УДК 681.3.06

Ю.М. Рябуха

Харківський університет Повітряних Сил ім. І. Кожедуба, Харків

МЕТОД ФОРМУВАННЯ ПСЕВДОВИПАДКОВИХ ПОСЛІДОВНОСТЕЙ МАКСИМАЛЬНОГО ПЕРІОДУ ІЗ ВИКОРИСТАННЯМ МОДУЛЯРНИХ ПЕРЕТВОРЕНЬ

Досліджуються методи формування послідовностей псевдовипадкових чисел, стійкість яких базується на зведенні задачі відновлення таємного ключа до вирішення добре відомої і надзвичайно складної математичної задачі. Пропонується удосконалений метод формування псевдовипадкових послідовностей із використанням модулярних перетворень, стійкість якого базується на вирішенні добре відомої проблеми RSA, але який, на відміну від відомих, дозволяє формувати послідовності максимального періоду.

Ключові слова: *псевдовипадкові послідовності, модулярні перетворення, стійкість претворення.*

Вступ

Постановка проблеми у загальному вигляді та аналіз літератури. Важливим завданням із забезпечення національної безпеки нашої країни є захист інформаційного середовища, в тому числі, захист вітчизняних інформаційних систем і технологій [1]. Особливу актуальність питання інформаційної безпеки набувають у системах управляння критичного застосування, порушення роботи яких може призвести до катастрофічних наслідків в промисловості, екології, військовій сфері. Тому розробка та дослідження перспективних засобів захисту інформації, їх теоретичне обґрунтування та сертифікація вповноваженими органами є надзвичайно важливим завданням, яке пов'язане із виконанням цілої низки державних та галузевих науково-технічних програм і проектів.

Серед відомих технологій криптографічного захисту інформації особливе місце займають методи формування псевдовипадкових послідовностей [2]. Вони використовуються практично в усіх механізмах криптографічного захисту інформації і призначені для вироблення послідовностей чисел, які володіють певними статистичними властивостями [3, 4]. Найбільш вдалими є методи, що засновані на медулярних перетвореннях, їх стійкість базується на зведенні задачі відновлення таємного ключа до вирішення добре відомої і надзвичайно складної математичної задачі з теорії чисел, наприклад, факторизації, дискретного логарифмування та ін. **Метою статті** є дослідження властивостей відомого генератора RSA, стійкість якого базується на вирішенні добре відомої теоретико-складної проблеми RSA, розробка удосконаленого методу формування псевдовипадкових послідовностей, який, на відміну від генератора RSA, дозволяє формувати послідовності максимального періоду.

Основний розділ

1. Метод формування псевдовипадкових послідовностей RSA. Відомий метод формування псевдовипадкових послідовностей RSA заснований на використанні модулярних перетворень, його стійкість базується на зведенні задачі відновлення таємного ключа до вирішення добре відомої і надзвичайно складної математичної задачі, відомої з теорії чисел як проблема RSA. Вона формулюється наступним чином [2, 3].

Нехай задане ціле число n через добуток двох великих простих чисел p і q, тобто $n = p \cdot q$. Нехай також задане ціле число e, взаємно просте із числом $p-1 \quad q-1$, тобто найбільший загальний дільник e і $p-1 \quad q-1$ дорівнює одиниці. Проблема RSA полягає у знаходженні такого цілого числа m по відомому цілому числу c, що $m^e \equiv c \bmod n$. Для фіксованих чисел n і e існує обчислювально ефективний алгоритм обчислення числа c по відомому числу m. Однак зворотня задача (проблема RSA), що полягає в обчисленні числа m по заданому числу c при фіксованих числах n і e, є надзвичайно складною задачею, на сьогоднішній день не відомо обчислювально ефективних алгоритмів її вирішення.

