УДК 511.216

Яремчук Ю.Є. *(Вінницький національний технічний університет)*

РЕКУРЕНТНІ ПОСЛІДОВНОСТІ ЯК ОСНОВА КРИПТОГРАФІЧНИХ МЕТОДІВ

Яремчук Ю.Є. Рекурентні послідовності як основа криптографічних методів. В роботі розглянуто рекурентну послідовність, яка складається з двох послідовностей V_k^+ і V_k^-. Встановлено залежності для V_k^+ –послідовності, які дозволяють побудувати криптографічні методи на їх основі.

Ключові слова: КРИПТОГРАФІЯ, РЕКУРЕНТНА ПОСЛІДОВНІСТЬ, V_k^+-ПОСЛІДОВНІСТЬ, V_k^--ПОСЛІДОВНІСТЬ, КРИПТОГРАФІЧНА СТІЙКІСТЬ

Яремчук Ю.Е. Рекуррентные последовательности как основа криптографических методов. В работе рассмотрена рекуррентная последовательность, которая состоит из двух последовательностей V_k^+ и V_k^-. Установлены зависимости для V_k^+-последовательности, которые позволяют построить криптографические методы на их основе.

Ключевые слова: КРИПТОГРАФИЯ, РЕКУРРЕНТНАЯ ПОСЛЕДОВАТЕЛЬНОСТЬ, V_k^+-ПОСЛЕДОВАТЕЛЬНОСТЬ, V_k^--ПОСЛЕДОВАТЕЛЬНОСТЬ, КРИПТОГРАФИЧЕСКАЯ СТОЙКОСТЬ

Iaremchuk Iu.Ie. The recurrent sequences as basis of cryptographic methods. A recurrent sequence which consists of two sequences V_k^+ and V_k^- is considered. Dependences are set for V_k^+-sequences which allow to build cryptographic methods on their basis.

Keywords: CRYPTOGRAPHY, RECURRENT SEQUENCE, V_k^+-SEQUENCE, V_k^--SEQUENCE, CRYPTOGRAPHIC FIRMNESS

Вступ. Рекурентні послідовності отримали широке застосування в різних галузях. В цьому зв'язку цікавим є дослідження рекурентних послідовностей щодо можливості побудови на їх основі криптографічних методів.

В загальному вигляді рекурентні послідовності породжується таким співвідношенням [1]

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

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

Певну цікавість представляють послідовності, в яких початкові елементи пов'язані з коефіцієнтами. Прикладом такої послідовності є послідовність, що описана в [2]. В даній статті пропонується одна з таких послідовностей.

Рекурентна послідовність, в якій початкові елементи пов'язані з коефіцієнтами. Назвемо V_k^+–послідовністю послідовність чисел, що обчислюються за формулою

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

при початкових значеннях $v_{0,k} = 1$, $v_{1,k} = g_2$ 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 числа.

Для $k = 2$ послідовність буде мати такий вигляд:

. . .	$v_{5,2}$	$v_{4,2}$	$v_{3,2}$	$v_{2,2}$	$v_{1,2}$	$v_{0,2}$
. . .	$g_2^5 + 4g_1g_2^3 + 3g_1^2g_2$	$g_2^4 + 3g_1g_2^2 + g_1^2$	$g_2^3 + 2g_1g_2$	$g_2^2 + g_1$	g_2	1

Для $k > 2$ послідовність буде мати такий вигляд:

	$v_{k,k}$	$v_{k-1,k}$	$v_{k-2,k}$	$v_{k-3,k}$	. . .	$v_{1,k}$	$v_{0,k}$
	g_k^2	g_k	1	0	. . .	0	0
. . .	$v_{2k-1,k}$		$v_{2k-2,k}$	$v_{2k-3,k}$	. . .	$v_{k+1,k}$	
. . .	$g_k^{k+1} + 2g_1g_k$		$g_k^k + g_1$	g_k^{k-1}	. . .	g_k^3	

Формула (1) описує рекурентну процедуру обчислення елементу $v_{n,k}$, однак при встановленні аналітичних залежностей цієї послідовності більш зручним є безпосереднє обчислення цього елементу через початкові елементи.

