картах с собственной операционной системой «УкрКОС» («УкрКОС» – единственная в мире ОС, одновременно соответствующая и международным, и Украинским стандартам). Все криптографические преобразования, включая генерацию ключевой информации, формирование и проверку электронной цифровой подписи, осуществляются внутри самого носителя.

Ключ безопасности USB

Альтернативой использования смарт-карт являются секретные ключи USB.

В настоящее время на рынке представлено большое количество ключей USB, но к сожалению, большинство из них строятся на обычных отдельных элементах микроэлектронной промышленности: микроконтроллер общего применения с внутренней или внешней памятью, что не обеспечивает гарантированный уровень безопасности хранимой в нем информации. USB-ключ считается надежным только в том случае, если он построен на смарт-чипе, что позволяет в полной мере использовать механизмы защиты смарт-карт технологии.

Рекомендации по выбору типа НКИ

При принятии решении о типе используемого НКИ надо учитывать тот фактор, что НКИ находится в постоянном обращении и использовании, поэтому может быть утерян, испорчен или сломан. С этой точки зрения экономически выгоднее разделение дорогостоящих электронных ключей на дешевые смарт-карты и стационарные устройства карт-ридеры. Также, например, бесконтактная смарт-карта очень удобна при одновременном ее использовании в системах контроля доступа. Однако при мобильном применении НКИ, например, использование NoteBook в командировках или при on-line операциях не со своего стационарного компьютера, более удобным в эксплуатации является ключ безопасности.

Заключение

В заключении хочется еще раз отметить, что качество, надежность и безопасность информационного обмена – это те критерии, которые должны лежать в основе всех информационно-телекоммуникационных систем. Поэтому при создании на предприятии комплексных систем информационной безопасности необходимо отталкиваться именно от этих принципов.

Обращаем Ваше внимание, что данная работа не ставит перед собой цель однозначно характеризовать надежность каждого продукта. В зависимости от требований к уровням безопасности информационной среды Вашей организации каждое решение может проявить как свои преимущества, так и недостатки, и порой поможет избежать лишних затрат при построении PKI.

Искренне надеемся, что проведенная нами работа позволит Вам максимально учесть все нюансы при построении PKI-инфраструктуры и выбрать тот продукт, который обеспечит Вам твердую почву под ногами в зыбком море информации.

УДК 681.3

НЕСИМЕТРИЧНЕ КОДУВАННЯ З ВИКОРИСТАННЯМ ЛИШКОВИХ КЛАСІВ

Вячеслав Василенко
Національний авіаційний університет

Анотація: **Пропонується використання несиметричного блокового криптографічного перетворення для задач забезпечення конфіденційності інформаційних об'єктів автоматизованих систем з використанням системи числення в лишкових класах.**
Summary: **The use of asymmetrical sectional cryptographic transformation for the tasks of providing of confidentiality of information's holding object of the automated systems with the use of scale of notation in remaining classes is offered.**
Ключові слова: Криптографічні перетворення, лишкові класи, несиметричні ключі, системи числення.

І Вступ

Відомо, що сенсом криптографічних перетворень є така зміна початкового повідомлення (тесту,

частини мовної конструкції тощо), при якій це повідомлення стає незрозумілим для тих, хто не володіє ключем зворотного перетворення, а пошук зворотного перетворення з тих чи інших причин є неприйнятним (наприклад, із-за занадто великих витрат часу – великої криптографічної стійкості). Існує багато способів таких перетворень із різною криптографічною стійкістю. Найвідомішими із таких перетворень є переклад на іншу мову (ключі перетворення – словники мов та діалектів); кодування в межах однієї з мов (наприклад, із застосуванням підміни понять, різних символів (алфавітів) для запису звуків, слів, речень тощо, коли ключами перетворення можуть бути, наприклад, кодувальні таблиці); перемішування символів з їх одночасною зміною, наприклад, із застосуванням матричних кодових перетворень та т. ін. Можливим є також комбінація із різних способів перетворення, наприклад, перехід на іншу мову (інший алфавіт) із застосуванням матричних кодових перетворень [1, 2].

Одним із найсучасніших напрямків у задачах асиметричного шифрування є шифрування на еліптичних кривих — наборах точок, обумовлених двома координатами, які є рішеннями певних рівнянь [3]. Операції в цьому рівнянні виконуються в деякому кінцевому полі, наприклад, полі лишків, по якому-небудь модулю p. Для цих точок визначається операція "додавання", що задовольняє властивостям комутативності й асоціативності. В таких нечислових конструкціях вдається визначити задачу логарифмування так, що знання секрету дозволяє реалізувати швидкий алгоритм. Зокрема, цей підхід використовується в прийнятому недавно російському стандарті асиметричного шифрування.

В еліптичних кривих виразилася загальна тенденція розвитку криптографічних алгоритмів з відкритим ключем: відмова від роботи із числовими об'єктами задач і перехід до більш складних й менш вивчених математичних конструкцій, благо для них сформульовано досить багато складних задач. Втім, нечислові конструкції вивчені слабко, а, отже, немає гарантії того, що через якийсь час не з'явиться ефективний алгоритм, що зробить такий шифр ненадійним. Тому таким важливим є розвиток власне теорії складності, що, можливо, дозволила б одержати теоретичні результати про можливості використання тих або інших задач для створення асиметричних шифрів.

