УДК 621.391.7

Ю.Є. Яремчук
Вінницький національний технічний університет

РОЗРОБЛЕННЯ ПРОГРАМНИХ ЗАСОБІВ РЕАЛІЗАЦІЇ ПРОТОКОЛІВ РОЗПОДІЛУ КЛЮЧІВ ТА АВТЕНТИФІКАЦІЇ СТОРІН ВЗАЄМОДІЇ НА ОСНОВІ РЕКУРЕНТНИХ ПОСЛІДОВНОСТЕЙ

Розглянуто математичний апарат рекурентних послідовностей та можливість побудови методів розподілу ключів, а також автентифікації сторін взаємодії на його основі. Розроблено структури програм розподілу ключів та автентифікації сторін взаємодії, які дають змогу реалізувати запропоновані методи у вигляді набору модулів, що виконують певні обчислювальні процедури. Наведено структури програм головних модулів розподілу ключів та автентифікації сторін взаємодії. Розглянуто особливості програмної реалізації запропонованих методів та наведено рекомендації щодо вибору параметрів.

Ключові слова: захист інформації, криптографія, розподіл ключів, автентифікація сторін взаємодії, рекурентні послідовності, програмні засоби.

In this work, we considered a mathematical apparatus of recurrent sequences, as well as a possibility of constructing methods of key distribution and authentication aspects of interaction parties, based on it. We developed structures of key distribution programs and authentication of interaction parties, allowing for implementation of modules that perform specific computational procedures. We programs structure of the main modules programs of key distribution and authentication of interaction parties. We considered peculiarities of software implementation of the proposed methods and provides recommendations for selecting the required parametes

Key words: information security, cryptography, key distribution, authentication of interaction parties, recurrent sequences, software.

Вступ

У роботі [1] Діффі та Хеллман вперше розглянули можливість побудови криптографічних методів на основі технології відкритого ключа, яка полягала у використанні дискретного піднесення до степеня для обміну секретними ключами між користувачами мережі із застосуванням тільки відкритих повідомлень. Пізніше було запропоновано цілий ряд варіантів [2] цього методу, крім того, було запропоновано низку методів асиметричного шифрування, автентифікації та цифрового підписування [2], основаних на піднесенні до степеня. Найвідомішими серед методів автентифікації є методи Фейге–Фіата–Шаміра, Гіллоу–Куіскуотера та Шнорра [2].

Однак операція піднесення до степеня, на якій ґрунтуються вказані методи, потребує виконання досить складних обчислень, що впливає на швидкість роботи кожного з методів при його практичній реалізації. Тому актуальними залишаються пошук та розроблення таких математичних апаратів, які забезпечували б спрощення обчислень і могли б стати основою побудови ефективних методів різного криптографічного призначення.

Так, у роботі [3] представлено метод розподілу секретних ключів відкритим каналом, який базується на рекурентних V_k^+ та U_k –послідовностях. Порівняно з відомим методом розподілу ключів Діффі–Хеллмана, запропонований метод за певних умов дає змогу спрощувати обчислення і має простішу процедуру задання параметрів. Крім того, він є стійкішим, а також дозволяє встановлювати необхідну криптостійкість залежно від порядку послідовності k .

У роботі [4] наведено метод автентифікації сторін взаємодії, який ґрунтується на рекурентних V_k^+ та U_k –послідовностях і який, порівняно з відомими методами Фейге–Фіата–Шаміра, Гіллоу-Куіскуотера та Шнорра, має простішу процедуру задання параметрів та приблизно вдвічі меншу складність обчислень. Крім того, якщо у відомих методах, окрім передавання параметрів, безпосередньо під час автентифікації необхідно виконувати три етапи передавання інформації, то у представленому методі лише два.

V_k^+ –послідовністю [3] називається 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.