Для будь-яких цілих додатних n і k, таких що $n \geq k$ отримано таку аналітичну залежність

$$v_{n,k} = \sum_{i=0}^{\left(\frac{n-(k-2)}{k}\right(} C^i_{n-(k-2)-(k-1)i} \cdot g_k^{n-(k-2)-ki} \cdot g_1^i \ . \qquad (2)$$

Проведемо аналіз індукцією по *n*.

Покажемо, що (2) виконується для n, які дорівнюють k, $k+1$, . . . , $2k-3$, $2k-2$, $2k-1$.

Для $k = 2$:

$v_{k,k} = v_{2,k} = C_2^0 g_2^2 g_1^0 + C_1^1 g_2^0 g_1^1 = g_2^2 + g_1$,

$v_{k+1,k} = v_{2k-1,k} = v_{3,k} = C_3^0 g_2^3 g_1^0 + C_2^1 g_2^1 g_1^1 = g_2^3 + 2g_1 g_2$.

Для $k > 2$:

$v_{k,k} = C_2^0 g_k^2 g_1^0 = g_k^2$,

$v_{k+1,k} = C_3^0 g_k^3 g_1^0 = g_k^3$,

. . .

$v_{2k-3,k} = C_{k-1}^0 g_k^{k-1} g_1^0 = g_k^{k-1}$,

$v_{2k-2,k} = C_k^0 g_k^k g_1^0 + C_1^1 g_k^0 g_1^1 = g_k^k + g_1$,

$v_{2k-1,k} = C_{k+1}^0 g_k^{k+1} + C_2^1 g_k^1 g_1^1 = g_k^{k+1} + g_k$.

Основа індукції, таким чином, доведена.

Нехай залежність (2) виконується для $n-k$, $n-k+1$, . . . , $n-1$. Покажемо, що вона виконується для n.

$$v_{n,k} = g_k v_{n-1,k} + g_1 v_{n-k,k} = \sum_{i=0}^{\left\lfloor \frac{n-1-(k-2)}{k} \right\rfloor} C^i_{n-1-(k-2)-(k-1)i} \cdot g_k^{n-(k-2)-ki} \cdot g_1^i +$$

$$+ \sum_{i=0}^{\left(\frac{n-k-(k-2)}{k}\right(} C^i_{n-k-(k-2)-(k-1)i} \cdot g_k^{n-k-(k-2)-ki} \cdot g_1^{i+1} =$$

$$= C^0_{n-k+1} g_k^{n-k+2} + C^1_{n-2k+2} g_k^{n-2k+2} g_1 + C^2_{n-3k+3} g_k^{n-3k+2} g_1^2 + C^3_{n-4k+4} g_k^{n-4k+2} g_1^3 + \ldots +$$

$$+ C^0_{n-2k+2} g_k^{n-2k+2} g_1 + C^1_{n-3k+3} g_k^{n-3k+2} g_1^2 + C^2_{n-4k+4} g_k^{n-4k+2} g_1^3 + C^3_{n-5k+5} g_k^{n-5k+2} g_1^4 + \ldots$$

Відомо [3], що

$$,,_n^r + C_n^{r+1} = C_{n+1}^{r+1} . \qquad (3)$$

і для будь-яких n та m

$$C_n^0 = C_m^0$$

Замінюючи в першому доданку виразу для $v_{n,k}$ $,,^0_{n-k+1}$ на $,,^0_{n-k+2}$, а також доданки попарно згідно (3) отримаємо :

$$v_{n,k} = C^0_{n-k+2} g_k^{n-k+2} + C^1_{n-2k+3} g_k^{n-2k+2} g_1 + C^2_{n-3k+4} g_k^{n-3k+2} g_1^2 + C^3_{n-4k+5} g_k^{n-4k+2} g_1^3 + \ldots =$$

$$= \sum_{i=0}^{\left(\frac{n-(k-2)}{k}\right(} C^i_{n-(k-2)-(k-1)i} \cdot g_k^{n-(k-2)-ki} \cdot g_1^i .$$

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

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

Проведемо аналіз індукцією по m.

