УДК 004.056.55

М.М. КАСЯНЧУК, І.З. ЯКИМЕНКО, Я.М. НИКОЛАЙЧУК

СИМЕТРИЧНІ КРИПТОАЛГОРИТМИ У СИСТЕМІ ЗАЛИШКОВИХ КЛАСІВ

Анотація. Представлено теоретичні основи симетричного шифрування на основі системи залишкових класів. Особливості цього підходу полягають у тому, що у випадку відновлення десяткового числа за його залишками з використанням китайської теореми про залишки множення здійснюється на довільно вибрані коефіцієнти (ключі). Встановлено, що криптостійкість розроблених методів визначається кількістю модулів та їхньою розрядністю. З'ясовано, що описані методи забезпечують можливість практично необмеженого збільшення блоку відкритого тексту для шифрування, при цьому зникає потреба у використанні різних режимів шифрування.

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

ВСТУП

Останніми роками внаслідок глобалізації інформаційного суспільства, багатократного збільшення обсягів конфіденційної інформації, розвитку різноманітних засобів інформаційних атак забезпечення інформаційної безпеки набуває все більшого значення [1]. Інформаційні ресурси потребують постійного захисту від несанкціонованого доступу інших користувачів [2]. Однак, надзвичайно стрімке поширення комп'ютерних систем у різних сферах людської діяльності сприяє збільшенню вразливостей автоматизованих систем обробки даних до деструктивних дій різного роду, наслідками яких можуть бути руйнування, модифікація або витік інформації. Для мінімізації ризиків несанкціонованого доступу широко використовують криптографічні методи захисту інформації, які діляться на дві великі групи: симетричні та асиметричні [3–5]. Слід відмітити, що алгоритми асиметричних криптосистем є досить трудомісткими, тому на практиці їх доцільно використовувати в тих випадках, коли обсяг шифрованої інформації є незначним, але дуже важливим. Відповідно, симетричні методи є найбільш поширеними для шифрування великих обсягів інформації. При цьому до них висувають надзвичайно високі вимоги, зокрема, щодо підвищення швидкодії та стійкості, які продиктовані саме стрімким розвитком обчислювальних засобів.

АНАЛІЗ ПУБЛІКАЦІЙ

Переважна більшість найбільш поширених симетричних криптосистем, зокрема, AES, IDEA, ГОСТ 28147-89, національний український стандарт шифрування «Калина» тощо є блочними, причому розмір блока зазвичай не перевищує розмір ключа [6–8]. Тому для шифрування досить великого тексту потрібно застосовувати криптоалгоритми кілька разів або в різних режимах роботи, що знижує стійкість та ускладнює програмну та/або апаратну реалізацію [9]. До того ж, симетричні криптосистеми, на відміну від асиметричних, не забезпечують можливість розширення блока шифрування.

Усунути зазначені недоліки можна за допомогою методів шифрування, розроблених у системі залишкових класів (СЗК) [10]. Нині вона активно використовується в асиметричних криптосистемах [11–13] для розпаралелювання процесу

виконання модулярних операцій множення та експоненціювання [14]. Цей підхід є найбільш перспективним для підвищення швидкодії обчислювальних систем та зменшення часової складності [15–17]. Крім того, перевагами СЗК є відсутність міжрозрядних переносів, можливість виконання операцій над числами, які є меншими за вибрані модулі, контроль переповнення розрядної сітки добутком модулів тощо.

Попри те, що СЗК мають низку недоліків (складність виконання ділення та порівняння, а також труднощі під час відновлення числа із його залишків у позиційну систему числення), їхнє успішне застосування в алгоритмах шифрування надає змогу розробити нові підходи до організації обчислень [18]. До того ж, спростити відновлення десяткового числа із його залишків можна завдяки використанню досконалої (ДФ) та модифікованої досконалої (МДФ) форм СЗК, оскільки при цьому не виконуються складні з обчислювального погляду операції пошуку мультиплікативного оберненого елемента за модулем та множення на нього [19, 20]. Ці особливості СЗК свідчать про її перспективність для розв'язання надзвичайно актуальної задачі з розроблення високопродуктивних симетричних криптоалгоритмів, які нададуть змогу забезпечити необхідний рівень захисту даних та більшу стійкість до криптоаналізу порівняно з класичними.