Крім еліптичних кривих є ще кілька перспективних нечислових конструкцій, які можна використати для криптографічних цілей. Одна з них — коди, що виправляють помилки [3]. Придумані вони були для цілей зменшення втрат інформації при її передачі або зберіганні, але алгоритми відновлення виявилися настільки складними, що їх можна використати й для криптографічних цілей. Суть технології стійких до помилок кодів полягає в пошуку найближчого кодового слова в багатомірному просторі базових векторів. Виявляється, ця задача має експонентну складність, оскільки для пошуку найближчого кодового слова потрібно обчислити відстані до всіх слів. У даній статті здійснена спроба показати можливість використання підходів, відомих із галузі теорії лишкових класів, до задач побудови алгоритмів криптографічного перетворення з несиметричними ключами із застосуванням елементів нечислових конструкцій типу цифрових кіл, що дотикаються.

II Властивості числових кілець

Прикладом застосування теорії кодів, що виправляють помилки, для криптографічних перетворень є завадостійкі криптографічні перетворення із симетричними ключами і переводом з однієї системи числення (мови запису числових послідовностей) в іншу. В [2] розглянуто варіант криптографічного матричного перетворення шляхом переходу з позиційної системи числення (ПСЧ) у систему лишкових класів (СЛК), коли ключами перетворення є набір основ чи інші константи системи числення.

Зрозуміло, що можливим має бути й варіант криптографічного перетворення шляхом переводу зі СЛК у позиційну. З цією метою достатньо розбити вихідний (призначений для шифрування) код позиційної системи числення, наприклад, двійкової, на певні групи розрядів і вважати кожну із таких груп двійковим відображенням символу деякої системи лишкових класів. У зв'язку з тим, що таке представлення є несправжнім, умовним, будемо називати таку СЛК системою умовних лишків (СУЛ).

Звернемо увагу на те, що при обмеженому діапазоні числення (обмеженій розрядній сітці), незалежно від системи числення, що розглядається, існує максимальне число, яке можна записати в цій системі. Таке число (див. рис. 1) дорівнює ($P - 1$) незалежно від системи числення (наприклад, у ПСЧ $P = q^n$, де q – основа системи числення; в СЛК $P = \prod_{i=1}^{n} p_i$, p_i – i-та основа СЛК, n – кількість символів (розрядів) в представленні чисел в даній системі числення). Величина P досить часто має назву "робочого" чи "правильного" діапазону представлення, а розряди, які утворюють цей "робочий" діапазон – розрядами робочого діапазону, чи просто робочими.

Рисунок 1 – Представлення системи числення у вигляді числової вісі

При спробі збільшувати числа в таких системах числення наступними знову стають числа 0, 1, 2, і т. д. Тобто будь-яка система числення при обмеженій розрядній сітці графічно може бути представлена не числовою віссю, як це робиться найчастіше (див. рис. 1, 2), а числовим кільцем (в термінах кінцевих полів), як це наведено на рис. 3, з початком відліку в точці 0 (P).

Звернемо увагу на те, що числові кільця, залежно від величини діапазону представлення P, тобто залежно від величини основ та їх кількості (величини розрядної сітки) мають різний розмір. При цьому сукупність числових кіл усіх систем числення для будь-яких значень основ системи числення, їх кількості чи довжин розрядних сіток має одну спільну точку дотику (рис. 3) якраз у точці початку відліку 0 (P).

В разі відсутності надлишковості при будь-якій модифікації (викривленні) інформації, яка відображена в робочих розрядах, модифіковане число завжди буде розташованим у межах усе того ж робочого діапазону. Тому для вирішення питань із виявлення та виправлення викривлень (модифікацій природного чи штучного характеру), в представлення чисел потрібно ввести певну надлишковість. Ця надлишковість вводиться за рахунок того чи іншого розширення розрядної сітки шляхом введення додаткових груп розрядів (чи основ).

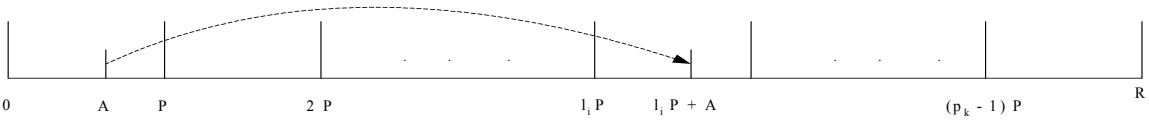

Рисунок 2 – Перенос викривленого числа на числовій вісі із робочого діапазону у контрольний

Між інформаційним змістом робочих та надлишкових розрядів установлюється певна відповідність. При цьому правила (алгоритми) вибору кількості і порядку розташування надлишкових розрядів та встановлення відповідності між інформацією робочих та надлишкових розрядів складають сутність кодування, яке за традицією прийнято називати завадостійким, а власне сукупність визначених таким чином змістовностей інформаційних та надлишкових розрядів має назву завадостійкого коду.

Примітка. Для виконання арифметичних операцій із від'ємними числами діапазон представлення (0, (P – 1)) в усіх системах числення певним чином розподіляється між позитивними та від'ємними числами. Цей факт на зміст того, що розглядається надалі, не впливає, тому він в межах даної статті ігнорується.