Покажемо, що (4) виконується для m, які дорівнюють 1, 2 , 3, . . . , k.

$$v_{n+1,k} = v_{k-1,k} v_{n,k} + g_1 v_{k-2,k} v_{n-k+1,k} + g_1 v_{k-3,k} v_{n-k+2,k} + ... + g_1 v_{0,k} v_{n-1,k}$$

Враховуючи значення початкових елементів, отримаємо

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

Знайдемо тепер $v_{n+2,k}$.

$$v_{n+2,k} = v_{k,k} v_{n,k} + g_1 v_{k-1,k} v_{n-k+1,k} + g_1 v_{k-2,k} v_{n-k+2,k} + g_1 v_{k-3,k} v_{n-k+3,k} + ... + \quad + g_1 v_{1,k} v_{n-1,k} \,.$$

З (1) $v_{k,k} = g_k v_{k-1,k} + g_1 v_{0,k} = g_k v_{k-1,k}$. Тоді

$$\begin{aligned} v_{n+2,k} &= g_k v_{k-1,k} v_{n,k} + g_1 v_{k-1,k} v_{n-k+1,k} + g_1 v_{k-2,k} v_{n-k+2,k} = \\ &= v_{k-1,k} (g_k v_{n,k} + g_1 v_{n-k+1,k}) + g_1 v_{n-k+2,k} = g_k v_{n+1,k} + g_1 v_{n-k+2,k} \,. \end{aligned}$$

Роблячи таким же чином, знайдемо $v_{n+3,k}$.

$$\begin{aligned} v_{n+3,k} &= v_{k+1,k} v_{n,k} + g_1 v_{k,k} v_{n-k+1,k} + g_1 v_{k-1,k} v_{n-k+2,k} + g_1 v_{k-2,k} v_{n-k+3,k} + \\ &\quad + g_1 v_{k-3,k} v_{n-k+4,k} + ... + g_1 v_{2,k} v_{n-1,k} = \\ &= (g_k v_{k,k} + g_1 v_{1,k}) v_{n,k} + g_1 v_{k,k} v_{n-k+1,k} + g_1 v_{k-1,k} v_{n-k+2,k} + g_1 v_{n-k+3,k} = \\ &= v_{k,k} (g_k v_{n,k} + g_1 v_{n-k+1,k}) + g_1 v_{k-1,k} v_{n-k+2,k} + g_1 v_{n-k+3,k} = \\ &= v_{k,k} v_{n+1,k} + g_1 v_{k-1,k} v_{n-k+2,k} + g_1 v_{n-k+3,k} = \\ &= (g_k v_{k-1,k} + g_1 v_{0,k}) v_{n+1,k} + g_1 v_{k-1,k} v_{n-k+2,k} + g_1 v_{n-k+3,k} = \\ &= v_{k-1,k} (g_k v_{n+1,k} + g_1 v_{n-k+2,k}) + g_1 v_{n-k+3,k} = \\ &= g_k v_{n+2,k} + g_1 v_{n-k+3,k} \end{aligned}$$

. . .

$$\begin{aligned} v_{n+k,k} &= v_{2k-2,k} v_{n,k} + g_1 v_{2k-3,k} v_{n-k+1,k} + g_1 v_{2k-4,k} v_{n-k+2,k} + g_1 v_{2k-5,k} v_{n-k+3,k} + ... + \\ &\quad + g_1 v_{k,k} v_{n-2,k} + g_1 v_{k-1,k} v_{n-1,k} = \\ &= (g_k v_{2k-3,k} + g_1 v_{k-2,k}) v_{n,k} + g_1 v_{2k-3,k} v_{n-k+1,k} + g_1 v_{2k-4,k} v_{n-k+2,k} + \\ &\quad + g_1 v_{2k-5,k} v_{n-k+3,k} + ... + g_1 v_{k,k} v_{n-2,k} + g_1 v_{k-1,k} v_{n-1,k} = \\ &= v_{2k-3,k} (g_k v_{n,k} + g_1 v_{n-k+1,k}) + g_1 v_{2k-4,k} v_{n-k+2,k} + g_1 v_{2k-5,k} v_{n-k+3,k} + ... + \\ &\quad + g_1 v_{k,k} v_{n-2,k} + g_1 v_{k-1,k} v_{n-1,k} = \\ &= v_{2k-3,k} v_{n+1,k} + g_1 v_{2k-4,k} v_{n-k+2,k} + g_1 v_{2k-5,k} v_{n-k+3,k} + ... + \\ &\quad + g_1 v_{k,k} v_{n-2,k} + g_1 v_{k-1,k} v_{n-1,k} = \\ &= (g_k v_{2k-4,k} + g_1 v_{k-3,k}) v_{n+1,k} + g_1 v_{2k-4,k} v_{n-k+2,k} + g_1 v_{2k-5,k} v_{n-k+3,k} + ... + \\ &\quad + g_1 v_{k,k} v_{n-2,k} + g_1 v_{k-1,k} v_{n-1,k} = \\ &= v_{2k-4,k} (g_k v_{n+1,k} + g_1 v_{n-k+2,k}) + g_1 v_{2k-5,k} v_{n-k+3,k} + ... + \\ &\quad + g_1 v_{k,k} v_{n-2,k} + g_1 v_{k-1,k} v_{n-1,k} = \\ &= v_{2k-4,k} v_{n+2,k} + g_1 v_{2k-5,k} v_{n-k+3,k} + ... + g_{1,k} v_{k,k} v_{n-2,k} + g_1 v_{k-1,k} v_{n-1,k} = ... = \\ &= v_{k-1,k} v_{n+k-1,k} + g_1 v_{k-2,k} v_{n,k} = \\ &= g_k v_{n+k-1,k} + g_1 v_{n,k} \,. \end{aligned}$$