За формулою (1) можна отримувати значення для n, що зростають, починаючи з $n = 0$. Можлива і зворотна процедура, коли елементи послідовності обчислюються для спадних n, починаючи з деякого значення $n = l$. Обчислюють елементи послідовності так

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

Для будь-яких цілих додатних n, m та k одержимо таку аналітичну залежність [3]

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

U_k –послідовністю [3] називається послідовність чисел, що обчислюються 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.

Для будь-яких цілих додатних n, m та k отримано таку залежність [3]

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

Для будь-яких цілих додатних n та k, таких що $n \geq k$, отримано залежність [3], яка дає змогу обчислювати елементи U_k –послідовності тільки на основі елементів V_k^+ – послідовності

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

На основі цього математичного апарату в [3] представлено метод розподілу секретних ключів відкритим каналом, а в роботі [4] – метод автентифікації сторін взаємодії. Програмна чи апаратна реалізація криптографічних методів на основі технології відкритого ключа має певні особливості. Одна з них – необхідність виконувати обчислення над числами великої розрядності (1024 – 4096 двійкових розрядів).

Однак апаратна реалізація не в усіх випадках прийнятна і можлива, тому розглядається можливість розроблення програмних засобів розподілу секретних ключів, а також автентифікації сторін взаємодії на основі рекурентних V_k^+ та U_k –послідовностей з урахуванням усіх особливостей та можливості прискорювати процеси криптографічних перетворень.

Мета роботи – розроблення програмних засобів швидкісного розподілу секретних ключів, а також автентифікації сторін взаємодії на основі рекурентних послідовностей, які б забезпечували достатній рівень криптостійкості.

Постановка задач досліджень

Розглянути математичний апарат рекурентних V_k^+ та U_k –послідовностей з позиції побудови швидкісних методів розподілу секретних ключів, а також автентифікації сторін взаємодії та розробити програмні засоби їх реалізації, які б враховували усі особливості та можливості спрощення обчислень.

Розроблення пакета програм розподілу ключів та автентифікації сторін взаємодії

Ідея методу розподілу ключів ґрунтується на властивості (5), яка дає змогу обчислити елемент $u_{n+m,k}$, використовуючи елементи V_k^+ та U_k –послідовностей, причому зробити це 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 $u_{m-i,k}$, $i=\overline{0,k-1}$.

Тоді, якщо один користувач для будь-якого вибраного ним випадкового числа a обчислить $u_{a-i,k}$, $i=\overline{0,k-1}$, а другий користувач аналогічно обчислить $u_{b-i,k}$, $i=\overline{0,k-1}$, то, обмінявшись обчисленими значеннями, кожен з них зможе отримати $u_{a+b,k}$, продовжуючи обчислення на своєму боці за формулою (5), використовуючи відповідно свої числа a або b. В цьому випадку $u_{a+b,k}$ буде ключем розподілу, а числа a і b секретним ключем кожного користувача. Причому a і b – це частини секретного ключа кожного користувача, оскільки будь-який користувач не може попередньо отримати ключ розподілу без одержання відповідної інформації від іншого користувача.

На цій самій ідеї можна побудувати метод автентифікації сторін взаємодії. При цьому спочатку претендент, який повинен довести свою автентичність, виконує попередню процедуру обчислення ключів. Для цього він у випадковий спосіб вибирає секретний ключ a, після чого обчислює і передає перевіряльнику відкритий ключ $u_{a-i,k}$, $i=\overline{0,k-1}$. Коли перевіряльник бажає перевірити автентичність претендента, він вибирає випадкове число b, обчислює $u_{b-i,k}$, $i=\overline{0,k-1}$, і передає отриманий набір елементів претенденту. Претендент, прийнявши цей набір елементів, здійснює на їх основі обчислення $u_{b+a,k}$. Водночас перевіряльник обчислює $u_{a+b,k}$. Потім претендент передає отримане значення $u_{b+a,k}$ перевіряльнику, який звіряє його зі значенням $u_{a+b,k}$, ідентифікуючи тим самим претендента.

