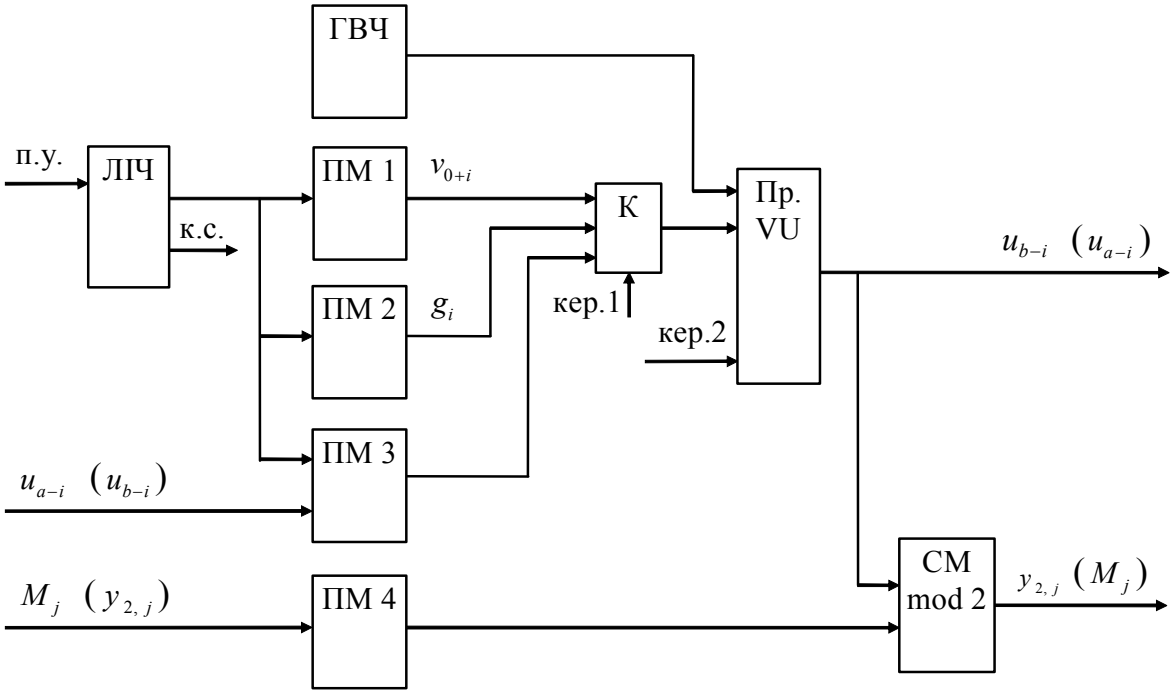

Рисунок 2 – Структурна схема процесора асиметричного шифрування (дешифрування)

Процесор містить генератор випадкових чисел ГВЧ; пристрій обчислення елементів V_k^+ – та U_k – послідовностей Пр.VU; суматор за модулем 2 СМ mod 2; блоки пам'яті ПМ 1, ПМ 2, призначені для зберігання відповідно елементів $v_{0+i,k}$, $i=\overline{-(k-1),0}$, та коефіцієнтів рекурентної залежності g_i, $i=\overline{1,k}$; блок пам'яті ПМ 3, призначений для зберігання відкритого ключа $u_{a-i,k}$, $i=\overline{0,k-1}$ при шифруванні інформації та елементів $u_{b-i,k}$, $i=\overline{0,k-1}$ при дешифруванні інформації; блок пам'яті ПМ 4, призначений для зберігання одного j-го кодового блоку відкритого повідомлення M_j або зашифрованого повідомлення $y_{2,j}$ відповідно при його шифруванні або дешифруванні; комутатор К; лічильник ЛІЧ.

Тут слід зазначити, що оскільки повідомлення M зазвичай розбивають на певне число частин, які шифруються окремо послідовно один за одним, розбиваємо M на Q частин M_1, M_2, ... , M_Q фіксованого розміру, і кожну частину M_j шифруємо окремо.

Робота процесора з боку Передавача під час шифрування інформації відбувається таким чином.

Генератор ГВЧ генерує випадкове число b, яке разом з даними, що знаходяться в блоці пам'яті ПМ 1, подаються на відповідні входи пристрою Пр.VU.

Далі здійснюється робота пристрою Пр.VU в першому режимі, після чого на вхід пристрою подаються дані з блоку пам'яті ПМ 2 і в третьому режимі обчислюються елементи $u_{b-i,k}$, $i=\overline{0,k-1}$, які передаються Приймачу.