Розглянемо випадок щодо представлення початкового числа A (слова для шифрування) в деяких системах, числення (незалежно від того, ПСЧ, СЛК чи СУЛ). Нехай для визначеності це число A буде наданим у початковій системі числення (на рис. 2, 3 це позначено точкою A в початковій СУЛ (ПСЧ)) у вигляді:

$$A = \alpha_1, \alpha_2, \alpha_3, ..., \alpha_n,$$

де α_i – i-та складова початкового числа A і, одночасно, – умовний "лишок" від ділення A на p_i. Як відомо, в цій системі числення однозначне представлення чисел є можливим при умові $A \le P$.

Нехай збільшення кількості основ у СУЛ здійснюється за рахунок введення додаткової основи p_k. При цьому діапазон представлення чисел розширюється до $R = P \cdot p_k$, тобто складається із p_k піддіапазонів P. Для представлення числа A в розширеній СУЛ слід якимось чином задати лишок A по цій новій основі – величину α_k. Із теорії лишкових класів відомо, що в разі визначення величини α_k як

$$\alpha_k = \{A\}_{p_k},$$

число

$$A = \alpha_1, \alpha_2, \alpha_3, ..., \alpha_n, \alpha_к$$

залишається в першому ("робочому") діапазоні (0, P] розширеного діапазону (0, R), якщо ж $\alpha_к \neq (A)_{p_k}$, а дорівнює, наприклад, $\alpha_к = x$, число A виходить за межі робочого діапазону і попадає в інший діапазон, наприклад, в діапазон $(l_i \cdot P, (l_i + 1) \cdot P]$ (див. рис. 2, 3).

Тобто, за рахунок додавання замість "правильного" лишку по основі $p_к$ іншого (наприклад,

випадкового чи помилкового числа $\alpha_k = x$ по цій же основі) здійснюється "викид" вихідного числа (точки A_1 чи A_2 на рис. 2) із робочого діапазону [0, P) у випадковий діапазон, наприклад, в діапазон ($l_i \cdot P$, (l_i + 1)$\cdot P$) в межах діапазону [0, R). Таке переміщення точки A числовими кільцями можна вважати випадковим "блуканням". При цьому в СУЛ таке число записується у вигляді

$$A^{/} = \alpha_1, \alpha_2, \alpha_3, ..., \alpha_n, x.$$

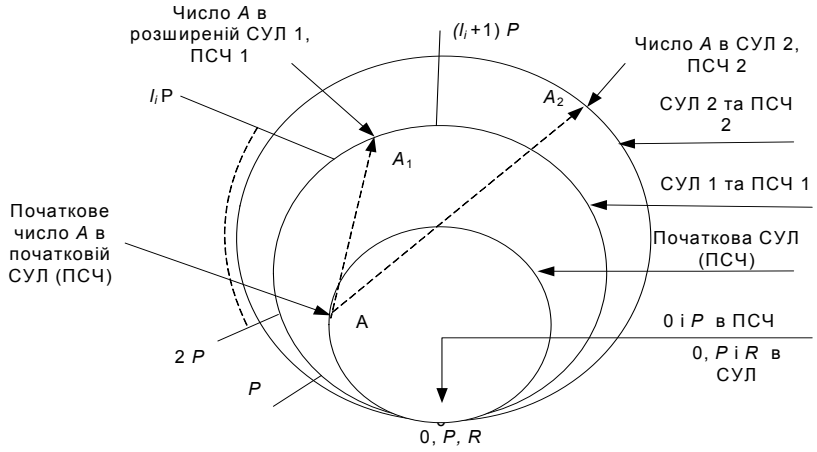

Рисунок 3 – "Блукання" точки, що відображає число *A*, числовими кільцями, що дотикаються в точках A = 0 (*P, R*)

До речі, такий "викид" буде спостерігатися і при модифікації лишку по будь-якій іншій основі. Визначити номер l_i, в який потрапляє число A при викривленні лишку по будь-якій основі, наприклад, по основі p_i, можна наступним чином. Викривлення по одній з основ у СУЛ має вигляд:

$$(\alpha_1, \alpha_2, \alpha_3, ..., \alpha_{i-1}, x, ..., \alpha_k) - (\alpha_1, \alpha_2, \alpha_3, ..., \alpha_{i-1}, \alpha_i, ..., \alpha_k) = 0, 0, ..., (x - \alpha_i)_{p_i}, ..., 0.$$

Числа такого виду, які мають в СУЛ усі лишки окрім одного (в даному випадку – p_i) такими, що дорівнюють нулю, є числами, кратними усім основам системи числення, за виключенням основи p_i. Тобто, є числами виду

$$l_i \cdot R_i = R / p_i$$

тоді:

$$(x - \alpha_i)_{p_i} = (l_i \cdot R_i)_{p_i},$$

звідкіля

$$l_i = \{(x - \alpha_i) / R_i\}_{p_i} = \{(x - A_{p_i}) / R_i\}_{p_i}.$$

Тобто здійснивши "випадкове", але відоме на боці передачі викривлення лишку по певній основі, досить просто знайти номер того інтервалу, куди попаде в своєму "блуканні" викривлене число.

