Ю. Яремчук. Особливості розроблення програмних засобів реалізації прото-колів асиметричного шифрування інформації на основі рекурентних послідовностей / Ю. Яремчук // Вісник ТНТУ. — 2013. — Том 69. — № 1. — С.174-182. — (приладобудування та інформаційно-вимірювальні технології).

УДК 621.391.7

Ю. Яремчук, канд. техн. наук

Вінницький національний технічний університет

ОСОБЛИВОСТІ РОЗРОБЛЕННЯ ПРОГРАМНИХ ЗАСОБІВ РЕАЛІЗАЦІЇ ПРОТОКОЛІВ АСИМЕТРИЧНОГО ШИФРУВАННЯ ІНФОРМАЦІЇ НА ОСНОВІ РЕКУРЕНТНИХ ПОСЛІДОВНОСТЕЙ

Резюме. *Розглянуто математичний апарат рекурентних послідовностей, а також можливість побудови методу асиметричного шифрування інформації на його основі. Для запропонованого методу розроблено структуру програми асиметричного шифрування, яка дозволяє реалізувати запропонований метод у вигляді набору модулів, що виконують певні обчислювальні процедури. Наведено структури програм шифрування (дешифрування) головного модуля. З метою спрощення обчислень криптографічних перетворень розглянуто особливості програмної реалізації запропонованого методу та наведено рекомендації щодо вибору параметрів.*

Ключові слова: *інформація, захист інформації, криптографія, шифрування, рекурентні послідовності, програмні засоби.*

I. Iaremchuk

PERCULIARITIES OF SOFTWARE MEANS DEVELOPMENT OF ASYMMETRIC ENCRYPTION PROTOCOLES IMPLEMENTATION BASED ON RECURRENT SEQUENCES

Summary. *The paper considers a topical problem of developing software means of fast asymmetric encryption-decryption of information based on recurrent sequences that would ensure an adequate level of reliability. We considered the mathematical apparatus of recurrent* V_k^+ *and* U_k *sequences, as well as a possibility of constructing a method of asymmetric information encryption based on it. The method considered is, under certain conditions, of less computational complexity in comparison with the known method of ElGamal, and it provides the same level of reliability. Moreover, the proposed method allows setting a required reliability depending on the parameter* k*, i.e. it is possible to increase the reliability along with the increase of this parameter. A peculiarity of the hardware implementation of the presented method of asymmetric encryption is that all the procedures therein are performed consistently, because the processors for encryption (decryption) contain one unit for calculating* V_k^+ *and* U_k *sequences. To simplify the organization of memory, we implemented as separate memory blocks for storage of various data. A comparison of processors that implement the proposed method, and the known ElGamal method, shows that the former offer almost the same time of encryption-decryption at* $k = 2$*, and longer time at* $k > 2$*. For the proposed method, we developed a software structure of asymmetric encryption, which allows implementing the proposed method as a set of modules that perform specific computational procedures. The most difficult of all the modules is a module performing arithmetic operations with large numbers. We provided structures of software encryption (decryption) of the main module. In order to simplify calculations of cryptographic transformations, we considered peculiarities of software implementation of the proposed method and provided recommendations for parameter selection.*

Key words: *information, information security, cryptography, encryption, recurrent sequences, software means.*

Постановка проблеми. Криптографічні методи [1, 2] застосовуються в системах захисту і додатках різного призначення. При цьому залишається актуальним питання спрощення обчислень криптографічних методів, особливо асиметричних, де використовуються великі ключі та числа великої розрядності. Виходячи з цього, актуальною є побудова асиметричних методів шифрування на основі таких математичних апаратів, які б могли забезпечувати спрощення обчислень.

Аналіз останніх досліджень і публікацій. З точки зору вирішення вказаної проблеми певний інтерес викликає апарат на основі рекурентних послідовностей [3], який дозволяє за певних умов спрощувати обчислення асиметричних методів, що базуються на його основі. З метою спрощення обчислень у роботі [4] запропоновано використовувати рекурентні послідовності Люка за модулем простого числа замість традиційного піднесення до степеня. Однак у роботі [5] було вказано на певну слабкість такого підходу щодо криптографічної стійкості.

