DOI: 10.18372/2410-7840.21.13764
УДК 004.056.55

МЕТОДОЛОГІЯ ОПРАЦЮВАННЯ БАГАТОРОЗРЯДНИХ ЧИСЕЛ В АСИМЕТРИЧНИХ КРИПТОСИСТЕМАХ

Михайло Касянчук, Микола Карпінський, Світлана Казмірчук

На сьогоднішній день збільшення довжини ключа неминуче приводить до зростання об'ємів обчислень для захисту інформаційних потоків при використанні асиметричних криптосистем, найбільш поширеними операціями в яких є модулярне множення та модулярне експоненціювання. Існуючі методи та алгоритми виконання вказаних операцій базуються на позиційних системах числення, які характеризуються значною часовою складністю в зв'язку з обмеженими можливостями розпаралелення процесу обчислень, що приводить до зменшення їх швидкодії. Використання нових підходів, зокрема, векторно-модульного методу модулярного множення та експоненціювання, а також системи залишкових класів, дозволить розширити функціональні можливості обчислювальних систем для шифрування/розшифровування інформації. З цією метою пропонується методологія, орієнтована на збільшення швидкодії асиметричних криптосистем, базовий механізм якої ґрунтується на восьми етапах: формування множини блоків відкритого тексту, формування вимог до параметрів криптосистем та захищеності інформації, вибір асиметричної криптосистеми, формування множини базових операцій, вибір методу виконання операцій, вибір форми системи залишкових класів, вибір методів побудови досконалої та модифікованої досконалої форм системи залишкових класів, реалізація основних асиметричних криптосистем на основі вказаних підходів. Така методологія дозволяє зменшити часову складність, підвищити швидкодію алгоритмів, спеціалізованого програмного і апаратного забезпечення при опрацюванні багаторозрядних чисел в асиметричних криптосистемах.

Ключові слова: *асиметричні криптосистеми, багаторозрядні числа, модулярне множення, модулярне експоненціювання, векторно-модульний метод, система залишкових класів, методологія опрацювання багаторозрядних чисел.*

Актуальність

На даний час асиметричні криптосистеми або криптосистеми з відкритим ключем, в яких для шифрування і розшифровування використовуються різні ключі, відіграють надзвичайно важливу роль під час захисту інформаційних потоків від несанкціонованого доступу [10]. Вони усувають основний недолік симетричних криптосистем: необхідність надійного каналу обміну ключем.

Базовими арифметичними операціями в найпоширеніших асиметричних криптосистемах RSA, Рабіна, Ель-Гамаля є модулярне множення та модулярне експоненціювання [9]. Однак в зв'язку із збільшенням довжини ключа (на даний час для досягнення прийнятного рівня захищеності необхідна довжина чисел становить 2048 розрядів з перспективою її зростання) все більше стали проявлятися недоліки двійкової системи числення, яка використовується в сучасних обчислювальних системах: наприклад, її багаторозрядність, строго послідовна структура, наявність міжрозрядних переносів тощо, які в значній мірі сповільнюють виконання арифметичних операцій [4].

Тому використання відповідних методів, моделей та методологій для опрацювання багаторозрядних чисел в обчислювальних системах є основою для зменшення часової складності, підвищення швидкодії програмного та апаратного забезпечення сучасних асиметричних криптосистем. Виходячи із сказаного, актуальною науковою задачею є створення методології опрацювання багаторозрядних чисел (МОБРЧ) та виконання над ними арифметичних операцій модулярного множення і модулярного експоненціювання, які використовуються в сучасних асиметричних криптосистемах.

Аналіз існуючих досліджень

Найперспективнішим шляхом підвищення швидкодії сучасних обчислювальних систем є розпаралелення процесу обробки інформації [6]. Цією властивістю володіє система залишкових класів (СЗК), яка є однією з альтернатив двійковому представленню чисел. Вона дозволяє істотно поліпшити параметри компонентів обчислювальних систем у порівнянні з пристроями, побудованими на тій же фізико-технологічній базі і які працюють у позиційних системах числення [5]. Хоча СЗК не позбавлена недоліків (труднощі при виконанні операцій ділення, порівняння, визначення переповнення розрядної сітки), однак її успішно можна застосовувати для модулярних операцій додавання, віднімання, піднесення до степеня, множення цілих багаторозрядних чисел, що є важливо для асиметричної криптографії. Безсумнівна перевага СЗК - це можливість виконання операцій над числами, які менші за вибрані модулі, та розпаралелення процесу обчислень. Крім того, використання досконалої (ДФ) [1] та модифікованої досконалої форм (МДФ) [7] СЗК дозволяє істотно спростити переведення чисел у позиційну систему числення.

Іншим напрямком підвищення швидкодії програмної та апаратної реалізацій виконання операцій модулярної арифметики при їх застосуванні в протоколах захисту інформації є використання матричних та векторних методів модулярного множення та експоненціювання [8]. Наприклад, в [3] наведено часові складності найбільш поширених методів модулярного множення в залежності від розрядності операндів n_0 (табл. 1).

Таблиця 1

Часова складність алгоритмів модулярного множення

Назва алгоритму	Часова складність
Стандартний	n_0^2
Шенхаге-Штрасена	$n_0 \cdot \log_2 n_0 \log_2(\log_2 n_0)$
Карацуби	$n_0^{\log_2 3} = n_0^{1,585}$
Монтгомері	$n_0 \cdot \log_2 n_0$
Матрично-модульний	$n_0 \cdot \log_2 n_0$
Векторно-модульний	$(n_0 \cdot \log_2 n_0)/2$

Порівняно невисока часова складність матрично- та векторно-модульних методів поєднується із простотою програмної та апаратної реалізації. Тому їх можна покласти в основу відповідної методології, яка дозволить побудувати обчислювальні системи для виконання базових арифметичних операцій модулярного множення та модулярного експоненціювання над багаторозрядними числами в сучасних асиметричних криптоалгоритмах.