На рис. 2, 3 видно що:

$$\Delta A = A^{/} - A = (l_i \cdot R_i)_{p_i}.$$

Останнє, у свою чергу, при визначених l_i та p_i дозволяє досить просто визначити величину "викривлення" $\Delta\alpha_i = (\Delta A)_{p_i}$:

$$\Delta\alpha_i = (\Delta A)_{p_i} = (x - \alpha_i)_{p_i} = (l_i \cdot R_i)_{p_i}$$

і здійснити, при потребі, корекцію цього "викривлення"

$$\alpha_i = (x - \Delta\alpha_i)_{p_i}.$$

Розглянута властивість точок, що "блукають" кільцями систем числення, надає можливість побудови криптосистем із несиметричними (відкритими) ключами.

III Варіант несиметричного криптоалгоритму на базі СУЛ (шифрують усі, розшифровує один)

Вихідне слово (для шифрування) А розглядається як число в СУЛ, тобто як послідовність із n символів α_i (i = 1, 2, ..., n).

Закриті ключі: сукупність p_i, які створюють кільце для "блукання чисел", що шифруються, а також випадкова величина x. Зрозуміло, що при цьому закритими є і решта базових констант системи числення – B_i та R.

Відкриті ключі: сукупність модифікованих випадковою величиною x констант B_i та R така, що $B_i^{/} = (B_i + x)$, $R_i^{/} = (R - x)$.

Зауважимо, що знання відкритих ключів у наведеному вигляді не дає криптоаналітику змоги відтворити закриті ключі через спотвореність цих ключів випадковим числом x.

Шифрування. Процес шифрування включає наступні операції з переводу в модифіковану ПСЧ:

1. формування $C = \sum_{i=1}^{n} \alpha_i \cdot B_i^{/} = \sum_{i=1}^{n} \alpha_i \cdot (B_i + x) = \sum_{i=1}^{n} \alpha_i \cdot B_i + \mathrm{x} \sum_{i=1}^{n} \alpha_i$;

2. обчислення $D = R_i^{/} \cdot \sum_{i=1}^{n} \alpha_i = (R - x) \cdot \sum_{i=1}^{n} \alpha_i = \mathrm{R} \cdot \sum_{i=1}^{n} \alpha_i - \mathrm{x} \cdot \sum_{i=1}^{n} \alpha_i$;

3. додавання $H = C + D = \sum_{i=1}^{n} \alpha_i \cdot B_i + x \cdot \sum_{i=1}^{n} \alpha_i + R \cdot \sum_{i=1}^{n} \alpha_i - x \cdot \sum_{i=1}^{n} \alpha_i = \sum_{i=1}^{n} \alpha_i \cdot B_i + \mathrm{R} \cdot \sum_{i=1}^{n} \alpha_i$.

Отримане слово Н є зашифрованим повідомленням (модифікованим в ПСЧ) і надсилається адресату.

Звернемо увагу на те, що за рахунок цих операцій здійснюється модифікація вихідного числа (повідомлення) на випадкову (для відправників) величину $R \cdot \sum_{i=1}^{n} \alpha_i$, чим забезпечується розглянуте вище "блукання" цього числа числовими кільцями.

Приклад 1. Нехай шифруванню підлягає послідовність A = 100111; закритим ключем є сукупність основ СУЛ p_1 = 4, p_2 = 5, p_3 = 7, та випадкова величина x = 11. Для такого набору основ СУЛ базовими константами є B_1 = 105 (R_1 = 35, m_1 = 3), B_2 = 56 (R_2 = 28, m_2 = 2), B_3 = 120 (R_3 = 20, m_3 = 6), R = 140, тоді як закритий ключ слід використовувати ($B_1 + x$) = 116, ($B_2 + x$) = 67, ($B_3 + x$) = 131, ($R - x$) = 129. Будемо вважати вихідну послідовність A як таку, що представлена у вигляді $A = (\alpha_1, \alpha_2, \alpha_3)$, де α_1 = 10, α_2 = 01, α_3 = 11. При таких умовах процес **шифрування** є послідовністю операцій із формування

$$C = \sum_{i=1}^{n} \alpha_i \cdot (B_i + x) = 2 \cdot 116 + 1 \cdot 67 + 3 \cdot 131 = 692;$$

$$D = (R - x) \cdot \sum_{i=1}^{n} \alpha_i = 129 \cdot (2 + 1 + 3) = 774;$$

$$H = C + D = 1466_{10} = 10110111010_2.$$

Дешифрування.

Дешифрування здійснюється шляхом обчислення величин $\alpha_i = \{H\}_{p_i}$ (i = 1, 2, ..., n). При цьому, оскільки лишки величини $\{R \cdot \sum_{i=1}^{n} \alpha_i\}_{p_i}$ по усім основам дорівнюють нулю – $\{R \cdot \sum_{i=1}^{n} \alpha_i\}_{p_i} = 0$, а лишки величин $\{\sum_{i=1}^{n} \alpha_i \cdot B_i\}_{p_i}$ дорівнюють нулю по усім основам, окрім основи p_i, коли $\alpha_i = \{\alpha_i \cdot B_i\}_{p_i}$, то отримують шукане вихідне повідомлення у вигляді сукупності ($\alpha_1, \alpha_2, ..., \alpha_n$).

Приклад: для умов попереднього прикладу (H = 1466_{10} = 10110111010_2) на секретному ключі обчислимо значення: $c_1 = \{1466\}_4 = \alpha_1 = 2$; $c_2 = \{1466\}_5 = \alpha_2 = 1$; $c_3 = \{1466\}_7 = \alpha_3 = 3$.

Порівнюючи вихідне слово для шифрування і результати дешифрування, упевнюємося в правильності функціонування запропонованих алгоритмів шифрування і дешифрування на відкритих ключах.