В роботі [6] показано можливість використання рекурентних V_k^+ та U_k-послідовностей для побудови криптографічних методів, що базуються на технології відкритого ключа. Запропонований підхід дозволяє за певних умов спрощувати обчислення криптографічних перетворень.

Програмна чи апаратна реалізація криптографічних методів на основі технології відкритого ключа має ряд особливостей. Одна з них – необхідність виконувати обчислення над числами великої розрядності (1024 – 4096 двійкових розрядів). З урахуванням цих особливостей в роботі [7] розроблено принципи побудови спеціалізованих процесорів асиметричного шифрування (дешифрування) інформації на основі рекурентних V_k^+ та U_k-послідовностей.

Однак апаратна реалізація не в усіх випадках є прийнятною і можливою. Тому розглядається можливість розроблення програмних засобів асиметричного шифрування та дешифрування інформації на основі рекурентних послідовностей з урахуванням усіх особливостей та можливості прискорювати процеси криптографічних перетворень.

Мета роботи – розроблення програмних засобів швидкісного 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 програмні засоби їх реалізації, які б враховували усі особливості та можливості спрощення обчислень.

Асиметричне шифрування інформації на основі рекурентних послідовностей. Рекурентні послідовності в загальному вигляді породжуються співвідношенням [3]

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

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

Назвемо послідовність чисел, які обчислюють за формулою

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

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 й зворотна процедура, коли елементи послідовності обчислюють для спадних n, починаючи з деякого значення $n=l$. Обчислення елементів такої послідовності буде здійснюватись таким чином:

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

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

$$v_{n+m,k}=v_{m+(k-2),k}\cdot v_{n,k}+g_1\cdot\sum_{i=1}^{k-1}v_{m+(k-2)-i,k}\cdot v_{n-k+i,k}\,. \tag{3}$$

Назвемо послідовність чисел, яку обчислюють за формулою

$$u_{n,k}=g_k u_{n-1,k}+g_1 u_{n-k,k} \tag{4}$$

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 – U_k-послідовністю.

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

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

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

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

Ідея методу асиметричного шифрування інформації полягає в побудові односторонньої функції на основі властивості (5), 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 (5) 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 й 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 (5) й 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.