Основна мета дослідження

Виходячи з аналізу існуючих досліджень та актуальності поставленої задачі, метою даної роботи є розробка МОБРЧ для зменшення обчислювальної складності, підвищення швидкодії алгоритмів, спеціалізованого програмного і апаратного забезпечення в асиметричних криптосистемах на основі модулярної арифметики та системи залишкових класів. На основі такої методології можна ефективно будувати обчислювальні системи для виконання базових операцій модулярного множення та модулярного експоненціювання, які найбільш поширені в сучасних асиметричних криптосистемах.

Основна частина дослідження

Для досягнення поставленої мети пропонується МОБРЧ (рис. 1), базовий механізм якої ґрунтується на восьми етапах: формування множини блоків відкритого тексту, формування вимог до параметрів криптосистем та захищеності інформації, вибір асиметричної криптосистеми, формування множини базових операцій, вибір методу виконання операцій, вибір форми СЗК, вибір методів побудови ДФ та МДФ СЗК, реалізація основних асиметричних криптосистем.

На першому етапі користувачу необхідно сформувати множину блоків відкритого тексту $BT = \left\{ \bigcup_{i=1}^{z_1} BT_i \right\} = \left\{ BT_1, BT_2, ..., BT_{z_1} \right\}$, ($z_1$ – кількість блоків відкритого тексту). Їх числові значення в основних асиметричних криптосистемах RSA, Рабіна, Ель-Гамаля мають бути меншими від відповідного параметру відкритого ключа [2], діленням на який числового значення відкритого тексту визначається величина z_1. Крім того, визначаються можливі загрози, які виникають при передачі даних у вигляді блоків зашифрованого тексту каналами зв'язку. В результаті формується визначена користувачем множина загроз $MЗ = \left\{ \bigcup_{i=1}^{z_2} MЗ_i \right\} = \left\{ MЗ_1, MЗ_2, ..., MЗ_{z_2} \right\}$, де z_2 – їх кількість.

На другому етапі на основі сформованих множин загроз та блоків відкритого тексту відбувається формування вимог до кількісних показників захищеності інформації $ЗІ = \left\{ \bigcup_{i=1}^{z_2} \bigcup_{j=1}^{z_3} ЗІ_{ij} \right\}$, які записуються у вигляді матриці, та параметрів криптосистем $ВП = \left\{ \bigcup_{i=1}^{z_4} ВП_i \right\} = \left\{ ВП_1, ВП_2, ..., ВП_{z_4} \right\}$. Для кожного блоку відкритого тексту $BT_i, i \in [1, z_1]$ та кожної можливої загрози $MЗ_i, i \in [1, z_2]$ ставиться у відповідність множина показників захищеності $ЗІ_i = \left\{ \bigcup_{j=1}^{z_3} ЗІ_{ij} \right\} = \left\{ ЗІ_{i1}, ЗІ_{i2}, ..., ЗІ_{iz_3} \right\}$, де z_3 – кількість можливих показників для i-ої загрози, та множина вимог до параметрів криптосистеми $ВП_i, i \in [1, z_4]$, де z_4 – кількість вимог.

Третій етап призначений для вибору асиметричної криптосистеми, найбільш поширеними з яких є RSA, Рабіна та Ель-Гамаля, згідно визначених у попередньому етапі вимог до їх параметрів. Аналіз криптосистем показує, що для генерації ключів, шифрування та розшифровування у них використовуються такі операції: пошук залишку, квадратного кореня за модулем, найбільшого спільного дільника (НСД), оберненого елемента, використання розширеного алгоритму Евкліда, відновлення десяткового числа за його залишками (китайська теорема про залишки), модулярне множення та модулярне експоненціювання, з яких на четвертому етапі формується відповідна множина $ОП = \left\{ \bigcup_{i=1}^{z_5} ОП_i \right\} = \left\{ ОП_1, ОП_2, ..., ОП_{z_5} \right\}$, $i \in [1, z_5]$, де z_5 – кількість операцій.