РОЗРОБЛЕННЯ СИМЕТРИЧНИХ МЕТОДІВ ШИФРУВАННЯ В СИСТЕМІ ЗАЛИШКОВИХ КЛАСІВ

Будь-яке десяткове число N в СЗК можна представити у вигляді невід'ємних залишків b_i від ділення N на кожний із системи натуральних попарно взаємно простих модулів p_i:

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

Зазвичай відновлення числа N здійснюється на основі китайської теореми про залишки (КТЗ) [21, 22]:

$$N = \left(\sum_{i=1}^{s} b_i M_i m_i \right) \bmod P, \tag{2}$$

де $P = \prod_{i=1}^{s} p_i$, $M_i = \dfrac{P}{p_i}$, m_i отримують з виразу $m_i = M_i^{-1} \bmod p_i$, s — кількість модулів [23, 24]. При цьому має виконуватися нерівність $N < P$.

Суть одного з методів симетричного шифрування в СЗК полягає в тому, що під час відновлення числа в позиційну систему числення за його залишками у сумі (2) множення здійснюють не на параметри $m_i = M_i^{-1} \bmod p_i$, а на довільно вибрані коефіцієнти k_i. Отже, для генерації ключів обидва абоненти повинні вибрати відомі тільки їм обом системи модулів p_i та відповідні коефіцієнти k_i, для яких виконуються такі умови: $1 < k_i < p_i$ та НСД $(k_i, p_i) = 1$. Якщо p_i є простим числом, то друга умова виконується завжди. Відповідно і відправнику, і отримувачу відомі параметри M_i та m_i. Для шифрування текстову інформацію необхідно записати у числовій формі. Найпоширенішим класичним методом є заміна букви на її номер в алфавіті, причому нумерація починається з 0. Тоді на етапі шифрування спочатку вибирають блок відкритого тексту $N < P$, який потім записують в СЗК згідно з виразом (1). Шифрування здійснюється під час відновлення числа в позиційну систему числення згідно з таким виразом:

$$N' = \left(\sum_{i=1}^{s} b_i M_i k_i \right) \bmod P. \tag{3}$$

Знайдене число є шифртекстом, який передається від одного абонента до іншого.

Під час розшифрування спочатку обчислюють такі величини:

$$q_i = (m_i (k_i^{-1} \bmod p_i)) \bmod p_i;\ b'_i = N' \bmod p_i. \tag{4}$$

Для отримання істинних залишків b_i необхідно виконати перетворення згідно із співвідношенням:

$$b_i = (b'_i q_i) \bmod p_i = (b'_i m_i k_i^{-1}) \bmod p_i. \tag{5}$$

Відповідно, відновлення числа N, яке є відкритим текстом, здійснюється за формулою (2) або можна використати такий вираз, який з неї випливає:

$$\begin{aligned} N &= \left(\sum_{i=1}^{s} M_i m_i ((b'_i m_i k_i^{-1}) \bmod p_i) \right) \bmod P = \\ &= \left(\sum_{i=1}^{s} M_i m_i ((b'_i q_i) \bmod p_i) \right) \bmod P. \end{aligned} \tag{6}$$

Коректність запропонованої криптосистеми встановлюється з властивостей конгруенцій з урахуванням того, що p_i є дільником числа P, та рівності $m_i = M_i^{-1} \bmod p_i$. Звідси отримуємо:

$$\begin{aligned} b_i &= (b'_i q_i) \bmod p_i = ((N' \bmod p_i) \cdot (m_i k_i^{-1}) \bmod p_i) \bmod p_i = \\ &= \left(\left(\left(\sum_{j=1}^{s} b_j k_j M_j \right) \bmod P \right) \bmod p_i \cdot (m_i k_i^{-1}) \bmod p_i \right) \bmod p_i = \\ &= ((b_i k_i M_i) \bmod P \cdot (m_i k_i^{-1}) \bmod p_i) \bmod p_i = (b_i m_i M_i) \bmod p_i = b_i. \end{aligned} \tag{7}$$

У табл. 1 наведено приклад використання запропонованої симетричної криптосистеми для трьох модулів ($s = 3$), відкритого тексту $RNS = (171318)$, модулів $p_1 = 47$, $p_2 = 59$, $p_3 = 71$ та вибраних коефіцієнтів $k_1 = 19$, $k_2 = 23$, $k_3 = 31$.