IV Варіант несиметричного криптоалгоритму на базі СУЛ (шифрує один, розшифровують усі)

Перед безпосереднім розглядом наступного криптоалгоритму на базі СУЛ, упевнимося в правильності таких перетворень:

$$\{\alpha_i \cdot B_i\}_R = \{\alpha_i \cdot m_i \cdot R / p_i\}_R = \{\alpha_i \cdot m_i\}_{p_i} \cdot R / p_i ,$$

де: α_i – лишок в СЛК за основою p_i;

m_i – "вага" ортогонального базису, константа СЛК;

вираз $\{X\}_Y$ означає обчислення лишку від ділення X на Y.

Дійсно, добуток $\alpha_i \cdot m_i$ можна представити у вигляді

$$\alpha_i \cdot m_i = \{\alpha_i \cdot m_i\}_{p_i} + [\alpha_i \cdot m_i / p_i] \cdot p_i = \{\alpha_i \cdot m_i\}_{p_i} + k \cdot p_i ,$$

де позначка [X] означає обчислення цілої частини від X і тоді

$$\{\alpha_i \cdot B_i\}_R = \{\alpha_i \cdot m_i \cdot R / p_i\}_R = \{(\{\alpha_i \cdot m_i\}_{p_i} + k \cdot p_i) \cdot R / p_i\}_R =$$

$$= \{\{\alpha_i \cdot m_i\}_{p_i} \cdot R / p_i + k \cdot R\}_R = \{\{\alpha_i \cdot m_i\}_{p_i} \cdot R / p_i\}_R = \{\alpha_i \cdot m_i\}_{p_i} \cdot R / p_i .$$

У цій низці перетворень останнє ґрунтується на тому, що обчислена за модулем p_i величина добутку $\{\alpha_i \cdot m_i\}_{p_i}$ є меншою ніж модуль, внаслідок чого усе значення виразу є меншим за R, тобто не потребує подальших перетворень за цим модулем.

Таке перетворення в контексті майбутніх міркувань щодо використання як криптоалгоритму прямого та зворотного переводів ПСЧ ↔ СЛК є корисним, принаймні, з двох причин. Перша з них полягає в можливості "маскування", додаткового кодування результатів перетворення чисел (вихідних блоків для шифрування) в СЛК, тобто використання замість лишків α_i величин $\{\alpha_i \cdot m_i\}_{p_i}$. Друга, як уже показано вище, пов'язана із певним спрощенням алгоритму за рахунок зменшення кількості операцій обчислення остаточного результату за модулем R.

Після цих міркувань розглянемо **перший варіант** алгоритму такого перетворення.

Вихідне слово (для шифрування) А будемо розглядати як число в ПСЧ, тобто як послідовність із n символів α_i (i = 1, 2, ..., n).

Закриті ключі, які створюють "випадкове" кільце для "блукання" чисел, що шифруються – сукупність $p_i^{/} = p_j (i, j = 1, 2, ..., n)$, де p_j – величина, яка з метою підвищення криптографічної стійкості перетворення випадковим чином вибрана із сукупності основ p_i так, що $i \neq j$.

Відкриті ключі – сукупність констант $B_i^{/} = B_i /(m_i \cdot p_j) = R /(p_i \cdot p_j)$, $R = \prod_{i=1}^{n} p_i$, де $B_i = m_i \cdot R / p_i$ – ортогональний базис, константа СЛК.

Процес **шифрування** включає перевід числа А з ПСЧ в СЛК (отримання лишків по основам p_i) із подальшою модифікацією цих лишків так, що $\alpha_i^{/} = \{\alpha_i \cdot m_i\}_{p_i} \cdot p_i^{/}$. При цьому $A_ш = \alpha_1^{/}, \alpha_2^{/}, ..., \alpha_n^{/}$.

Звернемо увагу, що і в цьому випадку в зв'язку з тим, що всі лишки зашифрованого числа є випадковим чином викривленими, також забезпечується розглянуте вище "блукання" числа $A_ш$ числовими кільцями.

Дешифрування здійснюється шляхом використання відомого алгоритму переводу зашифрованого числа з СЛК у ПСЧ відносно модифікованих значень $\alpha_i^{/}$ та $B_i^{/}$:

$$A = \{\sum_{i=1}^{n} \alpha_i^{/} \cdot B_i^{/}\} \bmod R = \{\sum_{i=1}^{n} \{\alpha_i \cdot m_i\}_{p_i} \cdot p_j \cdot R /(p_i \cdot p_j)\} \bmod R =$$

$$= \{\sum_{i=1}^{n} \{\alpha_i \cdot m_i\}_{p_i} \cdot R / p_i)\} \bmod R = \{\sum_{i=1}^{n} \alpha_i \cdot B_i\} \bmod R,$$

тобто отримується вихідне слово (слово для шифрування) А.

V Варіант базового несиметричного криптоалгоритму на базі СУЛ
(шифрує один, розшифровують усі)

Звернемо увагу на те, що в розглянутому вище алгоритмі серед елементів відкритого ключа є константи СЛК (величина діапазону представлення R, модифіковані ортогональні базиси $B_i^{/} = B_i /(m_i \cdot p_j) = R/(p_i \cdot p_j)$, які надають можливість шляхом розкладання їх на множники отримати сукупність основ p_i – основних констант СЛК. Внаслідок цього слід очікувати досить низької криптографічної стійкості такого алгоритму.

