ПРОГРАМНО-ТЕХНІЧНІ КОМПЛЕКСИ

УДК 004.056.55

Я.М. НИКОЛАЙЧУК
Західноукраїнський національний університет, Тернопіль, Україна,
e-mail: *kmm@wunu.edu.ua.*

І.З. ЯКИМЕНКО
Західноукраїнський національний університет, Тернопіль, Україна,
e-mail: *jiz@wunu.edu.ua.*

Н.Я. ВОЗНА
Західноукраїнський національний університет, Тернопіль, Україна,
e-mail: *nvozna@ukr.net.*

М.М. КАСЯНЧУК
Західноукраїнський національний університет, Тернопіль, Україна,
e-mail: *kasyanchuk@ukr.net.*

АСИМЕТРИЧНІ АЛГОРИТМИ ШИФРУВАННЯ У СИСТЕМІ ЗАЛИШКОВИХ КЛАСІВ

Анотація. Розроблено теоретичні основи асиметричного шифрування на базі системи залишкових класів та її модифікованої досконалої форми. При цьому модулі системи залишкових класів являють собою таємні ключі. Під час відновлення числа за його залишками множення відбувається на довільно вибрані коефіцієнти (відкриті ключі). Встановлено, що криптостійкість запропонованих алгоритмів ґрунтується на розв'язанні задачі факторизації або повного перебору наборів модулів. Розроблені підходи дають змогу практично необмежено збільшувати блок відкритого тексту, усуваючи необхідність використання різних режимів шифрування.

Ключові слова: система залишкових класів, криптоалгоритм, асиметрична криптосистема, шифртекст, криптоаналіз, стійкість.

ВСТУП

На сучасному етапі розвитку інформаційних технологій [1, 2] потрібно розв'язувати низку проблем та науково-технічних задач, пов'язаних з підвищенням стійкості комп'ютерних систем до різного виду атак [3, 4], швидкодії алгоритмів шифрування/розшифрування [5], зменшенням часових складностей виконання базових операцій в асиметричних криптоалгоритмах [6] та створенням засобів захисту інформаційних потоків [7, 8]. Досвід використання відомих алгоритмів шифрування на основі важкооборотних функцій хешування, факторизації [9], дискретного логарифмування, модулярних та інших операцій [10] і розвиток теорії алгоритмів [11], які широко застосовуються на практиці, показує, що їхній потенціал вже наближається до меж своїх можливостей і надалі вони не зможуть бути основою розвитку та вдосконалення засобів захисту інформаційних потоків у сучасних комп'ютерних системах [12, 13].

Зазначимо, що в сучасних асиметричних криптоалгоритмах, які ґрунтуються на позиційних системах числення, є нагальна потреба у розв'язанні трудомістких обчислювальних науково-практичних задач [14], які полягають у необхідності виконання значних обсягів обчислень в реальному часі [15, 16]. Таким чином, важливі та актуальні дослідження з вдосконалення наявних і розроблення нових методів і засобів підвищення продуктивності асиметрич-

них криптоалгоритмів [17] повною мірою відображають сучасні тенденції щодо забезпечення високого рівня захисту інформаційних потоків [18].

Отже, актуальною задачею є застосування непозиційних систем числення, зокрема системи залишкових класів (СЗК) [19, 20] та її різних форм [21, 22] для розроблення асиметричних криптоалгоритмів у СЗК.

ОГЛЯД НАУКОВИХ ПУБЛІКАЦІЙ

Накопичений світовий досвід теорії та методології розв'язання прикладних математичних проблем захисту інформаційних потоків у сучасних комп'ютерних та кіберфізичних системах вказує на основні задачі (побудова стійких криптоалгоритмів, підвищення продуктивності програмних та апаратних засобів захисту інформаційних потоків, зменшення часових складностей базових операцій), які потребують першочергового дослідження. Зокрема, у [23] наведено аргументовані аспекти реалізації програмного та апаратного забезпечення шифрування на основі поліноміальної системи числення залишкових класів, що дало змогу збільшити швидкість виконання операції додавання та розбиття великого блоку вхідних даних на менші підблоки для їхнього паралельного оброблення.

Важливий вклад у розвиток асиметричних криптосистем на основі використання СЗК зроблено в [24]. Авторам вдалося систематизувати і цілісно представити важливі концепції арифметики залишків та нових застосунків СЗК у сучасній криптографії, переходячи від аналізу алгоритмів та складності до сучасних апаратних реалізацій, додатково підвищивши продуктивність систем захисту інформаційних потоків.