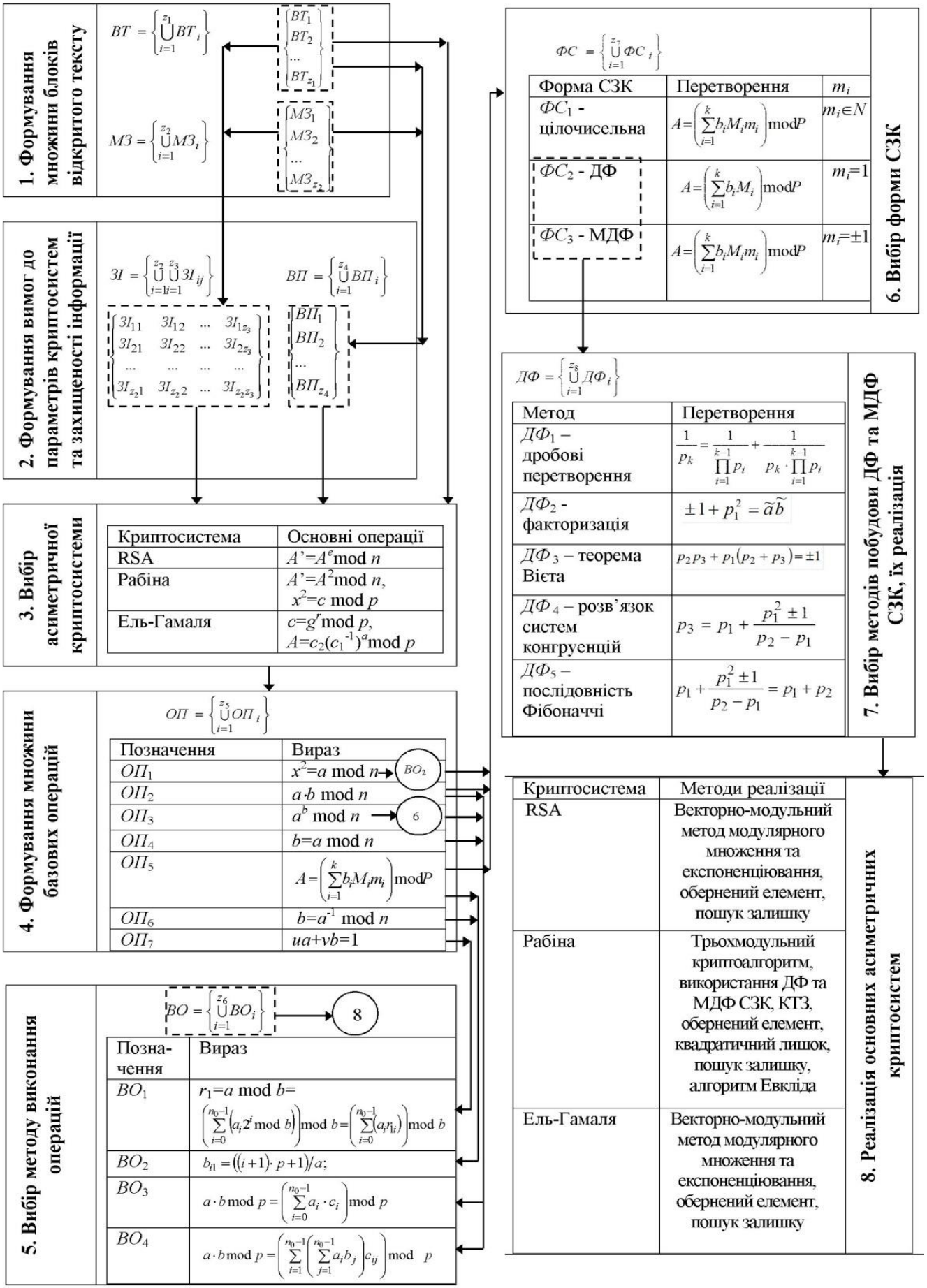

Рис. 1. Структурно-аналітичне відображення розробленої МОБРЧ

На п'ятому етапі відбувається формування множини методів виконання вказаних операцій $BO=\left\{\bigcup_{i=1}^{z_6} BO_i\right\}=\{BO_1, BO_2,...,BO_{z_6}\}$, $i\in[1,z_6]$, де z_6 – кількість операцій. Зокрема, модулярне множення двох n_0-розрядних чисел $a=a_{n_0-1}2^{n_0-1}+...+a_i2^i+...+a_1\cdot 2+a_0$ та $b=b_{n_0-1}2^{n_0-1}+...+b_i2^i+...+b_1\cdot 2+b_0$, де $a_i,b_j=0$ або 1 може виконуватися матрично-модульним методом. Для знаходження результату їх множення за модулем p потрібно побудувати матрицю, представлену в табл. 2, де $c_{ij}=2^{i+j} \bmod p$. Тоді добуток чисел a та $\cdot b$ за модулем p визначається згідно такої формули:

$$a\cdot b \bmod p=\left(\sum_{i=1}^{n_0-1}\left(\sum_{j=1}^{n_0-1}a_ib_j\right)c_{ij}\right)\bmod\ p=$$
$$\left(\sum_{i=1}^{n_0-1}\left(\sum_{j=1}^{n_0-1}a_ib_j\right)2^{i+j} \bmod p\right)\bmod\ p.$$

Таблиця 2

Матриця для модулярного множення

	b_{n_0-1}	…	b_j	…	b_1	b_0
a_{n_0-1}	$c_{n_0-1\ n_0-1}$	…	$c_{n_0-1\,j}$	…	$c_{n_0-1\ 1}$	$c_{n_0-1\ 0}$
…	…	…	…	…	…	…
a_i	$c_{i\ n_0-1}$	…	$c_{i\,j}$	…	$c_{i\ 1}$	$c_{i\ 0}$
…	…	…	…	…	…	…
a_1	$c_{1\ n_0-1}$	…	$c_{1\,j}$	…	$c_{1\ 1}$	$c_{1\ 0}$
a_0	$c_{0\ n_0-1}$	…	$c_{0\,j}$	…	$c_{0\ 1}$	$c_{0\ 0}$

Це означає, що шуканий результат отримується у вигляді суми за модулем p тих c_{ij}, для яких відповідні a_i та $\cdot b_j$ дорівнюють 1. Слід зазначити, що $c_{ij}=c_{ji}$ і кожне наступне значення c_{ij} визначається за допомогою рекурентних співвідношень:

$$c_{i\,j+1}=\begin{cases}2\cdot c_{ij},\ 2\cdot c_{ij}<p,\\ 2\cdot c_{ij}-p,\ 2\cdot c_{ij}\geq p;\end{cases}$$

(1)

$$c_{i+1\,j}=\begin{cases}2\cdot c_{ij},\ 2\cdot c_{ij}<p,\\ 2\cdot c_{ij}-p,\ 2\cdot c_{ij}\geq p.\end{cases}$$

Даний метод дозволяє замінити операцію множення матрично-модульною операцією сумування. Крім того, множення на 2 дуже просто реалізується за допомогою дописування нуля в кінці двійкового запису числа.

