Литература

1. Разработка методов повышения эффективности обнаружения и локализации мест протекания трубопроводов. Заключительный отчет госбюджетной НИР [Текст] / Руководитель НИР В.С. Чернега. – Севастополь: СевНТУ, 2004. – 145 с.
2. Brechbuehl, M. Beitrag zur akustischen Ortung von Leckstellen [Текст] / M. Brechbuehl. – Zuerich: Diss.ETH, 1988. – 182 с.
3. Строганов, В. А. Классификация сигналов утечек подземных трубопроводов с помощью искусственных нейронных сетей [Текст] / В. А. Строганов // Восточно-Европейский журнал передовых технологий, 2012.– № 6/4(60).– С. 33–36.
4. Строганов, В. А. Экспериментальное исследование сигналов утечек подземных трубопроводов [Текст] / В.А. Строганов, В. Н. Хоролич// Вестник СевНТУ. Сер. Информатика, электроника, связь: Сб. науч. тр. – Севастополь, 2010.– Вып.101.– С. 29–32.
5. Mallat, S. A wavelet tour of signal processing [Текст] / S.Mallat.– San Diego: Academic Press, 2001.– 620 с.
6. Daubechies, I. Ten lectures on wavelets [Текст] / I. Daubechies// CBMS-NSF conference series in applied mathematics. SIAM, 1992.– Том. 61.– 357 с.
7. Chui Charle, K. Wavelets: A Mathematical Tool for Signal Analysis [Текст] / Charles K. Chui // Siam Monographs on Mathematical Modeling and Computation.– 1997.–Том 1.– 210 с.
8. Mallat, S. A theory for multiresolution signal decomposition: the wavelet representation [Текст] / S. Mallat // IEEE Pattern Anal. and Machine Intell., 1989.– Том 11.– №7.– С. 674–693.
9. Chui Charles, K. An Introduction to Wavelets [Текст] / Charles K. Chui.– San Diego: Academic Press, 1992.– 264 с.
10. Бондарев, В. Н. Цифровая обработка сигналов: методы и средства [Текст] / В. Н. Бондарев, Г. Трестер, В. С. Чернега.– Севастополь: Изд-во СевГТУ, 1999.– 398 с.

УДК 681.3.067

ОЦІНЮВАННЯ КРИПТОСТІЙКОСТІ МЕТОДІВ ШИФРУВАННЯ ІНФОРМАЦІЇ НА ОСНОВІ РЕКУРЕНТНИХ ПОСЛІДОВНОСТЕЙ

Ю. Є. Яремчук
Кандидат технічних наук, доцент, професор кафедри, директор Центру
Центр інформаційних технологій і захисту інформації
Кафедра адміністративного та інформаційного менеджменту
Вінницький національний технічний університет
Хмельницьке шосе, 95, м. Вінниця, 21021, Україна
E-mail: yurevyar@vntu.net

В роботі проведено оцінювання криптографічної стійкості методу асиметричного шифрування інформації та методу шифрування інформації без попереднього розподілу ключів на основі математичного апарату рекурентних послідовностей. В результаті дослідження встановлено, що криптостійкість методів знаходиться на достатньому рівні, принаймні не меншому, ніж відомих аналогів

Ключові слова: захист інформації, криптографія, шифрування, розподіл ключів, криптографічна стійкість, рекурентні послідовності

В работе проведено оценивание криптографической стойкости метода ассиметричного шифрования информации и метода шифрования информации без предварительного распределения ключей на основе математического аппарата рекуррентных последовательностей. В результате исследования установлено, что криптостойкость методов находится на достаточном уровне, по крайней мере не меньшем, чем известных аналогов

Ключевые слова: защита информации, криптография, шифрование, распределение ключей, криптографическая стойкость, рекуррентные последовательности

1. Вступ

На сьогодні криптографічні методи [1, 2] мають широке застосування. При цьому актуальним залишається вирішення проблеми спрощення обчислень під час криптографічних перетворень, особливо в методах, що базуються на технології відкритого ключа, де використовуються великі ключі та числа великої розрядності. Виходячи з цього, певний інтерес викликає апарат на основі рекурентних послідовностей [3],

© Ю. Є. Яремчук, 2013

який дозволяє за певних умов спрощувати обчислення методів, що базуються на його основі. Так в роботах [4, 5] запропоновано використовувати рекурентні послідовності Люка за модулем простого числа замість традиційного піднесення до степеня. Однак у роботі [6] було вказано на певну слабкість такого підходу щодо криптографічної стійкості.