У статті [25] приділено значну увагу паралельній апаратній реалізації найбільш важливої операції скалярного множення точок в асиметричних криптосистемах з використанням математичного апарату еліптичних кривих на основі СЗК. Основна задача полягала у мінімізації та оптимізації алгоритмів додавання та подвоєння точок на еліптичній кривій. Крім того, проведено дослідження впливу різних наборів модулів СЗК та їхньої бітової довжини на швидкодію реалізації запропонованого алгоритму.

У [26] досліджено перетворення Монтгомері з використанням СЗК. Запропонований підхід реалізований апаратно для асиметричної криптосистеми RSA з використанням математичного апарату еліптичних кривих для виявлення та аналізу побічних каналів витоку інформації, а також протидії атакам на відмови. Основна мета роботи [27] — зменшення часу реалізації модульних цілочисельних арифметичних операцій у криптосистемі RSA на основі методів швидкого оброблення інформації, що ґрунтуються на використанні принципу кільцевого зсуву у модулярній системі числення.

Особливо актуальними є задачі зменшення часової складності базових операцій асиметричних криптоалгоритмів RSA, Ель-Гамаля та Рабіна, зокрема модулярного множення та експоненціювання, на основі використання векторно-модульних методів, СЗК та її модифікацій [28]. Запропоновані у [29, 30] підходи демонструють ефективність їхнього застосування у сучасних системах захисту інформаційних потоків та дають змогу підвищити продуктивність програмно-апаратних реалізацій. Крім того, використання різних форм СЗК, у яких під час переведення у позиційну систему числення операція пошуку оберненого елемента за модулем не потрібна, суттєво спрощує обчислювальний процес та підвищує ефективність асиметричних криптосистем.

Однак зазначені дослідження спрямовані на оптимізацію певних операцій у криптосистемах, а не на створення системи захисту, яка б поєднувала всі основні компоненти — надійність, продуктивність, стійкість до різного роду атак та ефективність. Тому в цій статті автори намагаються поєднати всі основні складові сучасних алгоритмів шифрування та оцінити їхню стійкість до криптоаналізу.

Будь-яке число S, представлене у позиційній системі числення, записується в СЗК як невід'ємні залишки b_i від ділення цього числа S на кожен із системи натуральних модулів p_i, які повинні бути попарно взаємно простими:

$$b_i = S \bmod p_i. \tag{1}$$

Зворотне переведення числа S у позиційну систему числення відбувається на основі китайської теореми про залишки (КТЗ) [31]:

$$S = \left(\sum_{i=1}^{\nu} b_i P_i f_i \right) \bmod P, \tag{2}$$

де $P = \prod_{i=1}^{\nu} p_i > S$, $P_i = P / p_i$, f_i визначають з виразу $f_i P_i \bmod p_i = 1$, ν — кількість модулів.

Під час генерації ключів для асиметричного шифрування у СЗК обидва абоненти повинні вибрати відомі тільки їм обом системи модулів p_i, які будуть таємними ключами, і відповідно обчислити параметри P_i та f_i. Звідси випливає симетричність запропонованої криптосистеми. Потім кожен абонент довільно вибирає цілі числа w_i, які являють собою відкриті ключі і для яких виконуються умови $1 \le |w_i| \le p_i$ та НСД $(|w_i|, p_i) = 1$. Якщо p_i є простим числом, то друга умова виконується завжди. Наявність відкритих ключів свідчить про асиметричність такої криптосистеми.

Під час шифрування блок відкритого тексту $S < P$ спочатку записують в СЗК у вигляді залишків згідно з виразом (1). Зазначимо, що конкатенація залишків b_i відразу ж може бути шифртекстом. Однак зловмисник, перехопивши декілька повідомлень, може зробити висновки про порядок параметрів p_i, що значно спростить криптоаналіз перехопленого тексту. Для усунення цього недоліку в процесі шифрування для відновлення десяткового числа із його залишків згідно з (2) множити потрібно не на коефіцієнти f_i, а на вибрані отримувачем відкриті ключі w_i, тобто

$$S' = \left(\sum_{i=1}^{\nu} b_i P_i w_i \right) \bmod P. \tag{3}$$

Знайдене число S' — це шифртекст. У свою чергу, отримувач під час розшифрування обчислює величини