Отже, згідно з виразом (3) шифртекст отримують у такий спосіб:

$$N' = (4189 \cdot 3 \cdot 19 + 3337 \cdot 41 \cdot 23 + 2773 \cdot 66 \cdot 31) \bmod 196883 = 2504.$$

Після пошуку параметрів b'_i, $k_i^{-1} \bmod p_i$ та q_i розшифрування здійснюється згідно з виразом (6):

$$\begin{aligned} N = (&4189 \cdot 8 \cdot ((13 \cdot 40) \bmod 47) + 3337 \cdot 34 \cdot ((26 \cdot 22) \bmod 59) + \\ &+ 2773 \cdot 18 \cdot ((19 \cdot 67) \bmod 71)) \bmod 196883 = 171318. \end{aligned}$$

Таблиця 1. Приклад використання запропонованої симетричної криптосистеми на основі СЗК

i	N	p_i	P	M_i	m_i	b_i	k_i	N'	b'_i	$k_i^{-1} \bmod p_i$	q_i
1	171318	47	196883	4189	8	3	19	2504	13	5	40
2		59		3337	34	41	23		26	18	22
3		71		2773	18	66	31		19	55	67

У тому разі, коли абоненти обмежені у часі, доцільно прийняти, що $k_i = 1$. Це зменшує стійкість до криптоаналізу, однак шифрування здійснюється за спрощеною формулою:

$$N' = \left(\sum_{i=1}^{s} b_i M_i \right) \bmod P. \tag{8}$$

До того ж, під час розшифрування зникає потреба у виконанні процедури пошуку оберненого елемента за модулем та множення на нього, оскільки $q_i = m_i$ та розшифрування здійснюється згідно з такими виразами:

$$b_i = (b_i' m_i) \bmod p_i; \; N = \left(\sum_{i=1}^{s} M_i m_i ((b_i' m_i) \bmod p_i) \right) \bmod P. \tag{9}$$

До прикладу, для заданих у табл. 1 вхідних параметрів за формулами (8), (9) можна отримати $N' = (4189 \cdot 3 + 3337 \cdot 41 + 2773 \cdot 66) \bmod 196883 = 135519$; $b_1' = 18$, $b_2' = 55$, $b_3' = 51$; $N = (4189 \cdot 8 \cdot ((18 \cdot 8) \bmod 47) + 3337 \cdot 34 \cdot ((55 \cdot 34) \bmod 59) + 2773 \cdot 18 \cdot$ $\cdot((51 \cdot 18) \bmod 71)) \bmod 196883 = 171318$.

Слід відмітити, що для зменшення операндів під час відновлення числа за його залишками деякі параметри k_i можна вибрати від'ємними. Зокрема, для вхідних даних з табл. 1 та $k_1 = -19$, $k_2 = -23$, $k_3 = 31$ суми (3), (6) стають знакозмінними: $N' = (-4189 \cdot 3 \cdot 19 - 3337 \cdot 41 \cdot 23 + 2773 \cdot 66 \cdot 31) \bmod 196883 = 122281$, $b_1' = 34$, $b_2' = 33$, $b_3' = 19$, $q_1 = -40$, $q_2 = -22$, $q_3 = 67$, $N = (4189 \cdot 8 \cdot ((-34 \cdot 40) \bmod 47) + 3337 \cdot$ $\cdot 34 \cdot ((-33 \cdot 22) \bmod 59) + 2773 \cdot 18 \cdot ((19 \cdot 67) \bmod 71)) \bmod 196883 = 171318$.

Інший метод симетричного шифрування у СЗК полягає в тому, що відкритий текст розбивають на блоки, які є меншими від вибраних модулів і виступають залишками b_i за цими модулями. Після вибору параметрів k_i шифрування здійснюється згідно з виразом (3), при цьому шифртекстом буде значення N'.

Розшифрування здійснюється за формулами (4), (5), згідно з якими шукають параметри q_i, b_i', та b_i. Конкатенація значень b_i утворює відкритий текст. Слід зазначити, що у разі потреби у швидкому розшифруванні шифртекстом можуть виступати також параметри b_i'.

Для вибраного вище відкритого тексту $RNS = (171318)$, модулів $p_1 = 47$, $p_2 = 59$, $p_3 = 71$ та коефіцієнтів $k_1 = 19$, $k_2 = 23$, $k_3 = 31$ з урахуванням даних табл. 1 згідно з (3) будемо мати: $N' = (4189 \cdot 17 \cdot 19 + 3337 \cdot 13 \cdot 23 + 2773 \cdot 18 \cdot$ $\cdot 31) \bmod 196883 = 157367$. Тоді за формулами (4), (5) отримуємо такі результати: $b_1' = 11$, $b_2' = 14$, $b_3' = 31$; $b_1 = (11 \cdot 8 \cdot 5) \bmod 47 = 17$; $b_2 = (14 \cdot 34 \cdot 18) \bmod 59 = 13$; $b_3 = (31 \cdot 18 \cdot 55) \bmod 71 = 18$. Отримані значення b_i відповідають відкритому тексту $RNS = (171318)$. Згідно з домовленостями між абонентами шифртекстом може виступати або параметр $N' = 157367$, або конкатенація значень b_i': 111431.