Як варіант підвищення криптографічної стійкості розглянемо наступний алгоритм, який у межах статті названо базовим.

Вихідне слово (для шифрування) А будемо розглядати також як число в ПСЧ, тобто як послідовність із n символів α_i (i = 1, 2, ..., n).

Закриті ключі, які створюють "випадкове" кільце для "блукання" чисел, що шифруються – сукупність основ СЛК p_i та випадкових величин x_i (i = 1, 2, ..., n), а також випадкова величина y.

Відкриті ключі – сукупність констант СЛК $B_i^{/} = B_i / m_i - x_i = R_i - x_i$, $R^{/} = R - y$, де $R = \prod_{i=1}^{n} p_i$ – діапазон представлення чисел в СЛК, $R_i = R / p_i$, $B_i = m_i \cdot R / p_i = m_i \cdot R_i$ – ортогональний базис системи. Звернемо увагу на те, що при такому формуванні величини $B_i^{/}$ та $R^{/}$ є випадковими.

Процес **шифрування** включає:

1. перевід числа А із ПСЧ у СЛК (отримання лишків α_i по основам p_i) із подальшою модифікацією цих лишків так, що $\alpha_i^{/} = \{\alpha_i \cdot m_i\}_{p_i}$; при цьому $A_{ш} = \alpha_1^{/}, \alpha_2^{/}, ..., \alpha_n^{/}$;

2. отримання величини $d = \sum_{i=1}^{n} x_i \cdot \alpha_i^{/}$;

3. обчислення $f = [\sum_{i=1}^{n} \alpha_i^{/} / p_i]$; звернемо увагу на те, що ця величина дорівнює кількості перевищень діапазону R під час переводу зашифрованого числа $A_{ш} = \alpha_1^{/}, \alpha_2^{/}, ..., \alpha_n^{/}$ в позиційну систему числення за класичним алгоритмом; дійсно, результат переводу

$$A = \{\sum_{i=1}^{n} \alpha_i^{/} B_i\}_R = \sum_{i=1}^{n} \alpha_i^{/} m_i R / p_i - [(1/R) \sum_{i=1}^{n} R \cdot \alpha_i^{/} m_i / p_i] \cdot R =$$

$$= \sum_{i=1}^{n} \alpha_i^{/} m_i R / p_i - [\sum_{i=1}^{n} \alpha_i^{/} m_i / p_i] \cdot R = \sum_{i=1}^{n} \alpha_i^{/} m_i R / p_i - f \cdot R;$$

4. обрахування $\beta = d - f \cdot y$.

Результатом шифрування є сукупність $A_{ш} = \alpha_1^{/}, \alpha_2^{/}, ..., \alpha_n^{/}$, β, f. Звернемо увагу, що і в цьому випадку в зв'язку з тим, що всі лишки зашифрованого числа є "викривленими" випадковим (невідомим криптоаналітику) чином, також забезпечується розглянуте вище "блукання" числа $A_{ш}$ числовими кільцями.

Звернемо увагу також на те, що величини f і β несуттєво збільшують розрядність зашифрованого блоку, оскільки мають досить малу власну розрядність тому, що максимальне $f_{\max}$ значення першої з них

$$f_{\max} = [\sum_{i=1}^{n} \max(\alpha_i^{/}) / p_i] = [\sum_{i=1}^{n} (p_i - 1) / p_i] = [\sum_{i=1}^{n} (1 - 1/p_i)] = [n - \sum_{i=1}^{n} (1/p_i)] \le n - 1,$$

а друга обраховується як різниця між чисельно близькими величинами.

Дешифрування здійснюється шляхом використання наступної послідовності операцій:

1. виконання алгоритму переводу зашифрованого числа зі СЛК у ПСЧ по відношенню до модифікованих значень $\alpha_i^{/}$, $B_i^{/}$ та $R^{/}$:

$$A^{/} = \sum_{i=1}^{n} \alpha_i^{/} \cdot B_i^{/} = \sum_{i=1}^{n} \alpha_i^{/} \cdot (R_i - x_i) = \sum_{i=1}^{n} \alpha_i^{/} \cdot R_i - \sum_{i=1}^{n} x_i \cdot \alpha_i^{/};$$

2. додавання до отриманого значення $A^{/}$ величини β:

$$A^{//} = \sum_{i=1}^{n} \alpha_i^{/} \cdot R_i - \sum_{i=1}^{n} x_i \cdot \alpha_i^{/} + \sum_{i=1}^{n} x_i \cdot \alpha_i^{/} - f \cdot y = \sum_{i=1}^{n} \alpha_i^{/} \cdot R_i - f \cdot y;$$

3. обчислення величини

$$c = f \cdot R^{/} = f \cdot (R - y) = f \cdot R - f \cdot y;$$

4. виконання операції обчислення за модулем R величини $A^{//}$ шляхом віднімання від неї c:

$$A^{//} = \sum_{i=1}^{n} \alpha_i^{/} \cdot R_i - f \cdot y - f \cdot R + f \cdot y = \sum_{i=1}^{n} \alpha_i^{/} \cdot R_i - R \cdot [\sum_{i=1}^{n} \alpha_i^{/} / p_i].$$

Зрозуміло, що отримане значення $A^{//}$ є шуканим розшифрованим блоком $A = A^{//}$, тобто внаслідок даної низки операцій отримується вихідне слово (слово для шифрування) А.