Проведено [3, 4] дослідження теоретичної криптостійкості та складності обчислень за розглянутими методами, а також порівняння їх відповідно з відомими методами Діффі–Хеллмана, а також Фейге–Фіата–Шаміра, Гіллоу–Куіскуотера та Шнорра. Показано, що розглянуті методи мають не менший рівень криптостійкості, ніж відомі методи, але при цьому за певних умов мають меншу складність обчислень порівняно з відомими.

Тепер розглянемо особливості розроблення пакета програм, що реалізують процедури розподілу секретних ключів, а також автентифікації сторін взаємодії згідно з представленими методами.

Розроблення пакета програм розпочнемо з визначення його складових програмних модулів. Для цього виділимо такі програмні модулі:

– головний модуль реалізації методу розподілу секретних ключів (або автентифікації сторін взаємодії) на основі V_k^+ – та U_k – послідовностей;

– модуль задання та вибору параметрів;

– модуль генерування випадкових чисел, зокрема простих, у заданому діапазоні;

– модуль обчислення елементів V_k^+ – та U_k – послідовностей;

– модуль виконання арифметичних операцій з великими числами.

На рис. 1 наведено узагальнену структуру програмної реалізації розподілу секретних ключів (або автентифікації сторін взаємодії) з відображенням зв’язків між її компонентами.

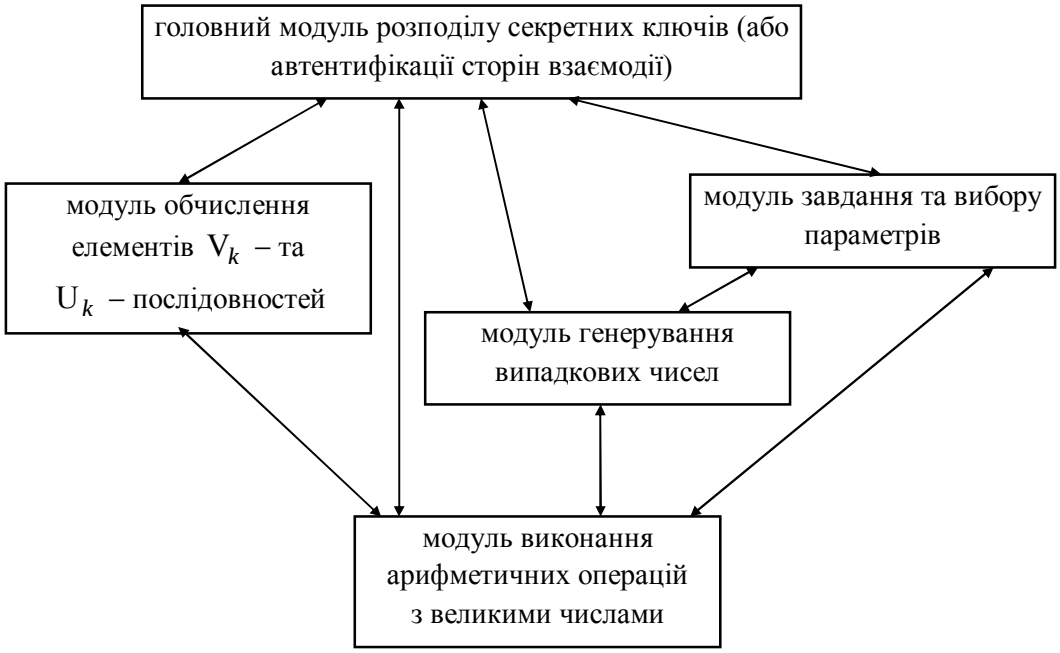

Рис. 1. Узагальнена структура програмної реалізації методу розподілу секретних ключів (або автентифікації сторін взаємодії) на основі елементів U_k *-послідовностей*

Розглянемо реалізацію кожного програмного модуля.