Для модулярного експоненіювання $a^b \bmod p$ (вважається, що $b\leq\phi(p)$, $\phi(p)$ – значеня функції Ейлера від модуля p) потрібно використати проміжну матрицю, представлену в табл. 3. Її розмірність дорівнює розрядності n_0 модуля p. В стовбцях матриці записані величини $A_i=a^{2^i} \bmod p$ у двійковій системі числення, тобто $a_{ij}=0,1$.

Тоді будь-який степінь числа a записується за степенями двійки і шуканий результат можна отримати, перемноживши значення у стовбцях, для яких відповідні b_i у розкладі $b=\sum_{i=0}^{n_0-1}b_i\cdot 2^i$ дорівнюють одиниці, за допомогою виразу $a^b \bmod p=\left(\prod_{i=0}^{n_0-1}a^{b_i2^i}\right)\bmod p=\prod_{i=0}^{n_0-1}\left(\left(\sum_{j=0}^{n_0-1}a_{ij}2^j\right)^{b_i}\right)\bmod p$, де a_{ij} – біти двійкового запису числа $a^{2^i} \bmod p=\sum_{j=0}^{n_0-1}a_{ij}2^j$.

Таблиця 3

Матриця піднесення до степеня

b_{n_0-1}	…	b_i	…	b_1	b_0
$a_{n_0-1\ n_0-1}$	…	$a_{i\ n_0-1}$	…	$a_{1\ n_0-1}$	$a_{0 n_0-1}$
…	…	…	…	…	…
$a_{n_0-1\,j}$	…	$a_{i\,j}$	…	$a_{1\,j}$	$c_{0\,j}$
…	…	…	…	…	…
$a_{n_0-1\ 1}$	…	$a_{i\ 1}$	…	$a_{1\ 1}$	$a_{0\ 1}$
$a_{n_0-1\ 0}$	…	$a_{i\ 0}$	…	$a_{1\ 0}$	$a_{0\ 0}$
$a^{2^{n_0-1}} \bmod p$	…	$a^{2^i} \bmod p$	…	$a^{2^1} \bmod p$	$a^{2^0} \bmod p$

Основними перевагами такого методу є здійснення операцій над залишками, а не над багаторозрядними числами, що дозволяє пришвидшити алгоритм модулярного експоненціювання. Слід зазначити, що для заповнення матриці доцільно скористатися таким рекурентним співвідношенням: $a^{2^{i+1}} \bmod p=\left(a^{2^i} \bmod p\right)^2 \bmod p$. Операцію множення можна виконувати методом, описаним вище.

Для зменшення об'єму пам'яті, в якій мають зберігатися проміжні результати матричних обчислень, можна використати векторно-модульний метод модулярного множення чисел $a=\sum_{i=0}^{n_0-1}a_i\cdot 2^i$ та $b=\sum_{j=0}^{n_0-1}b_j\cdot 2^j$. В цьому випадку будується два вектор-рядки (c_i та a_i), перший з яких складається з елементів $c_{\ i}=2\cdot c_{i-1} \bmod p$, $c_{\ 0}=2^0\cdot b \bmod p$, другий – з a_i (табл. 4).

Таблиця 4

Представлення вектор-рядків модульного множення

i	n_0-1	…	2	1	0
c_i	c_{n_0-1}	…	c_2	c_1	c_0
a_i	a_{n_0-1}	…	a_2	a_1	a_0

Слід зазначити, що кожне наступне значення c_i обчислюється за рекурентною формулою, аналогічною (1): $c_{i+1}=\begin{cases}2\cdot c_i,\ 2\cdot c_i<p,\\ 2\cdot c_i-p,\ 2\cdot c_i\ge p.\end{cases}$ Результат модулярного множення двох чисел отримується згідно виразу $a\cdot b \bmod p=\left(\sum_{i=0}^{n_0-1}a_i\cdot c_i\right)\bmod p$, тобто відбувається сумування тих c_i, для яких відповідні a_i дорівнюють 1. При вирішенні задач криптографії заміна операції множення додаванням значно розширює функціональні можливості апаратного забезпечення, а також спрощує реалізацію відповідних спецпроцесорів.

Аналогічно векторно-модульний метод можна використати для модулярного експоненціювання, у якому число a записується за степенями двійки у десятковому вигляді: $a_i=a^{2^i} \bmod p=a_{i-1}^2 \bmod p$, $a_0=a$, $i=0,1,...,n_0-1$ (табл. 5).

Таблиця 5

Матриця векторно-модульного методу модулярного експоненціювання

i	n_0-1	…	2	1	0
b_i	b_{n_0-1}	…	b_2	b_1	b_0
$a^{2^i} \bmod p$	$a^{2^{n_0-1}} \bmod p$	…	$a^{2^2} \bmod p$	$a^{2^1} \bmod p$	$a^{2^0} \bmod p$
a_i	a_{n_0-1}	…	a_2	a_1	a_0

Результат шукається згідно такого виразу: $a^b \bmod p=\left(\prod_{i=0}^{n_0-1}\left(a^{b_i\cdot 2^i}\right)\bmod p\right)\bmod p=\left(\prod_{i=0}^{n_0-1}a_i^{b_i}\right)\bmod p$.