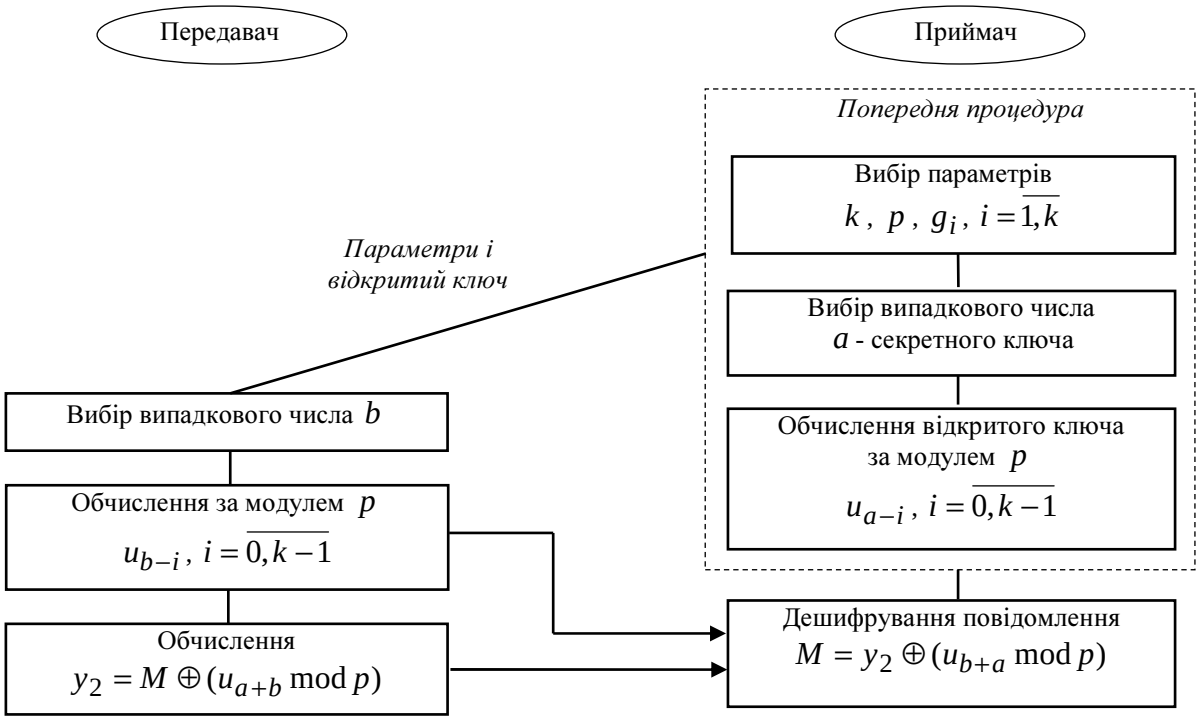

Рисунок 1. Процедура шифрування з відкритим ключем на основі елементів U_k -послідовностей

Figure 1. Procedure of public key encryption based on U_k sequences

Обчислення елементів u_{a-i} та u_{b-i} для $i=\overline{0,k-1}$ здійснюється за формулою (6) на основі елементів $v_{a+i,k}$ та $v_{b+i,k}$ для $i=\overline{-(k-1),k-2}$. Обчислення останніх може здійснюватися за алгоритмом прискореного обчислення елементів V_k^+-послідовності [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 у порівнянні 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.

Розроблення пакету програм асиметричного шифрування інформації. Розглянемо особливості розроблення пакета програм, що реалізують процедури шифрування та дешифрування інформації згідно з представленим методом асиметричного шифрування інформації.

Розроблення пакета програм пропонується розпочати з визначення його складових програмних модулів. Для цього пропонується виділити такі програмні модулі:

- головний модуль реалізації методу асиметричного шифрування інформації на основі V_k^+ - та U_k - послідовностей;
- модуль задавання та вибору параметрів;
- модуль генерування випадкових чисел, у т.ч. простих, у заданому діапазоні;
- модуль обчислення елементів V_k^+ - та U_k - послідовностей;
- модуль виконання арифметичних операцій з великими числами.

На рис. 1 представлена узагальнена структура програмної реалізації протоколу шифрування інформації з відображенням зв'язків між її компонентами.

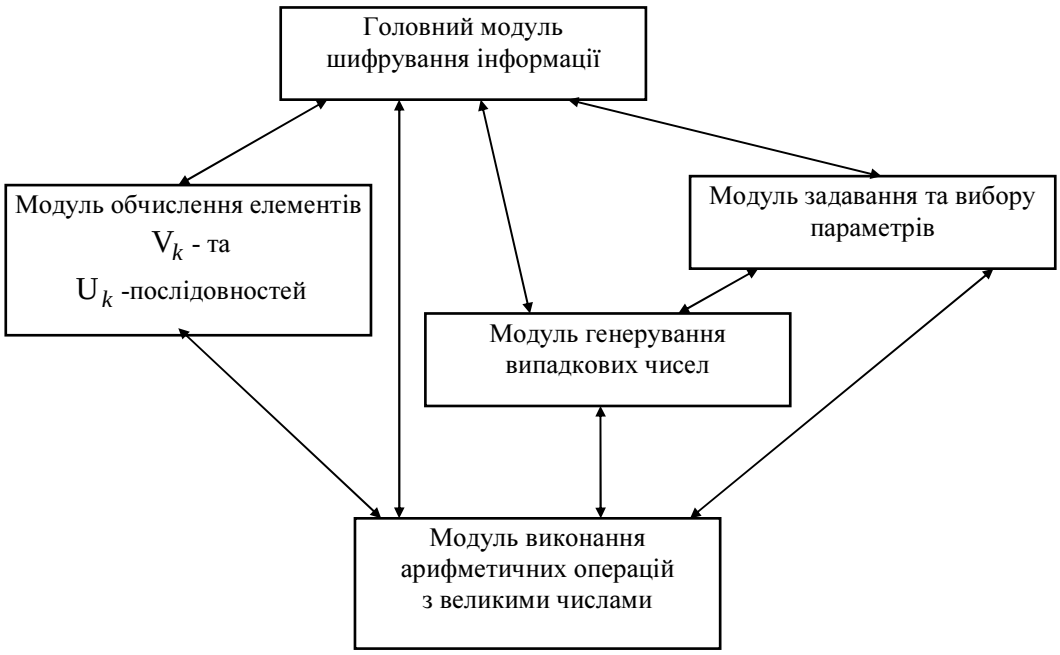

Рисунок 2. Узагальнена структура програмної реалізації методу шифрування інформації на основі елементів U_k -послідовностей

Figure 2. Generalized structure of software implementation of encryption based on U_k -sequences

Розглянемо реалізацію кожного програмного модуля.