Головний модуль містить програмні процедури реалізації дій, що виконують окремо користувач A та користувач B за представленим методом розподілу ключів, а також претендент та перевіряльник за методом автентифікації сторін взаємодії.

Алгоритми реалізації цих процедур представлено відповідно на рис. 2 і 3.

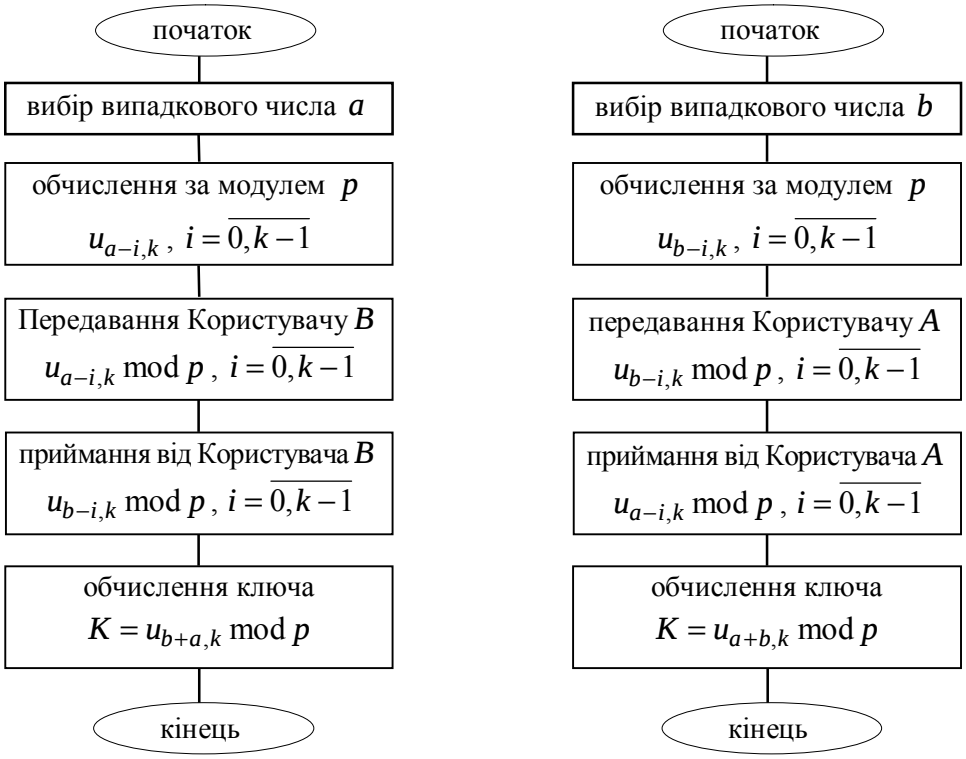

Рис. 2. Структура програми розподілу ключів на основі елементів U_k *-послідовностей з боку користувача* A *(а) та користувача* B *(б)*