$$r_i = (f_i (w_i^{-1} \bmod p_i)) \bmod p_i \tag{4}$$

та визначає зашифровані залишки

$$b_i' = S' \bmod p_i. \tag{5}$$

Для отримання справжніх залишків b_i виконують такі операції:

$$b_i = (b_i' r_i) \bmod p_i = (b_i' f_i w_i^{-1}) \bmod p_i. \tag{6}$$

Тоді відновлення десяткового числа S, яке є відкритим текстом, відбувається згідно з виразом (2). Крім того, можна використати формулу, яка з нього випливає:

$$S = \left(\sum_{i=1}^{\nu} P_i f_i ((b_i' f_i w_i^{-1}) \bmod p_i) \right) \bmod P = \left(\sum_{i=1}^{\nu} P_i f_i ((b_i' r_i) \bmod p_i) \right) \bmod P. \tag{7}$$

Коректність запропонованої криптосистеми, яка поєднує в собі симетричність та асиметричність, випливає із основних властивостей конгруенцій.

Крім того, потрібно врахувати, що p_i є дільником числа P, а також справджується рівність $f_i = P_i^{-1} \bmod p_i$. Звідси можна отримати

$$b_i = (b_i' r_i) \bmod p_i = ((S' \bmod p_i) \cdot (f_i w_i^{-1}) \bmod p_i) \bmod p_i =$$

$$= \left(\left(\left(\sum_{j=1}^{v} b_j w_j P_j \right) \bmod P \right) \bmod p_i \cdot (f_i w_i^{-1}) \bmod p_i \right) \bmod p_i =$$

$$= ((b_i w_i P_i) \bmod P \cdot (f_i w_i^{-1}) \bmod p_i) \bmod p_i = (b_i f_i P_i) \bmod p_i = b_i. \qquad (8)$$

Приклад 1. Виберемо кількість модулів $v = 4$, відкриті ключі $w_1 = 31$, $w_2 = 41$, $w_3 = 43$, $w_4 = 53$ та модулі $p_1 = 43$, $p_2 = 59$, $p_3 = 71$, $p_4 = 79$. Тоді відповідно $P = 14230033$. Як відкритий текст виберемо слово LINE. Якщо встановити найпростіше правило числового кодування буквених символів, коли кожній букві відповідає її номер в алфавіті (нумерація починається з нуля), то слову LINE відповідає число $S = 11081304$. Результат шифрування та попередні розрахунки для розшифрування з використанням звичайної цілочисельної СЗК із вказаними модулями наведено в табл. 1.

Отже, в результаті шифрування згідно з формулою (3) отримуємо такий шифртекст:

$$S' = (330931 \cdot 32 \cdot 31 + 241187 \cdot 42 \cdot 41 + 200423 \cdot 50 \cdot 43 +$$

$$+ 180127 \cdot 53 \cdot 59) \bmod 14230033 = 1710119.$$

Він являє собою суперпозицію декількох параметрів. Тому, не знаючи ключів (модулів), зловмисник, який перехопив це повідомлення, отримає дуже мало інформації про відкритий текст.

Після пошуку параметрів b_i', $w_i^{-1} \bmod p_i$ та r_i розшифрування відбувається згідно з виразом (6):

$$S = (330931 \cdot 29 \cdot ((9 \cdot 37) \bmod 43) + 241187 \cdot 47 \cdot ((4 \cdot 40) \bmod 59) +$$

$$+ 200423 \cdot 7 \cdot ((13 \cdot 53) \bmod 71) + 180127 \cdot 34 \cdot ((6 \cdot 22) \bmod 79)) \bmod 14230033 =$$

$$= 1177944010 \bmod 14230033 = 11081304.$$

Таблиця 1. Результат шифрування та попередні розрахунки для розшифрування з використанням звичайної цілочисельної СЗК

i	1	2	3	4
S	11081304			
p_i	43	59	71	79
P	14230033			
b_i	32	42	50	53
P_i	330931	241187	200423	180127
$P_i \bmod p_i$	3	54	61	7
f_i	29	47	7	34
w_i	31	41	43	59
S'	1710119			
b_i'	9	4	13	6
$w_i^{-1} \bmod p_i$	25	36	38	75
r_i	37	40	53	22

Отже, числове значення відкритого тексту та результат розшифровування є однаковими.

Якщо вибрати деякі значення параметра w_i від'ємними, то можна спростити проміжні обчислення за рахунок знакозмінності доданків у сумі (3) та відповідно зменшити розрядності операндів.