Для $k = 1$ згідно з (8), другою формулою (4) та першою формулою (9) маємо: $N' = (4189 \cdot 17 + 3337 \cdot 13 + 2773 \cdot 18) \bmod 196883 = 164508$; $b_1' = 8$, $b_2' = 16$, $b_3' = 1$; $b_1 = (8 \cdot 8) \bmod 47 = 17$; $b_2 = (16 \cdot 34) \bmod 59 = 13$; $b_3 = (1 \cdot 18) \bmod 71 = 18$.

Результат для знакозмінної суми у (3) ($k_1 = -19, k_2 = -23, k_3 = 31$) буде таким:

$$N' = (-4189 \cdot 17 \cdot 19 - 3337 \cdot 13 \cdot 23 + 2773 \cdot 18 \cdot 31) \bmod 196883 = 180939, \; b_1' = 36,$$

$$b_2' = 45, \; b_3' = 31, \; q_1 = -40, \; q_2 = -22, \; q_3 = 67, \; b_1 = (-36 \cdot 40) \bmod 47 = 17;$$

$$b_2 = (-45 \cdot 22) \bmod 59 = 13; \; b_3 = (31 \cdot 67) \bmod 71 = 18.$$

Іншим підходом для зменшення часової складності під час симетричного шифрування в СЗК може бути використання різних форм СЗК, зокрема її ДФ та МДФ. У цих формах модулі підібрано в такий спосіб, що відповідно виконуються

співвідношення $m_i = M_i^{-1} \bmod p_i = 1$ та $m_i = M_i^{-1} \bmod p_i = \pm 1$. Зокрема, умовам МДФ СЗК для трьох модулів відповідають такі залежності між модулями: $p_{2,3} = 2 \cdot p_1 \pm 1$. Шифрування здійснюється за формулою (3), а розшифрування — за формулами (4)–(6), з урахуванням того, що m_i може набувати значень 1 або –1.

У табл. 2 наведено приклад використання запропонованої криптосистеми на основі МДФ СЗК для трьох модулів ($s = 3$), відкритого тексту $RNS = (171318)$, модулів $p_1 = 37$, $p_2 = 73$, $p_3 = 75$ та коефіцієнтів $k_1 = 19$, $k_2 = 23$, $k_3 = 31$.

Залишки b_i шукають згідно з формулою (1), тоді з виразу (3) отримують шифртекст:

$$N' = (5475 \cdot 8 \cdot 19 + 2775 \cdot 60 \cdot 23 + 2701 \cdot 18 \cdot 31) \bmod 202575 = 91608.$$

Після пошуку відповідних параметрів b_i', $k_i^{-1} \bmod p_i$ та q_i розшифрування здійснюється згідно з виразом (6):

$$N = (-5475 \cdot ((-33 \cdot 2) \bmod 37) + 2775 \cdot ((66 \cdot 54) \bmod 73) +$$

$$+2701 \cdot ((33 \cdot 46) \bmod 71)) \bmod 202575 = 171318.$$

Для $k_i = 1$ та заданих у табл. 2 вхідних параметрів за формулами (8), (9) можна отримати $N' = (5475 \cdot 8 + 2775 \cdot 60 + 2701 \cdot 18) \bmod 202575 = 56343$; $b_1' = 29$, $b_2' = 60$, $b_3' = 18$; $N = (-5475 \cdot (-29) + 2775 \cdot 60 + 2701 \cdot 18) \bmod 202575 = 171318$.

Слід зазначити, що в цьому випадку $b_1' = p_1 - b_1$, $b_{2,3}' = b_{2,3}$, тому як шифртекст доцільно вибрати значення $N' = 56343$. До того ж, для $k_i = m_i$ ($k_1 = m_1 = -1$; $k_{2,3} = m_{2,3} = 1$) відкритий та зашифрований тексти будуть однаковими, тобто шифрування не здійснюватиметься.