Відомий метод формування псевдовипадкових послідовностей RSA [2] ґрунтується на тому, що ключова послідовність подається у вигляді вектору x_0, який ініціалізує початкове значення аргументу функції $f\ x = x^e \bmod n$ модульного зведення у ступінь. У якості модуля n обирається добуток великих простих чисел p і q, у якості ступеня e обирається число, взаємно просте з $p-1 \cdot q-1$. Наступне значення аргументу функції обраховується за допомогою пристроїв модульного зведення у ступінь а вихідні елементи послідовності псевдовипадкових чисел формуються шляхом зчитування значення функції модульного зведення за допомогою відповідних пристроїв, тобто шуканою послідовністю біт довжини m буде послідовність

$$b_0 \quad b_1 \quad b_2 \quad \ldots \quad b_i \quad \ldots \quad b_{m-1}, \ i = \overline{0,\ m-1},$$

де b_i – молодший біт числа x_i,

$$x_{i+1} = f\ x_i\ =\ x_i^{e}\ \mathrm{mod}\ n\ .$$

Задача вираховування функції $f\ x^{-1}$, яка є зворотною до функції модульного зведення у ступінь $f\ x\ = x^{e} \bmod n$, тобто вирахування деякого значення x_i за відомим значенням x_{i+1} є важко розв'язуваною теоретико-складною задачею (проблемою RSA), щодо вирішення якої на сьогоднішній день невідомо ефективних алгоритмів рішення. Тому цей спосіб формування послідовностей псевдовипадкових чисел є стійким.

2. Дослідження періодичних властивостей генератору RSA. Для проведення досліджень періодичних властивостей генератору RSA було розроблено його програмну реалізацію. Експериментальні дослідження полягали у вивченні періодичних властивостей відповідного генератору шляхом повного перебору всіх ключових послідовностей (всіх можливих значень вектору x_0), оцінці відповідних довжин періоду L формованих псевдовипадкових послідовностей та порівнянні із максимальною довжиною періоду $L_{max} = \min\ 2^{M} - 1, n - 1$, де M – бітова довжина ключових даних (бітова довжина вектору x_0).

При проведені експериментальних досліджень було обрано такі вихідні дані.

Експеримент 1. Вихідні дані: $p = 17$, $q = 37$, $n = 629$, $e = 257$. У якості таємного ключа обиралися всі цілі числа від 2 до 628.

Експеримент 2. Вихідні дані: $p = 131$, $q = 163$, $n = 21353$, $e = 1031$. У якості таємного ключа обиралися всі цілі числа від 2 до 21352.

Експеримент 3. Вихідні дані: $p = 521$, $q = 1031$, $n = 537151$, $e = 2029$. У якості таємного ключа обиралися всі цілі числа від 2 до 537150.

Експеримент 4. Вихідні дані: $p = 2053$, $q = 4099$, $n = 8415247$, $e = 2051$. У якості таємного ключа обиралися всі цілі числа від 2 до 8415246.

Отримані результати експериментальних досліджень узагальнені та наведені у якості діаграм на рис. 1 – 4. На діаграмах наведено розподіл кількості ключів за довжинами відповідних періодів формованих псевдовипадкових послідовностей, тобто, розподіл кількостей K таких векторів x_0, які дають відповідне значення періоду L. Таким чином, проведені експериментальні дослідження довели, що відомий генератор RSA володіє істотним недоліком – період формованих послідовностей не є максимальним. Фактично, було з'ясовано, що період формованих послідовностей менший за максимальний на 2-5 порядків, при збільшенні довжини максимального періоду ця різниця також збільшується.

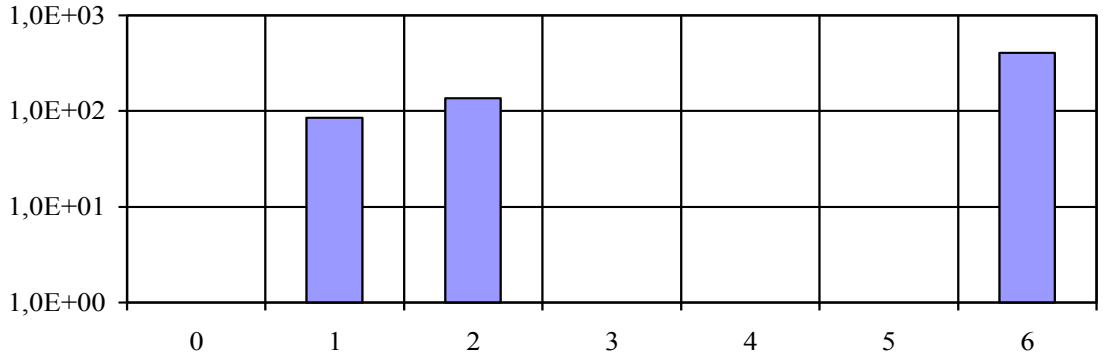

Рис. 1. Розподіл кількості ключів по довжинам періодів формованих послідовностей (експеримент 1, $L_{max} = 628$)