Приклад 2. Нехай, як і в попередньому прикладі шифруванню підлягає послідовність A = 39 = 100111; на **закритих ключах** – сукупності основ СУЛ p_1 = 4, p_2 = 5, p_3 = 7, та з "випадковими" величинами x_1 = 11, x_2 = 3, x_3 = 13, y = 5. Для такого набору основ СУЛ базовими константами є B_1 = 105 (R_1 = 35, m_1 = 3), B_2 = 56 (R_2 = 28, m_2 = 2), B_3 = 120 (R_3 = 20, m_3 = 6), R = 140.

Тоді, як **відкритий ключ** слід використовувати $B_1^{/} = (R_1 - x_1) = 24$, $B_2^{/} = (R_2 - x_2) = 25$, $B_3^{/} = (R_3 - x_3) = 7$, $(R - y) = 135$.

При таких умовах процес **шифрування** є послідовністю наступних операцій:

1. перевід числа А із ПСЧ у СЛК (отримання лишків α_i по основам p_i) із подальшою модифікацією цих лишків так, що $\alpha_i^{/} = \{\alpha_i \cdot m_i\}_{p_i}$;

$$\alpha_1^{/} = \{\alpha_1 \cdot m_1\}_{p_1} = \{3 \cdot 3\}_4 = 1,\ \alpha_2^{/} = \{\alpha_2 \cdot m_2\}_{p_2} = \{4 \cdot 2\}_5 = 3,\ \alpha_3^{/} = \{\alpha_3 \cdot m_3\}_{p_3} = \{4 \cdot 6\}_7 = 3;$$

при цьому $A_{ш}$ = 1, 3, 3;

2. отримання величини $d = \sum_{i=1}^{n} x_i \cdot \alpha_i^{/}$ = 11·1 + 3·3 + 13·3 = 59;

3. обчислення $f = [\sum_{i=1}^{n} \alpha_i^{/} / p_i]$ = [1/4 + 3/5 + 3/7] = [1,278] = 1;

4. обрахування $\beta = d - f \cdot y$ = 59 – 1·5 = 54.

Результатом шифрування є сукупність $A_{ш}$ = 1, 3, 3, 54, 1.

Дешифрування.

1. Виконання алгоритму переводу зашифрованого числа з СЛК в ПСЧ відносно до модифікованих значень $\alpha_i^{/}$, $B_i^{/}$ та $R^{/}$:

$$A^{/} = \sum_{i=1}^{n} \alpha_i^{/} \cdot B_i^{/} = 1 \cdot 24 + 3 \cdot 25 + 3 \cdot 7 = 120.$$

2. Додавання до отриманого значення $A^{/}$ величини β:

$A^{//}$ = 120 + 54 = 174.

3. Обчислення величини

$c = f \cdot R^{/} = 1 \cdot 135$.

4. Виконання операції обчислення за модулем R величини $A^{//}$ шляхом віднімання від неї c:

$A^{//} = 174 - 135 = 39 = 100111$.

Порівнюючи вихідне слово для шифрування і результати дешифрування, упевнюємося в правильності функціонування запропонованих алгоритмів шифрування і дешифрування на відкритих ключах.

VI Модифікації базового несиметричного криптоалгоритму

Звернемо увагу на те, що в процесі шифрування *за базовим алгоритмом* отримується блок, складовими якого є лишки по сукупності основ – закритих ключів p_i. Внаслідок цього в алгоритмі існує певна "дірка" для розкриття цих ключів, оскільки величина лишків по будь-якій основі зосереджена в числовому інтервалі [0, p_i –1]. Отже, маючи достатню вибірку ("статистику") із зашифрованих блоків, можна однозначно визначити величини цих закритих ключів.

Один із можливих шляхів подолання даної вади полягає в застосуванні *модифікацій базового алгоритму*. При використанні модифікацій, що пропонуються нижче, процес **шифрування** можна розглядати як такий, що складається із наступних операцій.

Перша із них, як і раніше, полягає в первинному шифруванні шляхом обрахування на "випадковому" кільці в СЛК $A_ш = \alpha_1^/, \alpha_2^/, ..., \alpha_n^/$.

Друга операція забезпечує "маскування" сукупності основ – закритих ключів p_i шляхом маскування величин лишків по кожній з основ. Сенс цієї операції зводиться до розбиття результату первинного шифрування $A_ш$ на дві складових. Таке розбиття на складові кожного з лишків після первинного шифрування слід здійснювати за певним алгоритмом чи випадковим чином. Зрозуміло, що процедура розбиття може бути в тому чи іншому сенсі оптимізованою (розміри зашифрованого блоку, швидкодія, кількість додаткових параметрів (змінних чи констант) та т. ін.). Винесемо питання цієї оптимізації за межі статті. Як алгоритм розбиття можна застосувати до елементів $A_ш = \alpha_1^/, \alpha_2^/, ..., \alpha_n^/$, наприклад, операцію отримання лишків по додатковій основі $p_д$, величина якої є досить близькою до найменшої з основ p_i, з фіксацією кількості k_{ni} переходів через $p_д$ при обрахуванні кожного із отриманих лишків $\alpha_{iд} = \{\alpha_i^/\}_{p_д}$. Тобто розглядати кожен із символів блоку первинного шифрування $\alpha_i^/ = \{\alpha_i^/\}_{p_д} + [\alpha_i^/ / p_д] \cdot p_l$. Позначимо кількість переходів через величину додаткової основи через $k_{ni} = [\alpha_i^/ / p_д]$. Тоді $\alpha_i^/ = \alpha_{iд} + k_{ni} \cdot p_д$. Для вирішення поставленого завдання з маскування основ будемо, наприклад, уважати ***для першої модифікації базового алгоритму*** першою складовою зашифрованого блоку сукупність