У разі вибору деяких k_i від'ємними (нехай, як і в попередніх випадках, $k_1 = -19$, $k_2 = -23$, $k_3 = 31$) та для заданих у табл. 2 вхідних параметрів згідно з (3), (6) результати є такими:

$$N' = (5475 \cdot 8 \cdot (-19) + 2775 \cdot 60 \cdot (-23) + 2701 \cdot 18 \cdot 31) \bmod 202575 = 86658, \; b_1' = 4,$$

$$b_2' = 7, \; b_3' = 33, \; q_1 = 2, \; q_2 = -54, \; q_3 = 46,$$

$$N = (-5475 \cdot ((2 \cdot 4) \bmod 37) + 2775 \cdot ((-54 \cdot 7) \bmod 73) +$$

$$+2701 \cdot ((46 \cdot 33) \bmod 75 \bmod 202575 = 171318.$$

У тому випадку, коли блоки відкритого тексту виступають залишками від ділення на вибрані модулі, для вхідних даних табл. 2 згідно з виразами (3)–(5) маємо:

$$N' = (5475 \cdot 17 \cdot 19 + 2775 \cdot 13 \cdot 23 + 2701 \cdot 18 \cdot 31) \bmod 202575 = 53808; \; b_1' = 10, \; b_2' = 7,$$

$$b_3' = 33; \; b_1 = (11 \cdot 8 \cdot 5) \bmod 47 = 17; \; b_2 = (14 \cdot 34 \cdot 18) \bmod 59 = 13;$$

$$b_3 = (31 \cdot 18 \cdot 55) \bmod 71 = 18.$$

Шифртекстом може виступати або параметр $N' = 53808$, або конкатенація значень b_i': 100733.

Таблиця 2. Приклад використання запропонованої симетричної криптосистеми на основі МДФ СЗК

i	N	p_i	P	M_i	m_i	b_i	k_i	N'	b_i'	$k_i^{-1} \bmod p_i$	q_i
1	171318	37	202575	5475	–1	8	19	91608	33	2	-2
2		73		2775	1	60	23		66	54	54
3		75		2701	1	18	31		33	46	46

Для $k_i = 1$ обчислення спростяться:

$$N' = (5475 \cdot 17 + 2775 \cdot 13 + 2701 \cdot 18) \bmod 202575 = 177768;\ b'_1 = 20,\ b'_2 = 13,\ b'_3 = 18.$$

У цьому випадку $b'_1 = p_1 - b_1$, $b'_{2,3} = b_{2,3}$, тому як шифртекст доцільно вибрати значення $N' = 177768$. Крім того, для $k_i = m_i$ $(k_1 = m_1 = -1; k_{2,3} = m_{2,3} = 1)$ шифртекст $N' = (-5475 \cdot 17 + 2775 \cdot 13 + 2701 \cdot 18) \bmod 202575 = 194193$; при цьому залишки b'_i та b_i будуть однаковими.

Якщо, аналогічно до розглянутого вище випадку, деякі значення k_i вибрати від'ємними (до прикладу $k_1 = -19$, $k_2 = -23$, $k_3 = 31$), то з урахуванням заданих у табл. 2 вхідних параметрів отримані результати є такими: $N' = (5475 \cdot 17 \cdot (-19) + 2775 \cdot 13 \cdot (-23) + 2701 \cdot 18 \cdot 31) \bmod 202575 = 124458$, $b'_1 = 27$, $b'_2 = 66$, $b'_3 = 33$, $q_1 = 2$, $q_2 = -54$, $q_3 = 46$, $b_1 = (27 \cdot 2) \bmod 37 = 17$; $b_2 = (-66 \cdot 54) \bmod 73 = 13$; $b_3 = (33 \cdot 46) \bmod 75 = 18$. Шифртекстом може виступати або параметр $N' = 124458$, або конкатенація значень b'_i: 276633.

ОЦІНКА КРИПТОСТІЙКОСТІ СИМЕТРИЧНОГО АЛГОРИТМУ ШИФРУВАННЯ В СИСТЕМІ ЗАЛИШКОВИХ КЛАСІВ

Криптостійкість запропонованого симетричного методу шифрування на основі СЗК, описаного виразом (3), ґрунтується на пошуку всіх можливих варіантів параметрів k_i та модулів криптоперетворень p_i. Завдяки використанню функції Ейлера $\varphi(p_i)$ можна обчислити кількість взаємно простих чисел із заданим p_i, причому значення буде максимальним у випадку $\varphi_{\max}(p_{i\max}^{(n)}) = p_{i\max}^{(n)} - 1$, тобто $p_{i\max}^{(n)}$ — максимальне просте число розрядності n [25, 26]. Для фіксованого максимального $p_1 = p_{i\max}^{(n)}$ кількість варіантів вибору p_2 становитиме $\varphi(p_1) = p_{i\max}^{(n)} - 1 = p_1 - 1$, для p_3 — відповідно $\varphi(p_2)$,..., для p_s — $\varphi(p_{s-1})$. Отже, кількість способів, у які можна отримати набори модулів криптоперетворення у запропонованому методі, є такою: $\prod_{i=1}^{s-1} \varphi(p_i)$. Криптостійкість буде найбільшою у тому випадку, коли $\varphi(p_i)$ набувають максимальних значень, тобто коли $p_i^{(n)}$ — найбільші прості числа певної розрядності.