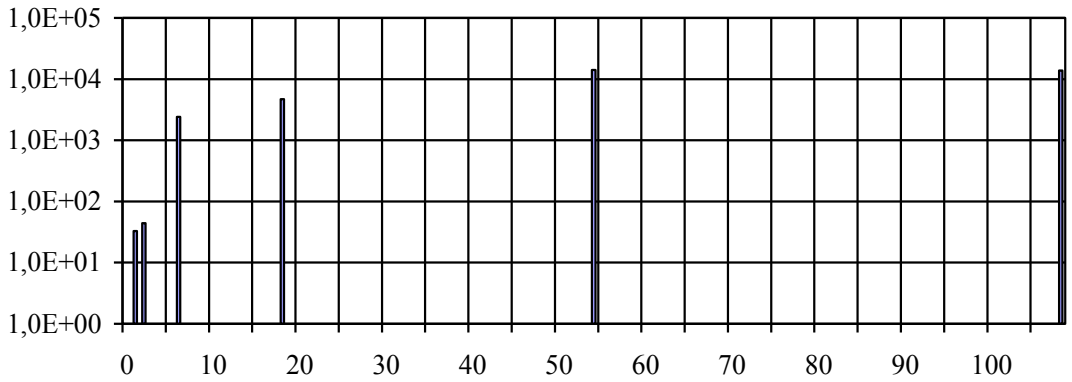

Рис. 2. Розподіл кількості ключів по довжинам періодів формованих послідовностей (експеримент 2, $L_{max} = 21352$)

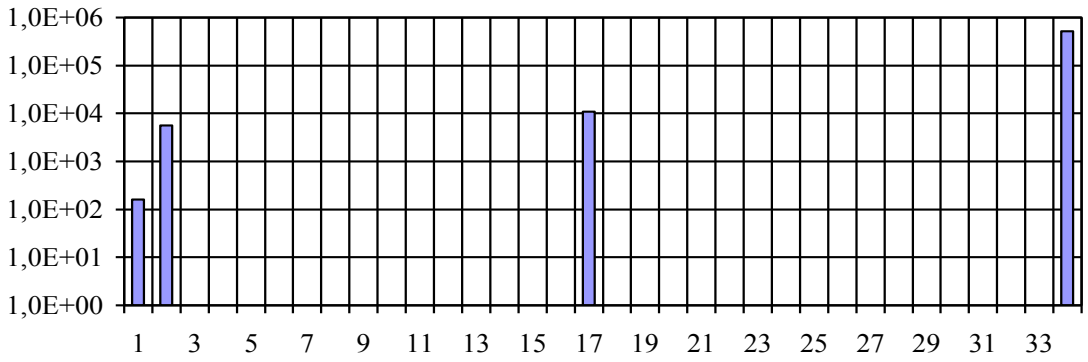

Рис. 3. Розподіл кількості ключів по довжинам періодів формованих послідовностей (експеримент 3, $L_{max} = 537150$)

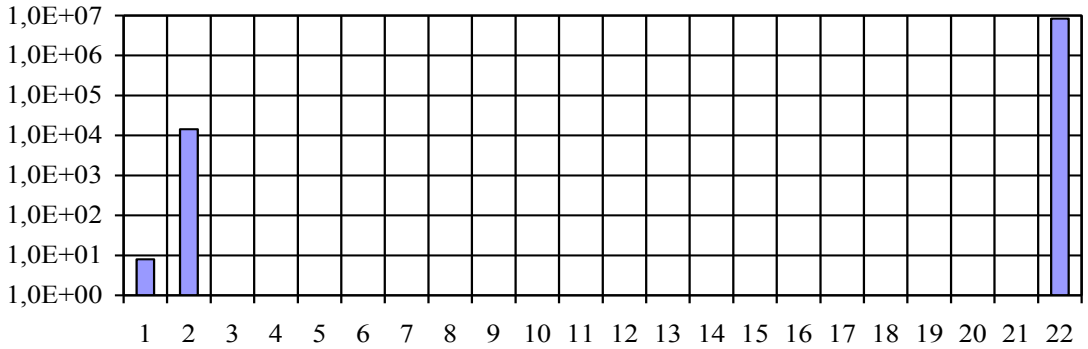

Рис. 4. Розподіл кількості ключів по довжинам періодів формованих послідовностей (експеримент 4, $L_{max} = 8415248$)