Головний модуль містить програмні процедури реалізації дій, що виконують окремо передавач та приймач за представленим методом асиметричного шифрування.

Алгоритми реалізації цих процедур представлені на рис. 3, 4.

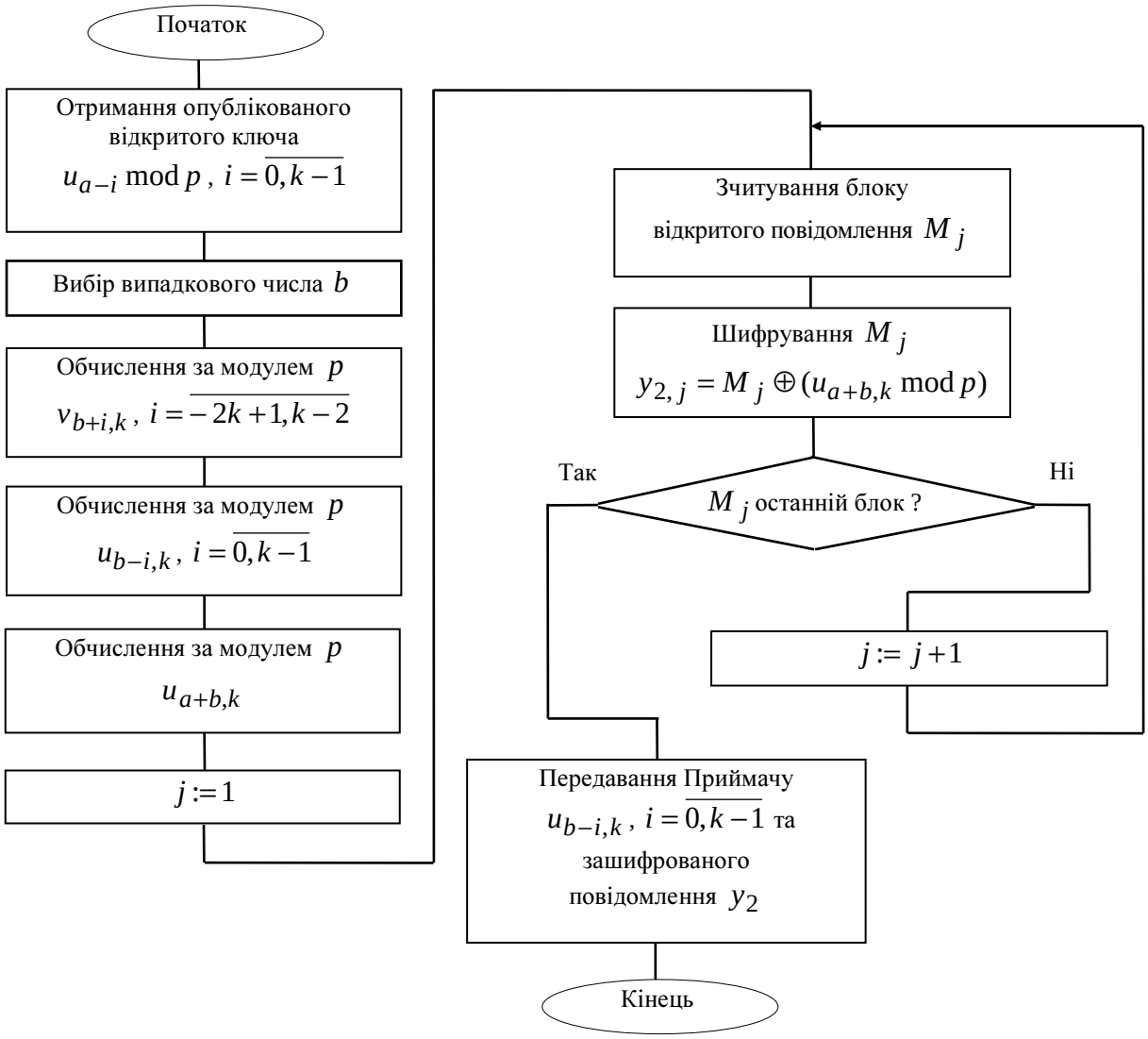

Рисунок 3. Структура програми шифрування на основі елементів U_k -послідовностей з боку передавача