В роботах [7] та [8] розглянуто методи відповідно асиметричного шифрування інформації та метод шифрування без попереднього розподілу ключів, які базуються на використанні математичного апарату рекурентних $\mathbf{V}_k$ та U_k послідовностей, а також їх аналітичних залежностей. При цьому відбувається заміна модулярного піднесення до степеня обчисленням за модулем елементу U_k послідовності з певним індексом. Метод асиметричного шифрування інформації має за певних умов меншу складність обчислень у порівнянні з відомим методом Ель-Гамаля [9], а метод шифрування без попереднього розподілу ключів забезпечує значне спрощення обчислень у порівнянні з відомим методом Шаміра [10].

V_k – послідовністю називається послідовність чисел, яка складається з V_k^+ – послідовності та V_k^- – послідовності [7].

V_k^+ послідовністю називається 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 $k = 2$; $v_{0,k} = v_{1,k} = ... = v_{k-3,k} = 0$, $v_{k-2,k} = 1$, $v_{k-1,k} = g_k$ для $k > 2$; де g_1, g_k цілі числа; n і k - цілі додатні.

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

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

V_k^- – послідовністю називається послідовність чисел, що обчислюються за формулою

$$v_{n,k} = \frac{v_{n+k,k} - g_k \cdot v_{n+k-1,k}}{g_1}. \qquad (3)$$

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 $k > 2$.

$\mathbf{U}_k$ – послідовністю [7] називається послідовність чисел, що обчислюються за формулою

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

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.

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

$$u_{n,k} = g_k^{n-(k-2)} + \sum_{i=1}^{\left(\frac{n}{k}\right)} g_k^{n-(k-2)-ki} \times \times g_1^i \left(\sum_{j=1}^{k-1} C^{i-1}_{n-(k-1)i-j} \cdot g_k^{k-j-1} \cdot g_j + C^i_{n-(k-1)-(k-1)i} \right). \qquad (5)$$

Для будь-яких цілих додатних n, m та k [7]

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

Для будь-яких цілих додатних n та k, таких що $n \geq k$, в [7] представлено залежність, яка дозволяє обчислювати елементи $\mathbf{U}_k$ – послідовності тільки на основі елементів V_k^+ – послідовності

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

На основі даного математичного апарату запропоновано методи асиметричного шифрування [7] та шифрування інформації без попереднього розподілу ключів [8]. При цьому актуальним стає дослідження криптографічної стійкості запропонованих методів шифрування та порівняння отриманих результатів з відомими аналогами.

2. Мета та задачі дослідження

Метою роботи є оцінювання криптографічної стійкості методів асиметричного шифрування інформації та методу шифрування без попереднього розподілу ключів, що базуються на використанні математичного апарату рекурентних $\mathbf{V}_k$ та U_k послідовностей, а також порівняння їх з відомими аналогами.

Виходячи з мети роботи, задачею є дослідження методів шифрування, представлених в роботах [7] та [8], з точки зору їх криптографічної стійкості та порівняння їх з відомими методами відповідно Ель-Гамаля та Шаміра.

3. Оцінювання криптографічної стійкості методів шифрування інформації

Як відомо існує два основних підходи до визначення стійкості криптографічних методів: теоретико-інформаційний та теоретико-складносний [1].

Теоретико-інформаційний підхід не може бути застосований до криптосистем, що базуються на технології відкритого ключа, оскільки в них алгоритм шифрування інформації та відкритий ключ є загальнодоступними.

Для визначення криптографічної стійкості представлених в [7] та [8] методів шифрування інформації використаємо теоретико-складносний підхід. Реалізуючи цей підхід до розглянутих методів шифрування визначимо таке.