Нехай залежність (4) виконується для $m-k$, $m-k+1$, . . . , $m-1$. Покажемо, що вона виконується для m.

$$
\begin{aligned}
v_{n+m,k} &= g_k v_{n+m-1,k} + g_1 v_{n+m-k,k} = \\
&= g_k v_{m-1+(k-2),k} v_{n,k} + g_1 g_k \sum_{i=1}^{k-1} v_{m-1+(k-2)-i,k} v_{n-k+i,k} + \\
&+ g_1 v_{m-k+(k-2),k} v_{n,k} + g_1^2 \sum_{i=1}^{k-1} v_{m-k+(k-2)-i,k} v_{n-k+i,k} = \\
&= g_k v_{m-1+(k-2),k} v_{n,k} + g_1 g_k v_{m-1+(k-2)-1,k} v_{n-k+1,k} + \\
&+ g_1 g_k v_{m-1+(k-2)-2,k} v_{n-k+2,k} + \ldots + g_1 g_k v_{m-1+(k-2)-(k-1),k} v_{n-1,k} + \\
&+ g_1 v_{m-k+(k-2),k} v_{n,k} + g_1^2 v_{m-k+(k-2)-1,k} v_{n-k+1,k} + \\
&+ g_1^2 v_{m-k+(k-2)-2,k} v_{n-k+2,k} + \ldots + g_1^2 v_{m-k+(k-2)-(k-1),k} v_{n-1,k} = \\
&= (g_k v_{m-1+(k-2),k} + g_1 v_{m-k+(k-2),k}) v_{n,k} + \\
&+ g_1 (g_k v_{m-1+(k-2)-1,k} + g_1 v_{m-k+(k-2)-1,k}) v_{n-k+1,k} + \\
&+ g_1 (g_k v_{m-1+(k-2)-2,k} + g_1 v_{m-k+(k-2)-2,k}) v_{n-k+2,k} + \ldots + \\
&+ g_1 (g_k v_{m-1+(k-2)-(k-1),k} + g_1 v_{m-k+(k-2)-(k-1),k}) v_{n-1,k} = \\
&= v_{m+(k-2),k} v_{n,k} + g_1 v_{m+(k-2)-1,k} v_{n-k+1,k} + g_1 v_{m+(k-2)-2,k} v_{n-k+2,k} + \ldots + \\
&+ g_1 v_{m+(k-2)-(k-1),k} v_{n-1,k} = \\
&= v_{m+(k-2),k} v_{n,k} + g_1 \sum_{i=1}^{k-1} v_{m+(k-2)-i,k} v_{n-k+i,k} \,.
\end{aligned}
$$

В окремому випадку, коли $m = n$ залежність (4) буде мати такий вигляд

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

Формула (1) дозволяє отримувати значення для зростаючих n, починаючи з $n = 0$, але певну цікавість становить зворотна процедура, яка складається з того, що елементи обчислюються для спадних n, починаючи з деякого значення $n = l$. Обчислення елементів такої послідовності буде здійснюватись таким чином

$$v_{n,k} = \frac{v_{n+k,k} - g_k \cdot v_{n+k-1,k}}{g_1} \,. \tag{6}$$

Для будь-яких цілих додатних n та m таких, що $1 < m < n$ отримано таку залежність

$$v_{n-m,2} = (-1)^m \cdot g_1^{-(m-1)} \cdot (v_{m-2,2} \cdot v_{n,2} - v_{m-1,2} \cdot v_{n-1,2}) \,. \tag{7}$$

Проведемо аналіз цієї залежності індукцією по m.