Інший підхід для запропонованого методу шифрування в СЗК полягає в тому, що блок відкритого тексту розбивається на підблоки, які менші від вибраних модулів. Вважається, що ці підблоки є залишками b_i за вибраними модулями. Після вибору параметрів w_i відбувається використання КТЗ згідно з виразом (3).

Далі за формулами (4), (5) обчислюють параметри r_i, b_i' та b_i. Шифртекстом може бути або значення S', або (коли потрібне швидке розшифрування) параметри b_i'. Відкритий текст утворює конкатенація значень b_i.

Для вибраного відкритого тексту LINE = (11081304), модулів $p_1 = 43$, $p_2 = 59$, $p_3 = 71$, $p_4 = 79$ та коефіцієнтів $w_1 = 31$, $w_2 = 41$, $w_3 = 43$, $w_4 = 59$, врахувавши дані табл. 1, згідно з (3) матимемо

$$S' = (330931 \cdot 11 \cdot 31 + 241187 \cdot 8 \cdot 41 + 200423 \cdot 13 \cdot 43 +$$

$$+ 180127 \cdot 4 \cdot 59) \bmod 14230033 = 4982444.$$

З урахуванням формул (4), (5) отримуємо такі результати: $b_1' = 34$, $b_2' = 12$, $b_3' = 19$, $b_4' = 72$, $b_1 = (34 \cdot 29 \cdot 25) \bmod 43 = 11$, $b_2 = (12 \cdot 47 \cdot 36) \bmod 59 = 8$, $b_3 = (19 \cdot 7 \cdot 38) \bmod 71 = 13$, $b_4 = (72 \cdot 34 \cdot 75) \bmod 79 = 4$. Конкатенація значень b_i дає змогу отримати відкритий текст LINE = (11081304). За угодою між відправником та отримувачем шифртекстом може бути або число $S' = 4982444$, або число, що являє собою конкатенацію значень b_i': 34121972.

ВИКОРИСТАННЯ МОДИФІКОВАНОЇ ДОСКОНАЛОЇ ФОРМИ СЗК ДЛЯ АСИМЕТРИЧНОГО ШИФРУВАННЯ

Для спрощення розрахунків і відповідно зменшення часу розшифрування доцільно використовувати набори модулів, що утворюють модифіковану досконалу форму (МДФ) СЗК [16, 17], для якої виконується умова $f_i = \pm 1$. У цьому випадку доданки у сумі (7) мають різні знаки, що спрощує проміжні результати обчислень.

Приклад 2. Нехай $p_1 = 49$, $p_2 = 50$, $p_3 = 69$, $p_4 = 71$. Параметри w_i та відкритий текст S залишаються такі ж самі, як і в прикладі 1. Результат шифрування та попередні розрахунки для розшифрування з використанням МДФ СЗК із вказаними модулями згідно з формулами (3)–(7) наведено в табл. 2.

Отже, в результаті шифрування згідно з формулою (3) отримуємо такий шифртекст:

$$S' = (244950 \cdot 3 \cdot 31 + 240051 \cdot 4 \cdot 41 + 173950 \cdot 42 \cdot 43 + 169050 \cdot 50 \cdot 59) \bmod 12002550 =$$

$$= 874999914 \bmod 12002550 = 10816314.$$

Відповідно до формули (7) матимемо відкритий текст:

$$S = (-244950 \cdot ((-5 \cdot 19) \bmod 49) + 240051 \cdot ((14 \cdot 11) \bmod 50) +$$

$$+ 173950 \cdot ((-12 \cdot 8) \bmod 69) - 169050 \cdot ((32 \cdot 6) \bmod 71)) \bmod 12002550 =$$

$$= -921246 \bmod 12002550 = 11081304.$$

Таблиця 2. Результат шифрування та попередні розрахунки для розшифрування з використанням МДФ СЗК

i	1	2	3	4
S	11081304			
p_i	49	50	69	71
P	12002550			
b_i	3	4	42	50
P_i	244950	240051	173950	169050
$P_i \bmod p_i$	$48 \bmod 49 = -1 \bmod 49$	1	1	$70 \bmod 71 = -1 \bmod 71$
f_i	–1	1	1	–1
w_i	31	41	43	59
S'	10816314			
b'_i	5	14	12	32
$w_i^{-1} \bmod p_i$	19	11	61	65
r_i	–19	11	–8	6

Отже, проміжні обчислення виконуються над меншими числами в порівнянні з попереднім прикладом, що дає змогу пришвидшити процес розшифрування повідомлення.