По-перше, представлені методи шифрування використовують фіксовані значення параметрів k, q, H. Наприклад, $k = 3$, $q = 16$, $H = 32$. Для застосування теоретико-складосного підходу необхідно, щоб задача, обчислювальну складність якої передбачається визначити, була масовою, а сам метод шифрування розглядався, як математична модель. Ця модель залежить від деякого параметру, що називають параметром безпеки, який може приймати будь-які великі значення. Будемо вважати, що параметр безпеки будь-яке натуральне число.

По-друге, визначення стійкості криптографічного методу залежить від тієї задачі, яка стоїть перед зловмисником, та від того, яка інформація про метод йому доступна. Будемо вважати, що противнику відома така інформація:

алгоритми шифрування - дешифрування;

параметри алгоритму k, p, g_i, $i=\overline{1,k}$;

відкритий ключ;

всі зашифровані повідомлення, що передаються в процесі шифрування від Передавача до Приймача та навпаки.

По-третє, необхідно визначити, який об'єм обчислень вважати «практично нездійсненим». З вищесказаного випливає, що ця величина не може бути константою, а повинна бути представлена, як функція від зростаючого параметру безпеки. Згідно тезису Едмонса [1], алгоритм, який противник застосовує для зламу, вважається ефективним, якщо час його виконання обмежений деяким поліномом від довжини вхідного слова, тобто, в нашому випадку, від параметру безпеки. В протилежному випадку, будемо вважати, що обчислення за даним алгоритмом є практично нездійсненими.

По-четверте, необхідно визначити, яку ймовірність можна вважати «знехтувано малою». Будемо вважати такою будь-яку ймовірність, яка для будь-якого поліному c та для всіх достатньовеликих n неперевищує $1/c(n)$, де n параметр безпеки.

Таким чином, проблема обґрунтування стійкості розроблених алгоритмів шифрування звелась до доведення відсутності поліноміального алгоритму, який вирішує задачу, що стоїть перед зловмисником. Визначимо можливі спроби криптоаналізу та математичні задачі, які їм еквівалентні, для кожного з розглянутих методів шифрування.

Здійснюючи криптоаналіз методу асиметричного шифрування на основі рекурентних $\mathbf{V}_k$ та $\mathbf{U}_k$ послідовностей зловмиснику відомі параметри k, p, g_i, $i=\overline{1,k-1}$, відкритий ключ $u_{a-i,k} \bmod p$, $i=\overline{0,k-1}$, а також $u_{b-i,k} \bmod p$, $i=\overline{0,k-1}$ та y_2, які Передавач передає до Приймача.

Перше, що може спробувати зловмисник, - отримати секретний ключ, а шляхом послідовних обчислень за модулем p за формулою (4), доки не буде отримано значення $u_{a,k} \bmod p$. Тоді, якщо зловмиснику це вдасться, він зможе обчислити $v_{a+i,k} \bmod p$, $i=\overline{-(k-1),k-2}$, за алгоритмами прискореного обчислення елементів V_k^+ послідовності, потім обчислити $u_{b+a,k} \bmod p$ за формулою (6) та дешифрувати повідомлення M.

Аналіз показує, що обчислення $u_{a,k}$ за модулем p з використанням формули (4) потребує виконання $3aH(4H+5)$ операцій над машинними одиницями інформації.

Навіть якщо продуктивність комп'ютера становить 2^{34} операцій за секунду і, якщо розрядність а становить 1024 розряди, $H=32$, то для обчислення $u_{a,k}$ за модулем p з використанням формули (4) потрібно приблизно 2^{979} років, що є практично нездійсненим.

Тут слід зазначити, що замість рекурентної формули (4) для отримання елементу $u_{a,k} \bmod p$ можна використовувати формулу безпосереднього обчислення цього елементу через початкові елементи, або формулу безпосереднього обчислення елементів $v_{a+i,k} \bmod p$, $i=\overline{-k,-1}$, через початкові елементи, а потім обчислення за модулем p елементу $u_{a,k} \bmod p$ за формулою (7).

Аналіз формул безпосереднього обчислення елементів $\mathbf{U}_k$ та V_k послідовностей через початкові елементи (2) та (5) показує, що дані формули є більш складними за кількістю виконуваних операцій, ніж формула (1).

Це означає, що спроба обчислення $u_{a,k} \bmod p$ за допомогою послідовного використання формули (2) або (5) є також практично нездійсненою.