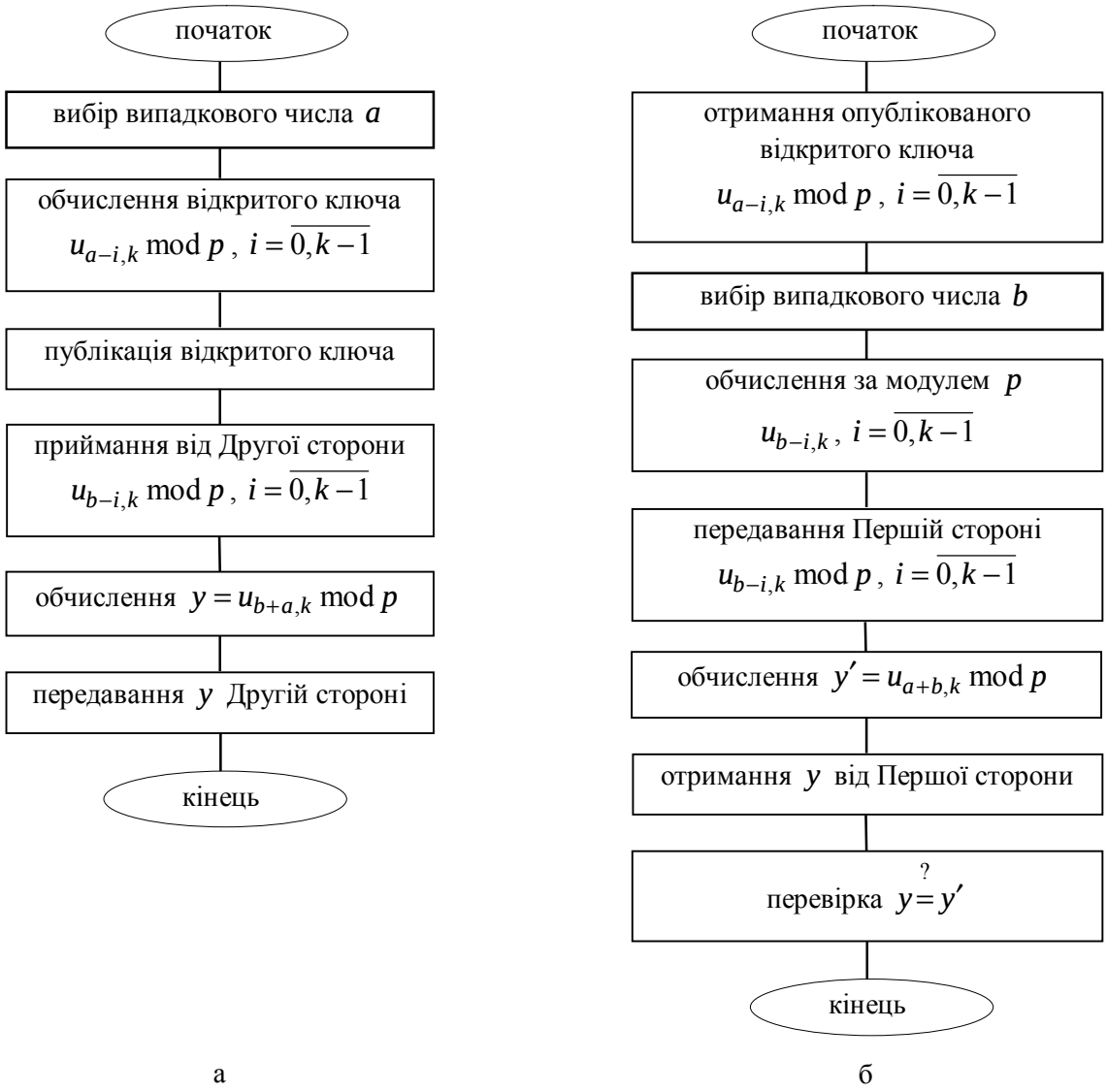

Рис. 3. Структура програми автентифікації сторін взаємодії на основі елементів U_k *-послідовностей з боку претендента (а) та перевіряльника (б)*

Операція за модулем p у програмах використовується для обмеження розрядності чисел під час виконання арифметичних операцій.

Вибір параметра p здійснюється у програмному модулі задання та вибору параметрів, де, окрім нього, задають параметр k та вибирають коефіцієнти рекурентного співвідношення g_i, $i = \overline{1,k}$.

Задаючи параметр k, слід враховувати, що від нього прямо залежить криптостійкість представлених методів розподілу секретних ключів та автентифікації сторін взаємодії, а також складність виконання, а отже, і час виконання програм реалізації цих методів.

Рекомендується вибирати параметр k, що дорівнює 2 або 3.