У випадку, коли підблоки відкритого тексту являють собою залишки b_i за модулями p_i, які утворюють МДФ СЗК, для вибраних вище параметрів S та w_i, врахувавши дані табл. 2, згідно з (3) отримаємо

$$S' = (244950 \cdot 11 \cdot 31 + 240051 \cdot 8 \cdot 41 + 173950 \cdot 13 \cdot 43 + 169050 \cdot 4 \cdot 59) \bmod 12002550 =$$
$$= 299398528 \bmod 12002550 = 11337328.$$

Для розшифрування за формулами (4), (5) матимемо такі результати: $b'_1 = 2$, $b'_2 = 28$, $b'_3 = 7$, $b'_4 = 48$, $b_1 = (-2 \cdot 19) \bmod 49 = 11$, $b_2 = (28 \cdot 11) \bmod 50 = 8$, $b_3 = (-7 \cdot 8) \bmod 69 = 13$, $b_4 = (48 \cdot 6) \bmod 71 = 4$.

Після конкатенації значень b_i утворюється відкритий текст LINE = (11081304). Аналогічно до попереднього за згодою абонентів шифртекстом може бути або число $S' = 11337328$, або число, що являє собою конкатенацію значень b'_i: 02280748.

ОЦІНЮВАННЯ КРИПТОСТІЙКОСТІ РОЗРОБЛЕНОГО АСИМЕТРИЧНОГО АЛГОРИТМУ ШИФРУВАННЯ З ВИКОРИСТАННЯМ СЗК

Для оцінювання криптостійкості розробленого асиметричного криптоалгоритму з використанням СЗК необхідно здійснити повний перебір усіх можливих варіантів взаємно простих модулів криптоперетворень p_i та знайти відповідні їм значення P_i та f_i або розв'язати задачу факторизації (аналогічно криптосистемі RSA). Знаючи зазначені параметри і перехопивши у каналі зв'язку S' та w_i, зловмисник зможе знайти відкритий текст S.

Тому оцінювання криптостійкості зводиться до визначення часових складностей пошуку p_i, P_i, b_i. Значення P_i обчислюється згідно з формулою $P_i = P / p_i$, $P = \prod_{i=1}^{\nu} p_i$. Оскільки для n-розрядних чисел необхідно виконати ν операцій множення та ділення на p_i, часову складність для визначення P_i можна оцінити як $O1(\nu \cdot n^2 (n+1)^2) \approx O1(\nu n^4)$.

Для кожного набору модулів часова складність знайденого на основі формули (3) добутку $b_i P_i w_i$ оцінюється як $O2(2n^2)$ (b_i, P_i, w_i — n-розрядні числа). Крім того, в (2) виконується сумування всіх наборів $b_i P_i w_i$ залежно від кількості модулів, отже часова складність цієї операції оцінюється як $O3(\nu n)$.

Найбільш трудомісткою операцією оцінювання криптостійкості запропонованого асиметричного алгоритму шифрування у СЗК є визначення набору попарно взаємно простих модулів криптоперетворення p_i. Пошук p_i виконується повним перебором n-бітних чисел. Застосування функції Ейлера $\varphi(p_i)$ дає змогу визначити кількість взаємно простих чисел із заданим p_i. Максимальне значення функції Ейлера досягається тоді, коли p_i буде найбільшим простим числом заданої розрядності n, тобто $\varphi_{\max}(p_i) = p_i - 1$ [32]. Для n-бітного фіксованого максимального простого модуля $p_1 = p_{i\max}^{(n)}$ кількість варіантів вибору модуля p_2 буде становити $\varphi(p_1) = p_{i\max}^{(n)} - 1 = p_1 - 1$, відповідно для p_3 буде $\varphi(p_2), \ldots,$ для p_ν становить $\varphi(p_{\nu-1})$. Вважатимемо, що $p_1 > p_2 > \ldots > p_{\nu-1} > p_\nu$, причому тільки один із цих модулів може бути складеним. Тоді набори модулів криптоперетворень розробленого асиметричного алгоритму шифрування у СЗК можна отримати такою кількістю способів:

$$Z = \prod_{i=1}^{\nu-1} \varphi(p_i). \tag{9}$$

Зазначимо, що криптостійкість розробленого алгоритму досягає свого максимуму, коли $\varphi(p_i^{(n)})$ набувають найбільших значень, тобто $p_i^{(n)}$ — максимальні прості числа. Отже, для наборів з ν модулів часова складність буде становити $O4(n^\nu)$. З урахуванням оцінок часових складностей базових операцій загальна складність математичної атаки становитиме $O(\nu^2 \cdot n^{\nu+7})$. Графік її залежності від розрядності модулів та їхньої кількості наведено на рис. 1.