У запропонованому підході до шифрування, крім модулів криптоперетворень, використовуються ще параметри k_i, вибір яких теж можна здійснити $\prod_{i=1}^{s-1} \varphi(p_i)$ способами. Отже, загальна складність математичної атаки з урахуванням часової складності КТЗ буде обчислюватися за таким співвідношенням:

$$O\left(s \cdot n^2 \cdot \left(\prod_{i=1}^{s-1} \varphi(p_i) \right)^2 \right).$$

Як видно з оцінки часової складності, збільшення криптостійкості можна досягнути за рахунок збільшення кількості модулів p_i та відповідно параметрів k_i (ключів), їхньої розрядності, а також вибору таких модулів, для яких значення $\varphi(p_i)$ буде максимальним.

Якщо вважати, що всі модулі мають розрядність n, то загальну стійкість можна оцінити виразом $O(\log_2(s-1) \cdot s \cdot n^6)$. Графік залежності стійкості від розрядності n та кількості модулів s представлено на рис. 1. З нього видно, що із збільшенням цих параметрів криптостійкість алгоритму різко зростає.

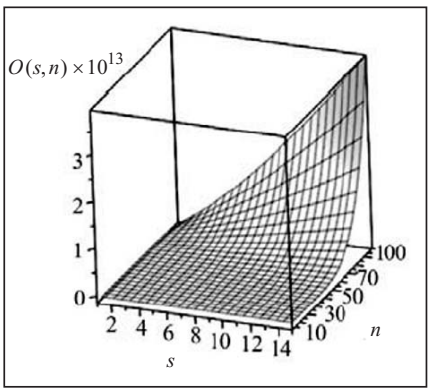

Рис. 1. Залежність криптостійкості алгоритму від розрядності модулів та їхньої кількості

Числові розрахунки показують, що для досягнення такої самої криптостійкості, як у симетричного криптоалгоритму AES [27] з довжиною ключа 256 біт, розрядність модулів має становити приблизно 45 біт.

ВИСНОВКИ

Розроблено високопродуктивні симетричні криптоалгоритми на основі СЗК та її МДФ, які на відміну від класичних надають змогу забезпечити необхідний рівень захисту даних за рахунок збільшення розмірності вхідних параметрів (розміру повідомлення, розрядності та кількості модулів). Особливості цього підходу полягають у тому, що під час відновлення числа за його залишками з використанням КТЗ множення здійснюється не на обернені елементи за модулем, а на довільно вибрані коефіцієнти (ключі) симетричного шифрування в СЗК, що дає можливість підвищити криптостійкість алгоритму. Отримано аналітичні вирази оцінки стійкості, які свідчать про те, що збільшення криптостійкості можна досягнути шляхом збільшення розрядності, кількості модулів та ключів, а також вибору таких модулів, для яких значення функції Ейлера буде максимальним. Представлено графічну залежність криптостійкості від розрядності та кількості модулів. Встановлено, що для досягнення такої самої криптостійкості, як у симетричного криптоалгоритму AES-256, розрядність модулів повинна становити приблизно 45 біт.