Для отримання елементів $v_{a+i,k} \bmod p$, $i=\overline{-(k-1),k-2}$, може бути застосований інший спосіб, який полягає у використанні формули (7) та відомих елементів $u_{a-i,k} \bmod p$, $i=\overline{0,k-1}$, для обчислення за модулем p елементів $v_{a+i,k} \bmod p$ для $i=\overline{-2k+1,-1}$, а потім і для $i=\overline{0,k-2}$ за формулою (1) на основі вже обчислених елементів.

Реалізація цієї спроби зводиться до розв'язання такої системи рівнянь

$$\begin{cases} u_{a,k} \bmod p = (g_k v_{a-1,k} + g_1 g_1 v_{a-2,k} + g_1 g_2 v_{a-3,k} + \ldots + g_1 g_{k-1} v_{a-k,k}) \bmod p \\ u_{a-1,k} \bmod p = (g_k v_{a-2,k} + g_1 g_1 v_{a-3,k} + g_1 g_2 v_{a-4,k} + \ldots + g_1 g_{k-1} v_{a-k-1,k}) \bmod p \\ \ldots \\ u_{a-(k-1),k} \bmod p = (g_k v_{a-k,k} + g_1 g_1 v_{a-k-1,k} + g_1 g_2 v_{a-k-2,k} + \ldots + g_1 g_{k-1} v_{a-2k+1,k}) \bmod p. \end{cases} \quad (8)$$

Система рівнянь (8) це система з k рівнянь та $k+1$ невідомими.

Математична задача розв'язання такої системи рівнянь, враховуючи велику розрядність коефіцієнтів та невідомих, на цей день не має ефективного поліноміального алгоритму, а отже є практично нездійсненою. Наступне, що може спробувати противник, знайти секретний ключ а, виходячи з формули (5), використовуючи відомий елемент $u_{a,k} \bmod p$.

Ця задача є більш складною ніж відома задача знаходження дискретного логарифму, оскільки формула (5) містить не одне число у степені, а суму декількох чисел з різними степенями. Тому її розв'язання також не може бути практично здійснено.

Проведемо тепер дослідження криптографічної стійкості методу шифрування інформації без попереднього розподілу ключів на основі рекурентних $\mathbf{V}_k$ та U_k послідовностей.

Здійснюючи криптоаналіз цього методу зловмиснику відомі параметри k, p, g_i, $i=\overline{1,k-1}$, а також $M \cdot u_{a-i,k} \bmod p$, $i=\overline{0,k-1}$, $M \cdot u_{a+b-i,k} \bmod p$, $i=\overline{0,k-1}$, та $M \cdot u_{b-i,k} \bmod p$, $i=\overline{0,k-1}$, що передаються в процесі шифрування.

Виходячи з цього можемо отримати таке рівняння

$$M \cdot (u_{a,k} + u_{b,k} + u_{a+b,k}) \bmod p = \gamma, \quad (9)$$

де γ - відоме значення.

З (9) видно, що для розшифрування повідомлення M необхідно визначити $u_{a,k} \bmod p$, $u_{b,k} \bmod p$ та $u_{a+b,k} \bmod p$.

Для цього виконаємо попарне ділення відомих добутків. Як наслідок, отримаємо таку систему рівнянь

$$\begin{cases} \dfrac{u_{a,k}}{u_{b,k}} \bmod p = \gamma_1 \\ \dfrac{u_{a,k}}{u_{a+b,k}} \bmod p = \gamma_2 \\ \dfrac{u_{b,k}}{u_{a+b,k}} \bmod p = \gamma_3 \end{cases}, \quad (10)$$

де γ_1, γ_2, γ_3 - відомі значення.

Аналіз системи (10) показує, що в ній третє рівняння може бути отримано з першого та другого рівняння. Тому система рівнянь (10) набуває такого вигляду

$$\begin{cases} \dfrac{u_{a,k}}{u_{b,k}} \bmod p = \gamma_1 \\ \dfrac{u_{a,k}}{u_{a+b,k}} \bmod p = \gamma_2 \end{cases}. \quad (11)$$

Система рівнянь (11) - це система з двох рівнянь та трьома невідомими $u_{a,k}$, $u_{b,k}$ і $u_{a+b,k}$. Як вже зазначалось раніше, розв'язання подібної системи є практично нездійсненою задачею.