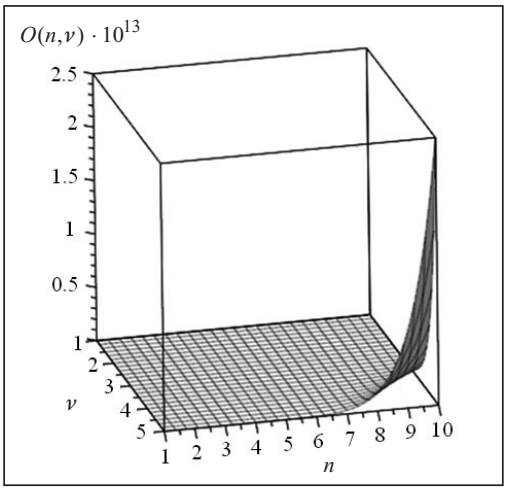

Рис. 1. Залежність криптостійкості запропонованого криптоалгоритму від розрядності та кількості модулів

Як бачимо з аналітичної оцінки часової складності та її графічної залежності, збільшення криптостійкості можна досягнути завдяки збільшенню кількості модулів, їхньої розрядності, а також вибором таких модулів, для яких значення $\varphi(p_i)$ буде максимальним.

ВИСНОВКИ

Вперше запропоновано асиметричні криптоалгоритми на основі СЗК та її МДФ, які за рахунок збільшення розмірності вхідних параметрів (розміру повідомлення, розрядності та кількості модулів) забезпечують необхідний рівень захисту даних. Особливості розглянутого підходу полягають в тому, що обрані системи модулів є таємними ключами, а для відновлення числа за його залишками з ви-

користанням КТЗ множення виконується не на обернені елементи за модулем, а на довільно вибрані коефіцієнти (відкриті ключі) асиметричного шифрування в СЗК, у результаті чого досягається підвищення криптостійкості алгоритму. Отримано аналітичні вирази, які вказують, що високої криптостійкості можна досягнути, збільшуючи розрядність вхідних параметрів, кількість модулів (ключів), а також вибираючи такі модулі, для яких значення функції Ейлера буде максимальним. Представлено графічну залежність криптостійкості від розрядності та кількості модулів. Встановлено, що криптостійкість запропонованих алгоритмів, аналогічно криптосистемі RSA, ґрунтується на розв'язанні задачі факторизації або повного перебору наборів модулів.

СПИСОК ЛІТЕРАТУРИ

1. Van Steen M., Tanenbaum A.S. A brief introduction to distributed systems. *Computing*. Vol. 98. 2016. P. 967–1009. https://doi.org/10.1007/s00607-016-0508-7.
2. Lopez V., Miñana G., Tejada J., Caro R. Benchmarking for stability evaluation of computer systems. In: Knowledge Engineering and Management. Advances in Intelligent Systems and Computing. Sun F., Li T., Li H. (Eds.). Vol. 214. Berlin; Heidelberg: Springer, 2014. P. 509–517. https://doi.org/10.1007/978-3-642-37832-4_46.
3. Zadiraka V.K., Kudin A.M. New models and methods for estimating the cryptographic strength of information security systems. *Cybernetics and Systems Analysis.* 2017. Vol. 53, N 6. P. 978–985. https://doi.org/10.1007/s10559-017-9999-2.
4. Idrizi F., Dalipi F., Rustemi E. Analyzing the speed of combined cryptographic algorithms with secret and public key. *International Journal of Engineering Research and Development.* 2013. Vol. 8, Iss. 3. P. 45–51.
5. Kasyanchuk M., Yakymenko I., Ivasiev S., Gomotiuk O., Shylinska I., Bilovus L. Algorithmic support for rabin cryptosystem implementation based on addition. *Proc. of the 10th Intern. Conf. "Advanced Computer Information Technology (ACIT 2020)"*. Deggendorf, Germany, 2020. P. 779–782. https://doi.org/10.1109/ACIT49673.2020.9208923.
6. Mukhtar A., Tiwari P.M. IoT security algorithms: A performance comparison. In: Intelligent Circuits and Systems. 1st ed. Ch. 87. CRC Press, 2021. P. 585–593. https://doi.org/10.1201/9781003129103-87.
7. Shevchuk R., Pastukh Ya. Improve the security of social media accounts. *Proc. 9th Intern. Conf. on Advanced Computer Information Technologies (ACIT-2019)* (Ceske Budejovice, Czech Republic, 5–7 June, 2019). Ceske Budejovice, 2019. P. 439–442. https://doi.org/10.1109/ACITT.2019.8779963.
8. Patila P., Narayankarb P., Narayan D.G., Meena S.M. A comprehensive evaluation of cryptographic algorithms: DES, 3DES, AES, RSA and Blowfish. *Procedia Computer Science. Intern. Conf. on Information Security & Privacy (ICISP 2015)* (11–12 December 2015). Nagpur, India, 2016. P. 617–624. https://doi.org/10.1016/j.procs.2016.02.108.
9. Khan A.G., Basharat S., Riaz M.U. Analysis of asymmetric cryptography in information security based on computational study to ensure confidentiality during information exchange. *International Journal of Scientific & Engineering Research*. 2018. Vol. 9, Iss. 10. P. 992–999. https://doi.org/10.13140/RG.2.2.30495.61602.
10. Ghafar A.H.A., Ariffin M.R.K., Asbullah M.A. Extending pollard class of factorable RSA modulus. *Proc. of the 6th Intern. Cryptology and Information Security Conf. 2018 (CRYPTOLOGY 2018).* 2018. P. 103–118.