Потім, після подачі на вхід пристрою Пр.VU даних з блоку пам'яті ПМ 3, в четвертому режимі обчислюється елемент $u_{a+b,k}$, який разом з кодовим блоком відкритого повідомлення M_j надходить на вхід суматора за модулем 2 СМ mod 2. Результат роботи СМ mod 2 – зашифроване повідомлення $y_{2,j}$ передається Приймачу.

Робота пристрою з боку Приймача аналогічна тій, яку виконує Передавач. Різниця полягає лише в тому, що обчислення елементів $u_{a-i,k}$, $i=\overline{0,k-1}$, проводиться один раз перед шифруванням – дешифруванням всього повідомлення M.

Після отримання Приймачем кодового блоку зашифрованого повідомлення $y_{2,j}$ пристрій дешифрування лише обчислює елемент $u_{b+a,k}$ під час роботи пристрою Пр.VU в четвертому режимі, та отримує кодовий блок відкритого повідомлення M_j за допомогою суматора за модулем 2 СМ mod 2.

Проведемо тепер дослідження часу роботи розроблених процесорів асиметричного шифрування (дешифрування) та порівняємо його з часом роботи процесорів, що реалізують відомі аналоги.

Встановлено, що час обчислення елементів V_k^+ –послідовності в першому і другому режимах його роботи дорівнює:

$$T_V = Hq \cdot \left(k^2 + k\right) \cdot T_{мн.Монт.},$$

де H – кількість машинних одиниць інформації для зберігання великого числа,

q – кількість розрядів машинної одиниці інформації,

$T_{мн.Монт.}$ – час множення за модулем за методом Монтгомері.

Час обчислення елементів U_k –послідовності в третьому, четвертому і п'ятому режимах дорівнює:

$$T_U = \left(k^2 + k\right) \cdot T_{мн.Монт.}.$$

Аналіз представленого методу асиметричного шифрування показує, що дешифрування одного блоку інформації в ньому потребує значно меншого часу, ніж шифрування, оскільки відкритий ключ $u_{a-i,k}$, $i = \overline{0, k-1}$, обчислюється лише перед шифруванням – дешифруванням всього повідомлення M, в той час, як обчислення $u_{b-i,k}$, $i = \overline{0, k-1}$, проводиться для кожного кодового блоку M_j.

Виходячи з цього, час шифрування згідно з запропонованим методом на процесорі, представленому на рис. 2, дорівнює:

$$T_ш = QHq \cdot \left(k^2 + k\right) \cdot T_{мн.Монт},$$

а час дешифрування –

$$T_{дш} = \left(Q + Hqk\right) \cdot \left(k + 1\right) \cdot T_{мн.Монт}.$$

Проаналізуємо можливість конвеєрної обробки інформації згідно з запропонованим методом з метою прискорення шифрування інформації.

Нехай обчислення елементів $v_{n+i,k}$, $i = \overline{-2k+1, k-2}$, елементів $u_{n-i,k}$, $i = \overline{0, k-1}$, та елементу $u_{n+m,k}$ здійснюється за допомогою трьох окремих пристроїв.

Якщо взяти за t – кількість розрядів двійкового представлення індексу елемента рекурентної послідовності, то протягом одного етапу обчислень на першому пристрої буде обчислюватись від k до $t \cdot k$ елементів за формулою обчислення $v_{n+m,k}$ та $2k-2$ елементів за формулою (1) або (2), на другому пристрої – k елементів за формулою (5), а на третьому пристрої – один елемент за формулою (4).

Однак, враховуючи те, що час обчислення одного елемента за формулою обчислення $v_{n+m,k}$ або (5), або (4) однаковий, а також те, що в сучасних системах шифрування інформації параметр t вибирається таким, що має 1024 або 4096 розрядів, завантаженість пристроїв буде значно відрізнятись.

Навіть, якщо обчислення елементів $u_{n-i,k}$, $i = \overline{0, k-1}$, та $u_{n+m,k}$ здійснювати послідовно на одному пристрої під час роботи пристрою обчислення елементів $v_{n+i,k}$, $i = \overline{-2k+1, k-2}$, завантаженість пристроїв все рівно буде значно різнитися. Тому побудувати ефективний конвеєр не можливо.

Проведемо тепер порівняння запропонованих процесорів для шифрування-дешифрування інформації з відповідними спеціалізованими процесорами, що реалізують відомий метод.