Даним методом також можна виконувати пошук залишку за модулем. Зокрема, для пошуку залишку $a \bmod p$ число a необхідно записати в двійковій системі числення $a=a_{n_0-1}2^{n_0-1}+...+a_i2^i+...+a_1\cdot 2+a_0$, де n_0 – розрядність числа a. Тоді:

$$a \bmod p=\left(\sum_{i=0}^{n_0-1}\left(a_i 2^i \bmod p\right)\right)\bmod p=\left(\sum_{i=0}^{n_0-1}\left(a_i a_{1i}\right)\right)\bmod p, \quad (2)$$

де $a_i=0$ або 1, $a_{1i}=2^i \bmod p$.

З (2) випливає, що шуканий залишок дорівнюватиме сумі тих степенів двійки (або a_{1i}), для яких відповідні $a_i=1$, що проілюстровано в табл. 6.

Таблиця 6

Таблиця знаходження залишку $a \bmod p$

i	n_0-1	n_0-2		2	1	0
a_i	a_{n_0-1}	a_{n_0-2}	…	a_2	a_1	a_0
$2^i \bmod p$	$2^{n_0-1} \bmod p$	$2^{n_0-2} \bmod p$		$2^2 \bmod p$	$2^1 \bmod p$	$2^0 \bmod p$
a_{1i}	$a_{1\,n_0-1}$	$a_{1\,n_0-2}$	…	$a_{1\,2}$	$a_{1\,1}$	$a_{1\,0}$

Два послідовні значення a_{1i} та a_{1i+1} пов'язані рекурентним співвідношенням, аналогічним (1):

$$a_{1i+1}=\begin{cases}2\cdot a_{1\,i},\ 2\cdot a_{1\,i}<p,\\ 2\cdot a_{1\,i}-p,\ 2\cdot a_{1\,i}\ge p.\end{cases} \quad (3)$$

Отже, для знаходження залишку за модулем в (3) не обов'язково виконувати обчислювально витратну операцію ділення з остачею, а обмежитись тільки відніманням модуля.

Метод додавання модуля доцільно використовувати при пошуку оберненого елемента та кореня квадратного за модулем, а також відновленні десяткового числа по його залишках. Зокрема, вираз $ab \bmod p=1$ можна переписати таким чином: $a\cdot b=\tilde{k}\cdot p+1$, де $\tilde{k}$ – деяке ціле число. Звідси слідує, що для пошуку мультиплікативного оберненого елемента необхідно до модуля додати 1 і перевірити, чи ділиться націло отримане число на a. Якщо не ділиться, то далі до отриманого числа послідовно додається модуль до тих пір, поки результатом ділення не буде ціле число. Математично це записується так:

$$p_{01}=p+1;\ \ b_{01}=(p+1)/a;$$
$$p_{11}=2\cdot p+1;\ \ b_{11}=(2\cdot p+1)/a;$$
$$....$$
$$p_{i1}=(i+1)\cdot p+1;\ \ b_{i1}=((i+1)\cdot p+1)/a=b;\ b_{i1}\in Z.$$

Відновлення десяткового числа по його залишках на основі КТЗ є досить громіздкою задачею. Нехай задано систему:

$$\begin{cases}A \bmod p_1=r_1;\\ A \bmod p_2=r_2;\\ .....\\ A \bmod p_i=r_i;\\ .....\\ A \bmod p_j=r_j.\end{cases} \quad (5)$$

Шукане число згідно КТЗ обчислюється за формулою:

$$A=\left(\sum_{i=1}^{j} M_i m_i r_i\right) \bmod P, \qquad (6)$$

де $M_i=\dfrac{P}{p_i}=p_1p_2...p_{i-1}p_{i+1}...p_j$, $m_i=M_i^{-1} \bmod p_i$.

Використання багаторозрядних чисел в (6)може привести до переповнення розрядної сітки. Якщо ж перше рівняння (5) записати у вигляді $A=\gamma_1 p_1+r_1$, де $\gamma_1=0,1,2,...,$ то для пошуку числа A до залишку потрібно додати модуль p_1 стільки разів, щоб виконувалось друге рівняння (5). Далі необхідно додавати добуток модулів p_1p_2, поки не буде виконуватися третє рівняння (5). Процес продовжується до тих пір, поки не буде виконуватися останнє рівняння (5). Математично це записується таким чином:

$$A_1=r_1;$$
$$A_2=A_1+\gamma_1p_1=r_1+\gamma_1p_1;\ A_2 \bmod p_2=r_2;$$
$$A_3=A_2+\gamma_2p_1p_2=r_1+\gamma_1p_1+\gamma_2p_1p_2;\ A_3 \bmod p_3=r_3; \quad (7)$$
$$\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots$$
$$A_i=A_{i-1}+\gamma_{i-1}p_1p_2...p_{i-1};\ A_i \bmod p_i=r_i;$$
$$\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots$$
$$A_j=A=A_{j-1}+\gamma_{j-1}p_1p_2...p_{j-1};\ A_j \bmod p_j=r_j.$$

Шукане число отримується без використання громіздких операцій та необхідності контролю переповнення розрядної сітки при виконанні проміжних обчислень. Даний метод подібний до алгоритму Гарнера, однак у ньому уникається пошук оберненого елемента за модулем для отримання відповідних коефіцієнтів.

Ще одним методом, який доцільно використовувати в асиметричних криптосистемах, є реалізація алгоритму Евкліда (пошуку НСД) на основі розмежованої системи числення. Нехай потрібно знайти НСД двох чисел $a=a_{n_0-1}2^{n_0-1}+...+a_i2^i+...+a_1\cdot 2+a_0$ та $b=b_{n_0-1}2^{n_0-1}+...+b_i2^i+...+b_1\cdot 2+b_0$, причому $a>b=r_0$; $a_i,b_i=0$ або 1.