Figure 3. Structure of software encryption based on U_k sequences of the transmitter

Шифрування інформації в наведених алгоритмах проводиться не для всього відкритого повідомлення M, а для окремих його частин M_j. Розмір однієї частини визначається параметром p. Тобто зашифроване повідомлення y_2 в алгоритмі шифрування складається з окремих частин.

Вибір параметру p здійснюється в програмному модулі задавання та вибору параметрів, де окрім нього задається параметр k та вибираються коефіцієнти рекурентного співвідношення g_i, $i = \overline{1,k}$.

При задаванні параметру k слід враховувати, що від цього параметру в прямій залежності знаходиться криптостійкість представленого методу асиметричного шифрування, а також складність виконання, а, отже, і час виконання програм шифрування/дешифрування інформації.

Рекомендується вибирати параметр k, що дорівнює 2 або 3.

Параметр p вибирається як випадкове число, розрядність якого кратна розрядності машинної одиниці інформації й залежить від можливостей комп'ютера, на якому реалізується програма шифрування інформації. Для сучасних комп'ютерів цю розрядність слід вибирати 1024, 2048 або 4096.

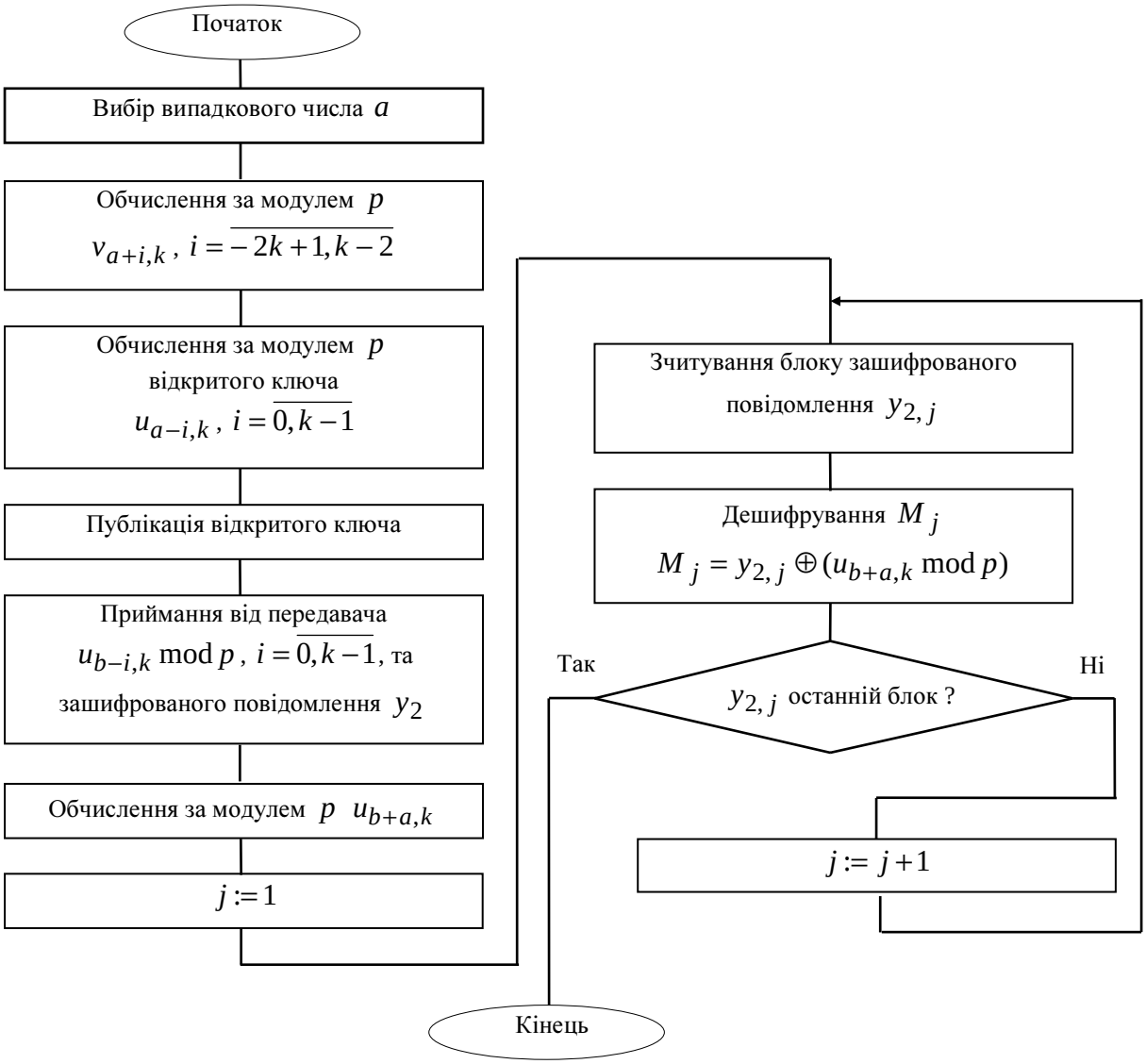

Рисунок 4. Структура програми шифрування на основі елементів U_k -послідовностей з боку приймача

Figure 4. Structure of software encryption based on U_k sequences of the receiver

В алгоритмах шифрування інформації усі арифметичні операції виконуються з великими числами. Необхідність виділення окремого програмного модуля для виконання операцій з великими числами пов'язана із певними обмеженнями реалізації таких операцій у відомих мовах програмування, які не завжди є прийнятними для реалізації криптографічних методів.