За основу порівняння візьмемо аналог – відомий метод Ель-Гамаля. Основною операцією, що виконується в методі Ель-Гамаля є піднесення до степеня за модулем. Ця операція може здійснюватись за методом Монтгомері [1], який має меншу складність обчислень, ніж відомий бінарний метод [6]. Метод піднесення до степеня за Монтгомері оснований на множенні за методом Монтгомері. Виходячи з цього пристрій піднесення до степеня за Монтгомері можна побудувати на основі пристрою множення за Монтгомері, який використовується в процесорі, що реалізує запропонований метод асиметричного шифрування.

Час виконання піднесення до степеня за модулем відповідним пристроєм буде дорівнювати

$$T_{ПДС\,\mathrm{mod}} = 2\left(Hq + 1\right) \cdot T_{мн.Монт.}$$

Використовуючи пристрій піднесення до степеня за модулем для побудови спеціалізованого процесору для шифрування (дешифрування) інформації за відомим методом Ель-Гамаля, отримаємо час шифрування інформації на процесорі для шифрування

$$T_{ЕГ,ш} = 4Q(Hq+1)\cdot T_{мн.Монт.},$$

а час дешифрування на цьому процесорі буде дорівнювати

$$T_{ЕГ,дш} = 2(Q+1)(Hq+1)\cdot T_{мн.Монт.}.$$

Для порівняння часу роботи процесорів за відомим та запропонованим методами введемо відносну оцінку, в результаті чого отримаємо

$$\delta_{\text{ЕГ}} = \frac{2(Hq+1)(3Q+1)}{(Q+1)Hq(k^2+k)}.$$

Значення $\delta_{\text{ЕГ}}$ для різних значень Hq, Q та k наведені нижче.

k	Q	Hq	$\delta_{\text{ЕГ}}$	k	Q	Hq	$\delta_{\text{ЕГ}}$
2	100	1024	0.9944	3	100	1024	0.4972
		2048	0.9939			2048	0.4969
		4096	0.9936			4096	0.4968
	1000	1024	1.0003		1000	1024	0.5002
		2048	0.9998			2048	0.4999
		4096	0.9996			4096	0.4998

Аналіз отриманих відносних оцінок показує, що час шифрування-дешифрування на процесорах, що реалізують запропонований метод приблизно однаковий для $k=2$ і більше для $k>2$, ніж на процесорах, що реалізують відомий метод Ель-Гамаля.

IV Висновки

Розглянуто математичний апарат рекурентних V_k^+ – та U_k – послідовностей. На його основі представлено метод асиметричного шифрування інформації, суть якого полягає в заміні піднесення до степеня обчисленням певного елементу U_k –послідовності. Особливість представленого методу шифрування полягає в тому, що всі процедури в ньому виконуються принципово послідовно, тому запропоновано процесор для шифрування (дешифрування), який містить один пристрій для обчислення елементів V_k^+ – та U_k – послідовностей. Для спрощення організації пам'яті вона реалізується у вигляді окремих блоків пам'яті для зберігання різних даних. Порівняння процесорів, що реалізують запропонований метод та відомий метод Ель-Гамаля показує, що перші забезпечують майже однаковий час шифрування – дешифрування при $k=2$ та більший час при $k>2$. Однак суттєвою перевагою запропонованого методу є те, що він дозволяє встановлювати необхідну криптостійкість залежно від параметру k. Також перевагою розроблених спеціалізованих процесорів асиметричного шифрування на основі рекурентних V_k^+ – та U_k –послідовностей може бути те, що принципи їх організації можуть стати основою для побудови спеціалізованих процесорів різного криптографічного призначення, що реалізують технологію відкритого ключа, зокрема в задачах автентифікації або цифрового підписування, де переваги щодо швидкості криптографічних перетворень на основі V_k^+ – та U_k –послідовностей можуть бути більш суттєвими і важливими.

Література: ***1.*** *Menezes A. J., van Oorschot P. C., Vanstone S. A. Handbook of Applied Cryptography. – CRC Press, 2001. – 816 p.* ***2.*** *Тилборг ван Х.К.А. Основы криптологии. – М.: Мир, 2006. – 471 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: Пер. с англ. – М.: Мир. – 1995. – 318 с.* ***5.*** *Маркушевич А. И. Возвратные последовательности. – М.: Наука, 1975. – 48 с.* ***6.*** *Кнут Д. Искусство программирования для ЭВМ, том 2. Получисленные алгоритмы. – М.: Вильямс, 2004. – 832 с.*