11. Ullah A., Hossain A. Design and implementation of android based text encryption and decryption technique. *Journal of Internet & Networking.* 2019. Vol. 1, Iss. 3. P. 1–16. https://doi.org/10.5281/zenodo.3428244.

12. Lone A.H., Khalique A. Generalized RSA using 2^k prime numbers with secure key generation. *Security and Communication Networks.* 2016. P. 4443–4450. https://doi.org/10.1002/sec.1619.

13. Vozna N.Y., Nykolaychuk Y.M., Volynskyi O.I. Algorithms for solving problems of cryptographic protection of color image pixels in the Rademacher's basis and residue number systems. *Cybernetics and Systems Analysis.* 2019. Vol. 55, N 3. P. 474–487. https://doi.org/10.1007/s10559-019-00155-2.

14. Abubakar S.I., Ariffin M.R.K., Asbullah M.A. A new simultaneous Diophantine attack upon RSA moduli N = pq. *Proc. of the 6th Intern. Cryptology and Information Security Conf*. 2018 (CRYPTOLOGY 2018). 2018. P. 119–138.

15. Overmars A., Venkatraman S. Mathematical attack of RSA by extending the sum of squares of primes to factorize a semi-prime. *Math. Comput. Appl.* 2020. P. 1–15. https://doi.org/10.3390/mca25040063.

16. Mohan Ananda P. Residue number systems: Theory and applications. Birkhäuser, 2016. 351 p.

17. Nykolaychuk Ya.M., Kasianchuk M.M., Yakymenko I.Z. Theoretical foundations of the modified perfect form of residue number system. *Cybernetics and Systems Analysis.* 2016. Vol. 52, N 2. P. 219–223. https://doi.org/10.1007/s10559-016-9817-2.

18. Kasianchuk M., Nykolaychuk Ya., Yakymenko I. 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*. 2016. Vol. 48, N 8. P. 56–63. https://doi.org/10.15588/1607-3274-2017-3-6.

19. Kalimoldayev M., Tynymbayev S., Magzom M. Software-hardware facilities for cryptosystems based on polynomial RNS. *Problems of Informatics*. 2018. N 4. P. 73–84.

20. Schinianakis D., Stouraitis T. Residue number systems in cryptography: Design, challenges, robustness. In: Secure System Design and Trustable Computing. Chang C.H., Potkonjak M. (Eds.). Cham: Springer, 2016. P. 115–161. https://doi.org/10.1007/978-3-319-14971-4_4.

21. Schinianakis D.M., Fournaris A.P., Harris E.M., Kakarountas A.P., Stouraitis T. An RNS implementation of an Fp elliptic curve point multiplier. *IEEE Transactions on Circuits and Systems. I: Regular Papers*. 2009. Vol. 56, Iss. 6. P. 1202–1213.

22. Bajard J.-C., Eynard J., Merkiche N. Montgomery reduction within the context of residue number system arithmetic. *Journal of Cryptographic Engineering*. 2018. Vol. 8. P. 189–200. https://doi.org/10.1007/s13389-017-0154-9.