З метою прискорення криптографічних перетворень даний програмний модуль розроблено на низькому рівні програмної реалізації. Зокрема, реалізовані такі операції над числами великої розрядності, як цілочисельне додавання, віднімання та операції за

модулем додавання, віднімання, обчислення мультиплікативно оберненої величини, лишку Монтгомері, множення за Монтгомері та обчислення величин, що необхідні для виконання прискореної операції піднесення до степеня за Монтгомері.

Зазначимо, що обчислення мультиплікативно оберненої величини за модулем виконується за умови $(p,b)=1$, а при обчисленні $g_1^{-1} \bmod p$ потрібно виконання умови $(g_1, p)=1$. Щоб задовольнити вказані умови, параметр p вибирається як просте число.

Коефіцієнти g_i, $i=\overline{1,k}$, вибираються як випадкові числа.

Оскільки параметр p є модулем при обчисленнях та визначає верхню границю усіх чисел, що використовуються в алгоритмах шифрування, вибір параметрів g_i, $i=\overline{1,k}$, здійснюється в діапазоні $[1, p]$.

Таким чином, для вибору параметрів алгоритмів шифрування/дешифрування потрібні генератори звичайних випадкових та простих випадкових чисел.

Тут зазначимо, що генератор випадкових чисел потрібен і для вибору секретних ключів a та b в алгоритмах шифрування/дешифрування інформації.

Програмна реалізація генераторів випадкових чисел здійснюється в модулі генерування випадкових чисел.

Для генерування параметрів g_i, $i=\overline{1,k}$ може використовуватись один з відомих генераторів випадкових чисел [1, 2], наприклад, лінійний конгруентний генератор.

Для вибору секретних ключів рекомендується використовувати більш випадкові генератори. Наприклад, генератор, заснований на затримках між натисненнями клавіш клавіатури.

Для генерування простих випадкових чисел пропонується використовувати відомі тести на простоту [1], зокрема тест Міллера-Рабіна.

Розглянемо реалізацію модуля обчислення елементів V_k^+ та U_k-послідовностей.