Параметр p вибирають як випадкове число, розрядність якого кратна розрядності машинної одиниці інформації і залежить від можливостей комп'ютера, на якому реалізується програма розподілу секретних ключів чи автентифікації сторін взаємодії. Для сучасних комп'ютерів цю розрядність необхідно вибирати 1024, 2048 або 4096.

В алгоритмах розподілу секретних ключів та автентифікації сторін взаємодії 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 прийнятні для реалізації криптографічних методів.

З метою прискорення криптографічних перетворень цей програмний модуль розроблено на низькому рівні програмної реалізації. Зокрема, реалізовані такі операції над числами великої розрядності, як цілочислове 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, щоб виконувалась умова $(g_1, p)=1$. Щоб задовольнити ці умови, параметр p вибирають як просте число.

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

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

Отже, для вибору параметрів алгоритмів розподілу секретних ключів та автентифікації сторін взаємодії потрібні генератори звичайних випадкових та простих випадкових чисел.

Тут зазначимо, що генератор випадкових чисел потрібен і для вибору чисел a і b, що використовуються в алгоритмах розподілу секретних ключів та автентифікації сторін взаємодії.

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 [2], наприклад, лінійний конгруентний генератор.

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

Для генерування простих випадкових чисел пропонується використовувати відомі тести на простоту [2], зокрема тест Міллера-Рабіна.

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

Аналіз алгоритмів, наведених на рис. 2 і 3, показує, що в них використовуються однакові блоки обчислення елементів V_k^+ та U_k-послідовностей тільки для різних значень індексу. Тому окремо виділимо 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 $u_{n+m-i,k}$, $i=\overline{0, k-1}$.

В 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 [3];

– пряме обчислення елемента $v_{n,k}$ за формулою (1);

– зворотне обчислення елемента $v_{n,k}$ за формулою (2).

Отже, визначено структуру програми розподілу секретних ключів (автентифікації сторін взаємодії), а також визначено, як проводити розроблення усіх програмних модулів 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 головних модулів реалізації наведених методів розподілу секретних ключів та автентифікації сторін взаємодії. Розмір машинного коду розробленого пакета програм – приблизно 30 Кбайт.

Висновки

На основі математичного апарату рекурентних V_k^+ та U_k -послідовностей та їх аналітичних залежностей розглянуто можливість побудови методів розподілу секретних ключів, а також автентифікації сторін взаємодії.

З метою прискорення обчислень розроблено узагальнену структуру програми розподілу секретних ключів (автентифікації сторін взаємодії) на основі елементів U_k -послідовностей, яка дає змогу реалізувати розглянуті методи у вигляді набору модулів, що виконують певні обчислювальні процедури. Найскладнішим з усіх модулів є модуль виконання арифметичних операцій з великими числами. Запропоновано програмну реалізацію повного набору арифметичних операцій за модулем.

Окремо розроблено структуру головних модулів - програм розподілу секретних ключів та автентифікації сторін взаємодії за розглянутими методами. Також наведено особливості програмної реалізації методів та рекомендації щодо вибору параметрів з метою спрощення обчислень криптографічних перетворень в них.

1. Diffie W., Hellman, M.E. New directions in cryptography [Текст] / W. Diffie, M.E. Hellman // IEEE Transactions on Information Theory. – 1976. – № 22. – P. 644–654. 2. Menezes A.J. Handbook of Applied Cryptography [Текст] / A.J. Menezes, P.C. van Oorschot, S.A. Vanstone. – CRC Press, 2001. – 816 p. 3. Яремчук Ю.Є. Використання рекурентних послідовностей для побудови криптографічних методів з відкритим ключем [Текст] / Ю.Є. Яремчук // Захист інформації. – 2012. – № 4. – С. 120 – 127. 4. Яремчук Ю. Є. Метод автентифікації сторін взаємодії на основі рекурентних послідовностей [Текст] / Ю.Є. Яремчук // Сучасний захист інформації. – 2013. – № 1. – С. 4–10.