СПИСОК ЛІТЕРАТУРИ

1. Shevchuk R., Pastukh Ya. Improve the security of social media accounts. *Proc. 9th International Conference on Advanced Computer Information Technologies* (*ACIT-2019*). (5–7 June 2019, Ceske Budejovice, Czech Republic). Ceske Budejovice, 2019. P. 439–442. https://doi.org/10.1109/ACITT.2019.8779963.
2. Andrijchuk V.A., Kuritnyk I.P., Kasyanchuk M.M., Karpinski M.P. Modern algorithms and methods of the person biometric identification. *Proc. Third IEEE International Workshop on Intelligent Data Acquisition and Advanced Computing Systems*: *Technology and Applications (IDAACS-2005).* (5–7 Sept. 2005, Sofia, Bulgaria. Sofia, 2005. P. 403–406. https://doi.org/10.1109/IDAACS.2005.283012.
3. Sousa L., Antao S., Martins P. Combining residue arithmetic to design efficient cryptographic circuits and systems. *IEEE Circuits and Systems Magazine*. 2016. Vol. 15, Iss. 4. P. 6–32. https://doi.org/10.1109/MCAS.2016.2614714.
4. Elminaam D.S.A., Kader H.M.A., Hadhoud M.M. Performance evaluation of symmetric encryption algorithms. *International Journal of Computer Science and Network Security*. 2008. Vol. 8, N 12. P. 280–286.
5. Al-Shabi M.A. A survey on symmetric and asymmetric cryptography algorithms in information security. *International Journal of Scientific and Research Publications*. 2019. Vol. 9, Iss. 3. P. 576–589. https://doi.org/10.29322/IJSRP.9.03.2019.p8779.
6. Rusia M.K., Rusia M. A literature survey on efficiency and security of symmetric cryptography. *International Journal of Computer Science and Network*. 2017. Vol. 6, Iss. 3. P. 425–429.
7. Goel R., Sinha R.R., Rishi O.P. Novel data encryption algorithm. *International Journal of Computer Science Issues*. 2011. Vol. 8, Iss. 4, No 2. P. 561–565.
8. Губка С.А., Губка А.С., Носова Н.Ю. Модернизация симметричного алгоритма шифрования. *Радіоелектронні і комп'ютерні системи*. 2011. № 1. С. 61–65.

9. Pikh V., Kimak V., Krulikovskyi B. Synthesis of high-performance components of spectral analyzers and special processors for data encryption in Rademacher-Krestenson's theoretical-numerical basis. *Proc. XIII-th International Conference "The Experience of Designing and Application of CAD Systems in Microelectronics* (*CADSM-2015*)". (23–25 February, 2015, Polyana-Svalyava (Zakarpattya), Ukraine), Polyana-Svalyava, 2015. P. 182–184.
10. Ananda Mohan P.V. Residue Number Systems: Theory and Applications. Basel: Birkhäuser, 2016. 351 p.
11. Zadiraka V., Nykolaichuk Ya., Franko Yu. Computer technologies in information security. Ternopil: "Kart-blansh", 2015. 387 p.
12. Djath L., Bigou K., Tisserand A. Hierarchical approach in RNS base extension for asymmetric cryptography. *Proc. IEEE 26th Symposium on Computer Arithmetic* (*ARITH*). (10–12 June 2019, Kyoto, Japan). Kyoto, 2019. P. 46–53. https://doi.org/10.1109/ARITH.2019.00016.
13. Fadulilahi I.R., Bankas E.K., Ansuura J.B.A.K. Efficient algorithm for RNS implementation of RSA. *International Journal of Computer Applications*. 2015. Vol. 127, N 5. P. 14–19. https://doi.org/10.5120/ijca2015906381.
14. 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. X-th International Conference "Modern Problems of Radio Engineering*, *Telecommunications and Computer Science (TCSET-2010)".* (23–27 February 2010, L'viv–Slavske, Ukraine. L'viv–Slavske, 2010. P. 241.
15. Saldamli G., Koc K. Spectral modular exponentiation. *Proc*. *18th IEEE Symposium on Computer Arithmetic* (*ARITH '07*). (25–27 June 2007, Montepellier, France). Montepellier, 2007. P. 123–130. https://doi.org/10.1109/ARITH.2007.34.
16. Yakymenko I., Kasianchuk M., Ivasiev S., Melnyk A., Nykolaichuk Ya. Realization of RSA cryptographic algorithm based on vector-module method of modular exponention. *Proc*. *14th International Conference on Advanced Trends in Radioelecrtronics*, *Telecommunications and Computer Engineering (TCSET-2018)*. (20–-24 Feb. 2018, L'viv–Slavske, Ukraine). Slavske, 2018. P. 550–554. https://doi.org/10.1109/TCSET.2018.8336262.
17. Yatskiv V., Sachenko A., Yatskiv N., Bykovyy P., Segin A. Compression and transfer of images in wireless sensor networks using the transformation of residue number system. *Proc. IEEE 10th International Conference on Intelligent Data Acquisition and Advanced Computing Systems*: *Technology and Applications (IDAACS-2019)*. (18–21 Sept. 2019, Metz, France). Metz, 2019. P. 1111–1114. https://doi.org/10.1109/IDAACS.2019.8924372.
18. Krasnobayev V.A., Yanko A.S., Koshman S.A. A method for arithmetic comparison of data represented in a residue number system. *Cybernetics and Systems Analysis*. 2016. Vol. 52, N 1. P. 145–150. https://doi.org/10.1007/s10559-016-9809-2.
19. Kasianchuk M., Yakymenko I., Pazdriy I., Zastavnyy O. Algorithms of findings of perfect shape modules of remaining classes system. *Proc. XIII International Conference "The Experience of Designing and Application of CAD Systems in Microelectronics* (*CADSM-2015*)". (24–27 Feb. 2015, Lviv, Ukraine). Lviv, 2015. P.168–171. https://doi.org/10.1109/CADSM.2015.7230866.
20. 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/10.1615/JAutomatInfScien.v48.i8.60.
21. Shoup V. Computational Introduction to Number Theory and Algebra. Cambridge University Press, 2005. 600 p. https://doi.org/10.1017/CBO9781139165464.
22. 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. 10th IEEE International Conference on Intelligent Data Acquisition and Advanced Computing Systems*: *Technology and Applications* (*IDAACS-2019*). (18–21 Sept. 2019, Metz, France). Metz, 2019. P. 13–17. https://doi.org/10.1109/IDAACS.2019.8924395.
23. Zhengbing Hu., Dychka I., Onai M., Bartkoviak A. The analysis and investigation of multiplicative inverse searching methods in the ring of integers modulo m. *International Journal of Intelligent Systems and Applications*. Vol. 8, N 11. 2016. P. 9–18. https://doi.org/ 10.5815/ijisa.2016.11.02.