Покажемо, що (7) виконується для $m = 2$ і $m = 3$.

$$v_{n-2,2} = g_1^{-1} \cdot (v_{0,2} v_{n,2} - v_{1,2} v_{n-1,2}) = g_1^{-1} \cdot (v_{n,2} - g_2 v_{n-1,2}) \,.$$

$$
\begin{aligned}
v_{n-3,2} &= -g_1^{-2} \cdot (v_{1,2} v_{n,2} - v_{2,2} v_{n-1,2}) = -g_1^{-2} \cdot (g_2 v_{n,2} - (g_2^2 + g_1) \cdot v_{n-1,2}) = \\
&= g_1^{-2} \cdot (-g_2 v_{n,2} + g_2^2 v_{n-1,2} + g_1 v_{n-1,2}) = -\frac{g_2}{g_1} \cdot \frac{v_{n,2} - g_2 v_{n-1,2}}{g_1} + \frac{v_{n-1,2}}{g_1} = \\
&= \frac{v_{n-1,2} - g_2 v_{n-2,2}}{g_1} \,.
\end{aligned}
$$

Припустимо, що залежність (7) виконується для $m+1$, $m+2$. Покажемо, що вона виконується для m.

Згідно формули (1)

$$v_{n-m,2} = g_2 v_{n-m-1,2} + g_1 v_{n-m-2,2} = g_2 v_{n-(m+1),2} + g_1 v_{n-(m+2),2} =$$

$$= (-1)^{m+1} g_1^{-m} g_2 (v_{m-1,2} v_{n,2} - v_{m,2} v_{n-1,2}) +$$

$$+ (-1)^{m+2} g_1^{-m} (v_{m,2} v_{n,2} - v_{m+1,2} v_{n-1,2}) =$$

$$= (-1)^m g_1^{-m} (-g_2 v_{m-1,2} v_{n,2} + g_2 v_{m,2} v_{n-1,2} + v_{m,2} v_{n,2} - v_{m+1,2} v_{n-1,2}) =$$

$$= (-1)^m g_1^{m-1} \cdot (\frac{v_{m,2} - g_2 v_{m-1,2}}{g_1} v_{n,2} - \frac{v_{m+1,2} - g_2 v_{m,2}}{g_1} v_{n-1,2}).$$

Враховуючи формулу (6), отримаємо

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

Обчислення за формулою (6) може продовжуватись і для $n < 0$, тобто існує два виду послідовностей. Перший вид послідовності формується для *n* – додатних за формулою (1). Другий вид послідовності формується для *n* – від'ємних за формулою (6). Назвемо V_k^--послідовністю послідовність чисел, що обчислюються за формулою (6) для n – від'ємних при початкових значеннях $v_{-1,k} = 0$, $v_{-2,k} = g_1^{-1}$ для $k = 2$; $v_{-1,k} = 0$, $v_{-2,k} = g_1^{-1}$, $v_{-3,k} = v_{-4,k} = ... = v_{-k,k} = 0$ для $k > 2$.

Послідовність чисел, яка складається з V_k^+-послідовності та V_k^--послідовності назвемо V_k – послідовністю.

Висновки. Розглянуто рекурентну V_k-послідовність, яка складається з двох послідовностей V_k^+ і V_k^-. Встановлено, що елементи V_k^+-послідовності можуть обчислюватись трьома шляхами. Залежність (2) для безпосереднього обчислення елементів через початкові елементи може використовуватись для дослідження послідовності щодо криптографічної стійкості методів на її основі.

Прискорене обчислення елементів рекурентної послідовності для зростаючих *n* можна здійснювати згідно залежності (4), а для спадних *n* (для *k*=2) згідно залежності (7). Дані залежності стануть основою побудови криптографічних методів.

Література

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

2. H. Lehmer. An extended theory of Lucas' functions.: Annals of Math, 1930.– PP. 419-448.

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