На основі відомої зловмиснику інформації, крім рівняння (9), можуть бути отримані рівняння у такому вигляді

$$M \cdot \sum_i u_{a-j,k} = \gamma',$$

$$M \cdot \sum_i u_{b-j,k} = \gamma'',$$

$$M \cdot \sum_i u_{a+b-j,k} = \gamma''',$$

де γ', γ'', γ''' - відомі значення,

i, j - будь-які цілі числа в діапазоні $[0, k-1]$.

Аналіз показує, що будь-які спроби розшифрування повідомлення M, використовуючи ці рівняння, аналогічні проведеній вище спробі і зводяться до розв'язання системи з t рівнянь та $t+1$ невідомими. Тобто всі ці спроби є практично нездійсненими.

4. Висновки

Таким чином, застосовуючи теоретико-складнісний підхід, проведено оцінювання криптографічної стійкості методів асиметричного шифрування інформації та шифрування без попереднього розподілу ключів на основі рекурентних $\mathbf{V}_k$ та $\mathbf{U}_k$ - послідовностей. Результати оцінювання показали, що усі спроби зловмисника є практично нездійсненими і зводяться в основному до задачі розв'язання системи з k рівнянь та $k+1$ невідомими.

Порівнюючи отримані результати з відомими методами Ель-Гамаля та Шаміра слід зазначити, що задача вирішення вказаної системи рівнянь є принаймні не менш складною щодо розв'язання, ніж задача дискретного логарифмування, на якій базуються відомі методи.

Враховуючи вищесказане, можна стверджувати, що методи шифрування інформації на основі рекурентних $\mathbf{V}_k$ та $\mathbf{U}_k$ - послідовностей забезпечують достатній рівень криптографічної стійкості і можуть мати поширення в інформаційних системах.

Литература

1. Menezes, A. J. Handbook of Applied Cryptography [Текст] / A. J. Menezes, P.C. van Oorschot, S.A. Vanstone. – CRC Press, 2001. – 816 p.
2. Van Tilborg, Henk C. A. Fundamentals of cryptology. A Professional Reference and Interactive Tutorial [Текст] / Henk C.A. van Tilborg. – Kluwer Academic Publishers, 2000. – 512 p.
3. Маркушевич, А. И. Возвратные последовательности [Текст] / А. И. Маркушевич. – М.: Наука, 1975. – 48 с.
4. Smith, P. LUC: A new public key system [Текст] / P. Smith, M. Lennon // Proceedings of the IFIP TC11 Ninth International Conference on Information Security. North-Holland. - 1993. - P.103–117.
5. Smith, P. A public-key cryptosystem and a digital signature system based on the Lucas function analogue to discrete logarithms [Текст] / P. Smith, C. Skinner // In Advances in Cryptology Asiacrypt '94. – Springer-Verlag, 1995. – P. 357–364.
6. Bleichenbacher, D. Some remarks on Lucas-based cryptosystems [Текст] / D. Bleichenbacher, W. Bosma, A. Lenstra // In Advances in Cryptology Crypto'95. – Springer-Verlag, 1995. – P.386–396.
7. Яремчук, Ю. Є. Спеціалізовані процесори асиметричного шифрування інформації на основі рекурентних послідовностей [Текст] / Ю.Є. Яремчук // Правове, нормативне та метрологічне забезпечення системи захисту інформації в Україні. – Випуск 2(24), 2012. – С. 63–69.
8. Яремчук, Ю.Є. Спеціалізовані процесори шифрування інформації без попереднього розподілу ключів на основі рекурентних послідовностей [Текст] / Ю.Є. Яремчук // Радіотехніка. – Вип. 172, 2013. – С. 109–117.
9. ElGamal, T. A public key cryptosystem and a signature scheme based on discrete logarithms [Текст] / T. ElGamal // IEEE Intern. Symp. Informat. Theory 1985. -V.IT31. №4. P.469-472.
10. Massey, J. L. An introduction to contemporary cryptology [Текст] / J.L. Massey // Proceedings of the IEEE. – 1988. – T.76. – P. 533–549.