23. Krasnobayev V.A., Tyrtyshnikov O.I., Sliusar I.I., Kurchanov V.N., Koshman S.A. The model and the method of implementation of integer arithmetic operations within the RSA crypto algorithms. *Information Processing Systems.* 2014. N 1(117). P. 117–122.

24. Jeffrey H., Jill P., Joseph H. An introduction to mathematical cryptography. Berlin: Springer, 2008. 540 p.

25. Kasianchuk M.M., Yakymenko I.Z., Nykolaychuk Y.M. Symmetric cryptoalgorithms in the residue number system. *Cybernetics and Systems Analysis.* 2021. Vol. 57, N 2. P. 329–336. https://doi.org/10.1007/s10559-021-00358-6.

26. Abomhara M., Koien G.M. Cyber security and the Internet of Things: Vulnerabilities, threats, intruders and attacks. *J. Cyber Secur. Mobil.* 2015. Vol. 4, Iss. 1. P. 65–88. https://doi.org/10.13052/jcsm2245-1439.414.

27. Ivasiev S., Kasianchuk M., Yakymenko I., Shevchuk R., Karpinski M., Gomotiuk O. Effective algorithms for finding the remainder of multi-digit numbers. *Proc. of the 9th Intern. Conf. "Advanced Computer Information Technologies (ACIT-2019)*". Ceske Budejovice, Czech Republic, 2019. P. 175–178. https://doi.org/10.1109/ACITT.2019.8779899.

28. Karpinski M., Rajba S., Zawislak S., Warwas K., Kasianchuk M., Ivasiev S., Yakymenko I. A method for decimal number recovery from its residues based on the addition of the product modules. *Proc. of the 10th IEEE Intern. Conf. "Intelligent Data Acquisition and Advanced Computing Systems: Technology and Applications (IDAACS-2019)".* Metz, France, 2019. P. 13–17. https://doi.org/10.1109/IDAACS.2019.8924395.

29. Yakymenko I., Kasyanchuk M., Nykolaychuk Ya. Matrix algorithms of processing of the information flow in computer systems based on theoretical and numerical Krestenson's basis. *Proc. of the X Intern. Conf. "Modern Problems of Radio Engineering, Telecommunications and Computer Science (TCSET–2010)"*. L'viv–Slavske, Ukraine, 2010. P. 241.

30. Rajba T., Klos-Witkowska A., Ivasiev S., Yakymenko I., Kasianchuk M. Research of time characteristics of search methods of inverse element by the module. *Proc. of the 2017 IEEE 9th Intern. Conf. "Intelligent Data Acquisition and Advanced Computing Systems: Technology and Applications (IDAACS-2017)"*. Bucharest, 2017. Vol. 1. P. 82–85. https://doi.org/10.1109/IDAACS.2017.8095054.

31. Kozaczko D. Kasianchuk M., Yakymenko I., Ivasiev S. Vector module exponential in the remaining classes system. *Proc. of the 2015 IEEE 8th Intern. Conf. on Intelligent Data Acquisition and Advanced Computing Systems: Technology and Applications (IDAACS-2015).* Warsaw, 2015. Vol. 1. P. 161–163.

32. Suárez-Albela M., Fraga-Lamas P., Fernández-Caramés T.M. A practical evaluation on RSA and ECC-based cipher suites for IoT high-security energy-efficient fog and mist computing devices. *Sensors*. 2018. Vol. 18, Iss. 11. 3868. https://doi.org/10.3390/s18113868.

Ya.M. Nykolaychuk, I.Z. Yakymenko, N.Ya. Vozna, M.M. Kasianchuk

RESIDUE NUMBER SYSTEM ASYMMETRIC CRYPTOALGORITHMS

Abstract. Theoretical foundations of asymmetric encryption based on the residue number system and its modified perfect form are developed. The selected moduli of the residue number system are considered to be secret keys. When recovering a number from its residues, multiplication by arbitrarily selected coefficients (public keys) takes place. It is established that cryptostability of the proposed algorithms is based on solving the problem of factorization or exhaustive search of sets of moduli. The developed approaches allow us to increase the block of plaintext almost indefinitely, eliminating the need to use different encryption modes.

Keywords: residue number system, cryptoalgorithm, asymmetric cryptosystem, ciphertext, cryptanalysis, stability.

Надійшла до редакції 25.10.2021