Аналіз алгоритмів, представлених на рис. 3, 4, показує, що в цих алгоритмах використовуються однакові блоки обчислення елементів V_k^+- та U_k-послідовностей тільки для різних значень індексу. Тому окремо слід виділити такі процедури:

- обчислення за модулем p $v_{n+i,k}$, $i=\overline{-2k+1,k-2}$ для додатних n;
- обчислення за модулем p $u_{n-i,k}$, $i=\overline{0,k-1}$;
- обчислення за модулем p $u_{n+m-i,k}$, $i=\overline{0,k-1}$.

При реалізації процедури обчислення елемента $v_{n,k}$ за модулем p для додатних значень n пропонується виділити окремо такі процедури:

- прискорене обчислення елемента $v_{n,k}$ для додатних n, наприклад, за алгоритмом, який наведено в роботі [6];
- пряме обчислення елемента $v_{n,k}$ за формулою (1);
- зворотне обчислення елемента $v_{n,k}$ за формулою (2).

Таким чином визначена структура програми шифрування інформації, а також визначено, як розробляти усі програмні модулі цієї структури.

Здійснено повну реалізацію на низькому рівні програмних модулів виконання арифметичних операцій з великими числами, вибору параметрів, обчислення елементів V_k^+ - та U_k -послідовностей, а також головного модуля реалізації представленого методу асиметричного шифрування інформації. Розмір машинного коду розробленого пакета програм складає приблизно 30 Кбайт.

Висновки. Розглянуто рекурентні V_k^+ - та U_k -послідовності та отримано для них аналітичні залежності, які дозволили створити математичний апарат для побудови методу асиметричного шифрування інформації на його основі.

З метою прискорення обчислень розроблено узагальнену структуру програми шифрування інформації на основі елементів U_k -послідовностей, яка дозволяє реалізувати запропонований метод у вигляді набору модулів, що виконують певні обчислювальні процедури. Найскладнішим з усіх модулів є модуль виконання арифметичних операцій з великими числами. Запропонована програмна реалізація повного набору арифметичних операцій за модулем.

Окремо розроблено структуру головного модуля – програм асиметричного шифрування/дешифрування згідно з запропонованим методом. Також наведено особливості програмної реалізації методу та рекомендації щодо вибору параметрів з метою спрощення обчислень криптографічних перетворень.

Conclusions. We considered recurrent V_k^+ and U_k -sequences, and received their analytical dependences, which helped create mathematical tools for construction of a method of asymmetric information encryption based on it.

In order to accelerate computing a generalized structure of encryption software based on U_k -sequences, which allows implementing the proposed method as a set of modules that perform specific computational procedures, was developed. The most difficult of all the modules is a module performing arithmetic operations with large numbers. Software implementation of a complete set of arithmetic operations within the module was proposed.

Besides, a structure of the main module – the software of asymmetric encryption/decryption, as per the proposed method was developed. In addition, peculiarities of the software implementation of the method and recommendations as to the choice of parameters in order to simplify calculations of cryptographic transformations, were provided.

Список використаної літератури

1. Menezes, A.J. Handbook of Applied Cryptography / A.J. Menezes, P.C. van Oorschot, S.A. Vanstone. – CRC Press, 2001. – 816 p.
2. Шнайер, Б. Прикладная криптография. Протоколы, алгоритмы, исходные тексты на языке Си [Текст] / Б. Шнайер. – М.: Триумф, 2002. – 816 с.
3. Маркушевич, А.И. Возвратные последовательности [Текст] / А.И. Маркушевич. – М.: Наука, 1975. – 48 с.
4. Smith, P. A public-key cryptosystem and a digital signature system based on the Lucas function analogue to discrete logarithms / Smith P., C. Skinner // In Advances in Cryptology Asiacrypt ’94, Springer-Verlag. – 1995. – P. 357 – 364.
5. Bleichenbacher, D. Some remarks on Lucas-based cryptosystems / D. Bleichenbacher, W. Bosma, A. Lenstra // In Advances in Cryptology Crypto ’95, Springer-Verlag. – 1995. – P.386 – 396.
6. Яремчук, Ю.Є. Використання рекурентних послідовностей для побудови криптографічних методів з відкритим ключем [Текст] / Ю.Є. Яремчук // Захист інформації. – 2012. – № 4. – С. 120 – 127.
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. – 2012. – Випуск 2 (24). – С. 63 – 69.
8.

Отримано 01.02.2013