3. Розробка удосконаленого методу формування псевдовипадкових послідовностей максимального періоду із використанням модулярних перетворень. Проведені дослідження довели, що недоліком методу-прототипу (методу RSA) є те, що він не дозволяє формувати послідовності псевдовипадкових чисел максимального періоду, що суттєво зменшує його ефективність та обмежує можливості щодо практичного використання.

В основу розробленого методу поставлена задача створити спосіб формування послідовностей псевдовипадкових чисел який, за рахунок додаткового введення рекурентних перетворень, що реалізуються, наприклад, за допомогою лінійних рекурентних регістрів зі зворотними зв'язками, дозволить формувати послідовності псевдовипадкових чисел максимального періоду, що підвищить його ефективність та розширить можливості щодо практичного використання [5].

Поставлена задача вирішується за рахунок додаткового введення рекурентних перетворень які дозволяють формувати послідовності псевдовипадкових чисел максимального періоду. Технічний результат, який може бути отриманий при застосуванні відповідного генератору, полягає в отриманні можливості формувати послідовності псевдовипадкових чисел максимального періоду, що підвищує ефективність та розширює його можливості.

Сутність запропонованого методу формування послідовностей псевдовипадкових чисел полягає в тому, що ключова послідовність подається у вигляді вектору x_0, який ініціалізує початкове значення аргументу функції $f\ x = x^e \bmod n$ модульного зведення у ступінь та початкове значення y_0 рекурентного перетворення $L\ y$, що реалізуються, наприклад, за допомогою лінійних рекурентних регістрів зі зворотними зв'язками. У якості модуля n обирається добуток великих простих чисел p і q , у якості ступеня e обирається число, взаємно просте з $p-1 \cdot q-1$. Наступне значення аргументу функції обраховується за допомогою пристроїв модульного зведення у ступінь та за допомогою рекурентного перетворення, що реалізується, наприклад, за допомогою лінійних рекурентних регістрів зі зворотними зв'язками. Вихідні елементи послідовності псевдовипадкових чисел формуються шляхом зчитування значення функції модульного зведення за допомогою відповідних пристроїв, тобто шуканою послідовністю біт довжини m буде послідовність

$$b_0 \quad b_1 \quad b_2 \quad \ldots \quad b_i \quad \ldots \quad b_{m-1}, \ i = \overline{0,\ m-1},$$

де b_i – молодший біт числа x_i,

$$x_{i+1} = f\ x_i + L\ y_i \ = \ x_i + L\ y_i \ ^e \bmod n .$$

Задача вираховування функції $f(x)^{-1}$, яка є зворотною до функції модульного зведення у ступінь $f(x) = x^e \bmod n$, тобто вирахування деякого значення $x_i + L(y_i)$ за відомим значенням x_{i+1} є важко

розв'язуваною теоретико-складною задачею (проблемою RSA), щодо вирішення якої на сьогоднішній день невідомо обчислювально ефективних алгоритмів. Тому цей спосіб формування послідовностей псевдовипадкових чисел є стійким. Додатково введене рекурентне перетворення L_y, що реалізуються, наприклад, за допомогою лінійних рекурентних регістрів зі зворотними зв'язками, дозволяє формувати послідовності псевдовипадкових чисел максимального періоду.

Запропонований спосіб може бути реалізовано у вигляді пристрою, структурна схема якого зображена на рис. 5 [5].