Виходячи з стандартного алгоритму Евкліда, пошук залишку здійснюється згідно виразів (2)-(3):

$$r_1=a \bmod b=\left(a_{n_0-1}2^{n_0-1}+...+a_i2^i+...+a_1\cdot 2+a_0\right) \bmod b=$$
$$\left(\sum_{i=0}^{n_0-1}\left(a_i 2^i \bmod b\right)\right) \bmod b=\left(\sum_{i=0}^{n_0-1}\left(a_i r_{1i}\right)\right) \bmod b,$$

де $r_{1i}=2^i \bmod b$. Найпростіше реалізувати описаний крок алгоритму Евкліда в розмежованій системі числення за допомогою табл. 7 відповідно до табл. 6.

Таблиця 7

Таблиця знаходження залишку $a \bmod b$

i	n_0-1	n_0-2	…	2	1	0
a_i	a_{n_0-1}	a_{n_0-2}	…	a_2	a_1	a_0
r_{1i}	$r_{1\,n_0-1}$	$r_{1\,n_0-2}$	…	r_{12}	r_{11}	r_{10}

Згідно таблиці 7, r_1 шукається як сума r_{1i} за модулем b, над якими у верхньому рядку розміщено 1, тобто $r_1=\left(\sum_{i=0}^{n_0-1} r_{1i}\right) \bmod b$ при умові, що $a_i=1$. Аналогічно будується табл. 8.

Таблиця 8

Таблиця знаходження залишку $b \bmod r_1$

$b_i=r_{0i}$	$b_{n_0-1}=r_{0\,n_0-1}$	$b_{n_0-2}=r_{0\,n_0-2}$	…	$b_2=r_{02}$	$b_1=r_{01}$	$b_0=r_{00}$
r_{2i}	$r_{2\,n_0-1}$	$r_{2\,n_0-2}$	…	r_{22}	r_{21}	r_{20}

Відповідно $r_2=\left(\sum_{i=0}^{n_0-1} r_{2i}\right) \bmod r_1$ при умові $b_i=1$. Звідси запишеться вираз для знаходження будь-якого залишку: $r_j=\left(\sum_{i=1}^{n_0-1} r_{j-2i}r_{ji}\right) \bmod r_{j-1}$, де $r_{j-2\,i}=0,\ 1$; $r_{j\,i}=2^i \bmod r_{i-1}$. Кількість кроків стандартного алгоритму Евкліда та алгоритму Евкліда в розмежованій системі числення однакові. Однак обчислювально складна операція ділення з остачею на кожному кроці замінюється додаванням.

Більшість з описаних на четвертому етапі операцій можна виконувати на основі СЗК, множина форм якої формується на шостому етапі: $\Phi C=\left\{\bigcup_{i=1}^{z_7}\Phi C_i\right\}=\left\{\Phi C_1,\Phi C_2,...,\Phi C_{z_7}\right\}$, $i\in[1,z_7]$, де z_7- кількість форм СЗК. Представленню десяткового числа A у звичайній цілочисельній СЗК відповідають найменші невід'ємні залишки r_i цього числа у системі взаємно простих модулів p_i, тобто $r_i=N \bmod p_i$. При цьому діапазон обчислень має

лежати в межах $0 \le N \le P-1$, де $P = \prod_{i=1}^{j} p_i$, де j - кількість модулів. СЗК дозволяє розпаралелювати процес виконання обчислень, що є дуже важливо при опрацюванні багаторозрядних чисел в асиметричних криптосистемах.

Зворотнє перетворення у десяткову систему числення відбувається на основі КТЗ (6). У ДФ СЗК модулі p_i підібрані таким чином, що $M_i \bmod p_i = 1 = m_i$. Це дозволяє уникнути операції пошуку оберненого елемента за модулем та множення на нього в (11). Відновлення десяткового числа відбувається згідно такого виразу: $A = \left(\sum_{i=1}^{j} M_i r_i \right) \bmod P$. Недоліком ДФ СЗК є те, що модулі дуже швидко зростають, що неприпустимо у випадку необхідності вибору модулів однакової розрядності. Крім того, перші модулі повинні бути строго визначені і дорівнювати 2 та 3.

У МДФ СЗК модулі підбираються таким чином, щоб $M_i \bmod p_i = \pm 1 = m_i$. Відновлення десяткового числа відбувається за формулою (6), однак $m_i = \pm 1$. Дана умова також усуває необхідність пошуку оберненого елемента та множення на нього в (6). Крім того, проміжні результати набувають менших значень, що спрощує пошук залишку за модулем P.

На сьомому етапі формується множина методів побудови ДФ та МДФ СЗК: $ДФ = \left\{ \bigcup_{i=1}^{z_8} ДФ_i \right\} = \left\{ ДФ_1, ДФ_2, ..., ДФ_{z_8} \right\}$, $i \in [1, z_8]$, де z_8 – кількість методів. У методі дробових перетворень для побудови ДФ СЗК використовується вираз

$$\begin{cases} p_1 = 2, \\ p_i = p_1 p_2 ... p_{i-1} + 1, \ 1 < i < k, \\ p_k = p_1 p_2 ... p_{k-1} - 1, \end{cases}$$

тобто кожен наступний модуль, крім останнього, на одиницю більший від добутку попередніх. Модуль p_k на одиницю менший від добутку попередніх. Для отримання МДФ СЗК кожен наступний модуль на одиницю відрізняється від добутку попередніх:

$$\begin{cases} p_2 = p_1 + 1, \\ p_i = p_1 p_2 ... p_{i-1} \pm 1. \end{cases}$$

Метод факторизації для побудови ДФ СЗК приводить до таких виразів:

$\tilde{a}\tilde{b} = \sum_{i=1}^{k-2} \frac{P}{p_i} - \prod_{i=1}^{k-2} p_i + \left(\prod_{i=1}^{k-2} p_i \right)^2$ (для знаходження модулів праву частину потрібно факторизувати), $\left(\tilde{a}, \tilde{b} - \prod_{i=1}^{k-2} p_i \right) \bmod \left(\sum_{i=1}^{k-2} \frac{P}{p_i} - \prod_{i=1}^{k-2} p_i \right) = 0$, де використана заміна

$$p_{k-1}, p_k = \frac{\tilde{a}, \tilde{b} - \prod_{i=1}^{k-2} p_i}{\sum_{i=1}^{k-2} \frac{P}{p_i} - \prod_{i=1}^{k-2} p_i}.$$

Відповідно, умови пошуку модулів МДФ СЗК: $\tilde{a}\tilde{b} = \pm \sum_{i=1}^{k-2} \frac{P}{p_i} + \left(\prod_{i=1}^{k-2} p_i \right)^2$ (права частина потребує факторизації), $\left(\tilde{a}, \tilde{b} - \prod_{i=1}^{k-2} p_i \right) \bmod \left(\sum_{i=1}^{k-2} \frac{P}{p_i} \right) = 0$, де параметри $\tilde{a}$ і $\tilde{b}$ визначаються із заміни

$$p_{k-1}, p_k = \frac{\tilde{a}, \tilde{b} - \prod_{i=1}^{k-2} p_i}{\sum_{i=1}^{k-2} \frac{P}{p_i}}.$$

Для побудови трьохмодульної МДФ СЗК можна використати методи на основі теореми Вієта, розв'язку систем конгруенцій та послідовності Фібоначчі. Умови побудови МДФ СЗК приводять до рівності $p_2 p_3 + p_1 (p_2 + p_3) = \pm 1$, яка містить суму та добуток невідомих модулів p_2 та p_3. За допомогою теореми Вієта будується квадратне рівняння, розв'язками якого будуть шукані параметри. Розв'язок системи конгруенцій

$$\begin{cases} p_1 p_3 \bmod (p_2) = \pm 1, \\ p_2 p_3 \bmod p_1 = \pm 1, \\ p_1 p_2 \bmod p_3 = \pm 1, \end{cases}$$

який приводить до такого виразу: $p_3 = p_1 + \frac{p_1^2 \pm 1}{p_2 - p_1}$. Крім того, будь-які три послідовні елементи послідовності Фібоначчі, у якій кожне наступне значення дорівнює сумі двох попередніх, утворюють МДФ СЗК.

Восьмий етап передбачає реалізацію вибраної асиметричної криптосистеми (RSA, Рабіна, зокрема трьохмодульної, або Ель-Гамаля) з базовими модулярними операціями (етап 4) на основі вибору методу їх виконання (етап 5) або з використанням відповідних форм СЗК (етап 6), методи побудови яких визначені на етапі 7.

Розроблена методологія за рахунок використання матрично та векторно модульних методів пошуку залишку, модулярного множення та експоненціювання, знаходження оберненого елемента на основі додавання модуля, а також використання ДФ та МДФ СЗК, дозволяє забезпечити зменшення обчислювальної складності, підвищення швидкодії алгоритмів, спеціалізованого програмного і апаратного забезпечення в асиметричних криптосистемах.

ЛІТЕРАТУРА

[1]. М. Касянчук, "Теорія та математичні закономірності досконалої форми системи залишкових класів", *Праці Міжнародного симпозіуму "Питання оптимізації обчислень (ПОО–XXXV)"*, Т. 1. Київ–Кацивелі, С. 306-310, 2009.

[2]. М. Касянчук, І. Якименко, О. Волинський, І. Пітух, "Теорія алгоритмів RSA та Ель–Гамаля в розмежованій системі числення Радемахера–Крестенсона", *Вісник Хмельницького національного університету. Технічні науки*, №3, С. 265-273, 2011.

[3]. Я. Николайчук, М. Касянчук, І. Якименко, С. Івасьєв, "Ефективний метод модулярного множення в теоретико-числовому базисі Радемахера–Крестенсона", *Вісник Національного університету «Львівська політехніка». Комп'ютерні системи та мережі*, № 806, С. 195-199, 2014.

[4]. V. Adki, S. Hatkar, "A Survey on Cryptography Techniques", *International Journal of Advanced Research in Computer Science and Software Engineering*, Vol. 6, No. 6, pp. 469-475, 2016.

[5]. P. Ananda Mohan, *Residue Number Systems: Theory and Applications*, Birkhäuser, 2016, 351 p.

[6]. M. Deryabin, N. Chervyakov, A. Tchernykh, M. Babenko, M. Shabalina, "High Performance Parallel Computing in Residue Number System", *International Journal of Combinatorial Optimization Problems and Informatics*, Vol. 9, No 1, pp. 62-67, 2018.

[7]. M. Kasianchuk, Ya. Nykolaychuk, I. Yakymenko, "Theory and Methods of Constructing of Modules System of the Perfect Modified Form of the System of Residual Classes", *Journal of Automation and Information Sciences*, Vol. 48, No 8, pp. 56-63, 2016.

[8]. D. Kozaczko, S. Ivasiev, I. Yakymenko, M. Kasianchuk, "Vector Module Exponential in the Remaining Classes System", *Proceedings of the 2015 IEEE 8th International Conference on Intelligent Data Acquisition and Advanced Computing Systems: Technology and Applications (IDAACS–2015),* Warsaw (Poland), V. 1, pp. 161-163, 2015.