24. 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. 2017 IEEE 9th International Conference on Intelligent Data Acquisition and Advanced Computing Systems*: *Technology and Applications (IDAACS-2017)*. (21–23 Sept. 2017, Bucharest, Romania). Bucharest, 2017. P. 82–85. https://doi.org/10.1109/IDAACS.2017.8095054.

25. Dasgupta S., Papadimitriou C., Vazirani U. Algorithms. McGraw-Hill Science/Engineering/Math, 2006. 336 p.

26. Jeffrey H., Jill P., Joseph H. An Introduction to Mathematical Cryptography. Berlin: Springer, 2008. 540 p.

27. Bogdanov A., Khovratovich D., Rechberger C. Biclique cryptanalysis of the full AES. *Proc. International Conference on the Theory and Application of Cryptology and Information Security "Advances in Cryptology – ASIACRYPT 2011*". (4–8 December 2011, Seoul, Korea), Seoul, 2011. *LNCS*. Vol. 7073. P. 344–371. https://doi.org/10.1007/978-3-642-25385-0_19.

Надійшла до редакції 29.05.2020

М.Н. Касянчук, И.З. Якименко, Я.Н. Николайчук
СИММЕТРИЧНЫЕ КРИПТОАЛГОРИТМЫ В СИСТЕМЕ ОСТАТОЧНЫХ КЛАССОВ

Аннотация. Представлены теоретические основы симметричного шифрования на основе системы остаточных классов. Особенности этого подхода заключаются в том, что при восстановлении десятичного числа по его остаткам с использованием китайской теоремы об остатках умножения осуществляются на произвольно выбранные коэффициенты (ключи). Установлено, что криптостойкость разработанных методов определяется количеством модулей и их разрядностью. Отмечено, что описанные методы позволяют практически неограниченно увеличивать блок открытого текста для шифрования, что устраняет необходимость использования различных режимов шифрования.

Ключевые слова: система остаточных классов, криптоалгоритм, симметричная криптосистема, шифртекст, криптоанализ, устойчивость.

M.M. Kasianchuk, I.Z. Yakymenko, Ya.M. Nykolaychuk
SYMMETRIC CRYPTOALGORITHMS IN THE RESIDUE NUMBER SYSTEM

Abstract. This paper presents the theoretical backgrounds of symmetric encryption based on a residue number system. The peculiarities of this approach include that when restoring a decimal number to its residuals appears using the Chinese remainder theorem, multiplication occurs by arbitrarily chosen coefficients (keys). It is established that cryptostability of the developed methods is determined by the number of modules and their bit size. In addition, the described methods allow almost indefinitely increase the block of plain text for encryption, which eliminates the need to use different encryption modes.

Keywords: residue number system, cryptoalgorithm, symmetric cryptosystem, ciphertext, cryptanalysis, stabilitlity.

Касянчук Михайло Миколайович,
доктор техн. наук, доцент, доцент кафедри Західноукраїнського національного університету, Тернопіль, e-mail: kasyanchuk@ukr.net.

Якименко Ігор Зіновійович,
кандидат техн. наук, доцент, доцент кафедри Західноукраїнського національного університету, Тернопіль, e-mail: jiz@wunu.edu.ua.

Николайчук Ярослав Миколайович,
доктор техн. наук, професор, завідувач кафедри Західноукраїнського національного університету, Тернопіль, e-mail: kmm@wunu.edu.ua.