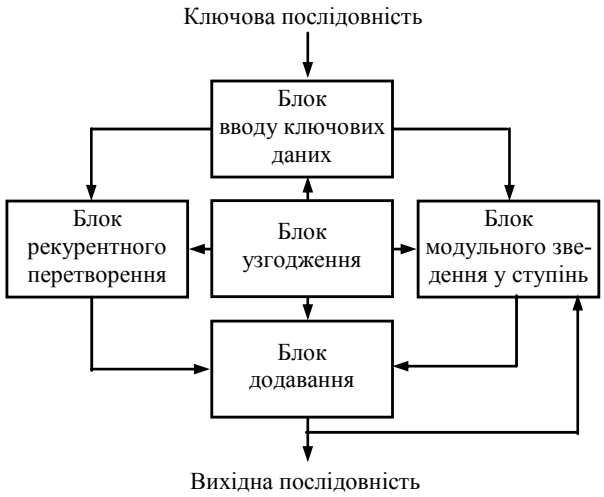

Рис. 5. Структурна схема пристрою формування псевдовипадкових послідовностей

Таким чином, за рахунок додаткового введення рекурентних перетворень, що реалізуються, наприклад, за допомогою лінійних рекурентних регістрів зі зворотними зв'язками, вдається формувати послідовності псевдовипадкових чисел максимального періоду, що підвищує ефективність та розширює можливості практичного використання.

Висновки

Проведені дослідження показали, що відомі генератори псевдовипадкових послідовностей із застосуванням модулярних перетворень володіють певними недоліками, зокрема період формованих послідовностей не є максимальним. Запропоновано удосконалений метод формування псевдовипадкових послідовностей із використанням модулярних перетворень, стійкість якого базується на вирішенні добре відомої проблеми RSA та який, на відміну від відомих, дозволяє формувати послідовності максимального періоду.

Список літератури

1. Поповский В.В. Защита информации в телекоммуникационных системах: учебник / В.В. Поповский, А.В. Персиков; Харьковский национальный университет радиоэлектроники. – Х.: ООО "Компания Смит", 2006. – 238 с.

2. Иванов М.А. Теория, применение и оценка качества генераторов псевдослучайных последовательностей / М.А. Иванов, И.В. Чугунков. – М.: КУДИЦ-ОБРАЗ, 2003. – 240 с.

3. Шнайер Б. Прикладная криптография. Протоколы, алгоритмы, исходные тексты на языке Си. – М.: Издательство ТРИУМФ, 2002 – 816 с.

4. Final report of European project number IST-1999-12324, named New European Schemes for Signatures, Integrity, and Encryption, April 19, 2004 – Version 0.15 (beta), Springer-Verlag, p 829.

5. Спосіб формування послідовностей псевдовипадкових чисел Пат. UA 38402 U, МКІ (2006) G09C 1/00 / Кузнецов О.О. Євсеєв С.П., Рябуха Ю.Н., Корольов Р.В., Пудов В.А. – № и 200810861; заявл. 03.09.2008; опубл. 12.01.2009, Бюл. №1, 2009р. – 4 с.

Надійшла до редколегії 22.10.2009

Рецензент: д-р техн. наук, проф. О.О. Кузнецов, Харківський університет Повітряних Сил ім. І. Кожедуба, Харків.

МЕТОД ФОРМИРОВАНИЯ ПСЕВДОСЛУЧАЙНЫХ ПОСЛЕДОВАТЕЛЬНОСТЕЙ МАКСИМАЛЬНОГО ПЕРИОДА С ИСПОЛЬЗОВАНИЕМ МОДУЛЯРНЫХ ПРЕОБРАЗОВАНИЙ

Ю.М. Рябуха

Исследуются методы формирования последовательностей псевдослучайных чисел, стойкость которых базируется на сводке задачи возобновления тайного ключа к решению хорошо известной и чрезвычайно сложной математической задачи. Предлагается усовершенствованный метод формирования псевдослучайных последовательностей с использованием модулярных преобразований, стойкость которого базируется на решении хорошо известной проблемы RSA, но который, в отличие от известных, позволяет формировать последовательности максимального периода.

Ключевые слова: *псевдослучайные последовательности, модулярные преобразования, стойкость преобразования.*

METHOD OF FORMING OF PSEUDOCASUAL SEQUENCES OF MAXIMAL PERIOD WITH THE USE OF MODULYARNIKH OF TRANSFORMATIONS

Yu.M. Ryabukha

The methods of forming of sequences of pseudocasual numbers firmness of which is based on the report of task of proceeding in the secret key to the decision well known and extraordinarily intricate mathematical problem are probed. The improved method of forming of pseudocasual sequences is offered with the use of modular transformations, firmness of which is based on a decision well of the known problem of RSA, but which, unlike known, allows to form the sequences of maximal period.

Keywords: *pseudocasual sequences, modular transformations, stability of transformations.*