[9]. A. Okeyinka, "Computational Speeds Analysis of RSA and ElGamal Algorithms", *Proceedings of the World Congress on Engineering and Computer Science (WCECS 2015)*, San Francisco (USA), V. I, pp. 237-242, 2015.

[10]. W. Stallings, *Cryptography and Network Security: Principles and Practice*, 5th Prentice Hall Press Upper Saddle River, NJ, USA, 2010, 719 p.

МЕТОДОЛОГИЯ ОБРАБОТКИ МНОГОРАЗРЯДНЫХ ЧИСЕЛ В АСИММЕТРИЧНЫХ КРИПТОСИСТЕМАХ

На сегодняшний день увеличение длины ключа неизбежно приводит к росту объемов вычислений для защиты информационных потоков при использовании асимметричных криптосистем, наиболее распространенными операциями в которых является модулярное умножение и модулярное экспоненцирование. Существующие методы и алгоритмы выполнения указанных операций базируются на позиционных системах счисления, которые характеризуются значительной временной сложностью в связи с ограниченными возможностями распараллеливания процесса вычислений, что приводит к уменьшению их быстродействия. Использование новых подходов, в частности, векторно-модульного метода модулярного умножения и экспоненцирования, а также системы остаточных классов, позволит расширить функциональные возможности вычислительных систем для шифрования/расшифрования информации. С этой целью предлагается методология, ориентированная на увеличение быстродействия асимметричных криптосистем, базовый механизм которой основывается на восьми этапах: формирование множества блоков открытого текста, формирование требований к параметрам криптосистем и защищенности информации, выбор асимметричной криптосистемы, формирование множества базовых операций, выбор метода выполнения операций, выбор формы системы остаточных классов, выбор методов построения совершенной и модифицированной совершенной форм системы остаточных классов, реализация основных ассиметрических криптосистем на основе указанных подходов. Такая методология позволяет уменьшить временную сложность, повысить быстродействие алгоритмов, специализированного программного и аппаратного обеспечения при обработке многоразрядных чисел в асимметричных криптосистемах.

Ключевые слова: асимметричные криптосистемы, многоразрядные числа, модулярное умножение, модулярное экспоненцирование, векторно-модульный метод, система остаточных классов, методология обработки многоразрядных чисел.

METHODOLOGY OF PROCESSING MULTI-DIGIT NUMBERS IN ASYMMETRIC CRYPTOSYSTEMS

To date, an increase in the key length inevitably leads to an increase in computational volumes to protect information flows using asymmetric cryptosystems, where the most common operations there is the modular multiplication and modular exponentiation. Existing methods and algorithms for performing above-mention operations are based on positional numerical systems that are characterized by considerable time complexity due to the limited possibilities of parallelizing the computation process, which leads to a decrease in their performance. Using of new approaches, in particular, the vector-modular method of modular multiplication and exponential, as well as the system of residual classes, will allow expanding the functionality of computing systems to encrypt / decrypt information. To this goal, a methodology which allows to increase the speed of asymmetric cryptosystems is proposed, and the basic mechanism of which is grounded on the eight stages: the formation of a plurality of open-ended blocks, the formation of requirements for cryptosystem parameters and information security, the choice of an asymmetric cryptosystem, the formation of a set of basic operations, the choice of the method of operations execution , the choice of the form of the system of residual classes, the choice of methods for constructing perfect and modified perfect forms of the system of residual classes, the implementation of basic asymmetries cryptosystems based on these approaches. The proposed methodology can reduce the temporal complexity, increase the speed of algorithms, specialized software and hardware during the processing of multi-digit numbers in asymmetric cryptosystems.

Keywords: asymmetric cryptosystems, multi-digit numbers, modular multiplication, modular exponentiation, vector-modular method, system of residual classes, methodology of processing multi-digit numbers.

Касянчук Михайло Миколайович, кандидат фізико-математичних наук, доцент, доцент кафедри кібербезпеки Тернопільського національного економічного університету.
E-mail: kasyanchuk@ukr.net.
Orcid ID: 0000-0002-4469-8055.
Касянчук Михаил Николаевич, кандидат физико-математических наук, доцент, доцент кафедры кибербезопасности Тернопольского национального экономического университета.
Kasianchuk Mykhailo, PhD in Physics and Mathematics, Associate Professor, Associate Professor of Department of Cybersecurity, Ternopil National Economic University (Ternopil, Ukraine).

Карпінський Микола Петрович, доктор технічних наук, професор, завідувач кафедри інформатики та автоматики Університет у Бельсько-Бялій (м. Бельсько-Бяла, Польща).
E-mail: mpkarpinski@gmail.com.
Orcid ID: 0000-0002-8846-332X.
Карпинский Николай Петрович, доктор технических наук, профессор, заведующий кафедрой информатики и автоматики Университет в БельскоБялой (г. Бельско-Бяла, Польша).
Karpinski Mikolaj, Dr.Sc., Professor, Chairman of Department of Computer Science and Automatics University of Bielsko-Biala (Bielsko-Biala, Poland).

Казмірчук Світлана Володимирівна, доктор технічних наук, зав. кафедри кафедри комп'ютеризованих систем захисту інформації Національного авіаційного університету.
E-mail: sv.kazmirchuk@gmail.com.
Orcid ID: 0000-0001-6083-251X.
Казмирчук Светлана Владимировна, доктор технических наук, зав. кафедры кафедры компьютеризированных систем защиты информации Национального авиационного университета.
Kazmirchuk Svitlana, Dr Eng (Information security), Head of Computerised Information Security Systems Academic Department, National Aviation University.