$$A_ш^1 = \alpha_{1д}, \alpha_{2д}, ..., \alpha_{nд}.$$

3. Тоді другою складовою зашифрованого блоку слід розглядати результати переводу в ПСЧ сукупності величин k_{ni}:

$$A_{ПСЧ}^1 = \sum_{i=1}^{n} (k_{ni} \cdot p_д) \cdot B_i^/ ,$$

4. Третьою та четвертою складовими зашифрованого блоку β, f за розглянутими вище формульними виразами будуть:

$$d = \sum_{i=1}^{n} x_i \cdot \alpha_i^/ \ , \ f = [\sum_{i=1}^{n} \alpha_i^/ / p_i] , \ \beta = d - f \cdot y .$$

Отже, зашифрований блок складається із $A_ш^1$, $A_{ПСЧ}^1$, β, f.

Процес **дешифрування після** отримання зашифрованого блоку $A_{ПСЧ}^1$, $A_ш^1$, β, f зводиться до операцій:

1. виконання алгоритму переводу другої складової зашифрованого числа з СЛК у ПСЧ по відношенню до модифікованих значень $\alpha_{iд}$, $B_i^/$ та $R^/$:

$$A_{ПСЧ}^2 = \sum_{i=1}^{n} \alpha_{iд} \cdot B_i^/ = \sum_{i=1}^{n} \alpha_{iд} \cdot (R_i - x_i) = \sum_{i=1}^{n} \alpha_{iд} \cdot R_i - \sum_{i=1}^{n} x_i \cdot \alpha_{iд};$$

2. додавання до отриманого значення $A_{ПСЧ}^2$ величини β ::

$$A_{ПСЧ}^2 = \sum_{i=1}^{n} \alpha_{iд} \cdot R_i - \sum_{i=1}^{n} x_i \cdot \alpha_{iд} + \sum_{i=1}^{n} x_i \cdot \alpha_{iд} - f \cdot y = \sum_{i=1}^{n} \alpha_{iд} \cdot R_i - f \cdot y;$$

3. обчислення величини

$c = f \cdot R^{/} = f \cdot (R - y) = f \cdot R - f \cdot y$;

4. отримання

$$A_{ПСЧ} = A^1_{ПСЧ} + A^2_{ПСЧ} = \sum_{i=1}^{n} (k_{ni} \cdot p_{\partial}) \cdot R_i + \sum_{i=1}^{n} \alpha_{i\partial} \cdot R_i - f \cdot y = \sum_{i=1}^{n} \alpha_i^{/} \cdot R_i - f \cdot y;$$

5. виконання операції обчислення за модулем R величини $A_{ПСЧ}$ шляхом віднімання від неї c:

$$A_{ПСЧ} = \sum_{i=1}^{n} \alpha_i^{/} \cdot R_i - f \cdot y - f \cdot R + f \cdot y = \sum_{i=1}^{n} \alpha_i^{/} \cdot R_i - R \cdot [\sum_{i=1}^{n} \alpha_i^{/} / p_i].$$

Видно, що отримане значення $A_{ПСЧ}$ співпадає із отриманим в наслідок реалізації *базового алгоритму* і є шуканим розшифрованим блоком, тобто, внаслідок даної низки операцій отримується вихідне слово (слово для шифрування) А. Але в цій модифікації алгоритму неможливо установити значення сукупності основ – закритих ключів p_i шляхом використання статистики.

Приклад 3. Нехай, як і в попередньому прикладі, шифруванню підлягає послідовність A = 39 = 100111; на **закритих ключах** – сукупності основ СУЛ $p_1 = 4$, $p_2 = 5$, $p_3 = 7$, та "випадкових" величин $x_1 = 11$, $x_2 = 3$, $x_3 = 13$, $y = 5$ з базовими константами є $B_1 = 105$ ($R_1 = 35$, $m_1 = 3$), $B_2 = 56$ ($R_2 = 28$, $m_2 = 2$), $B_3 = 120$ ($R_3 = 20$, $m_3 = 6$), $R = 140$.

Відкритим ключем, як і раніше, є $B_1^{/} = (R_1 - x_1) = 24$, $B_2^{/} = (R_2 - x_2) = 25$, $B_3^{/} = (R_3 - x_3) = 7$, $(R - y) = 135$.

При таких умовах процес **шифрування** є послідовністю наступних операцій:

1. перевід числа А із ПСЧ у СЛК (отримання лишків α_i по основам p_i) із подальшою модифікацією цих лишків так, що $\alpha_i^{/} = \{\alpha_i \cdot m_i\}_{p_i}$,

$\alpha_1^{/} = \{\alpha_1 \cdot m_1\}_{p_1} = \{3 \cdot 3\}_4 = 1$, $\alpha_2^{/} = \{\alpha_2 \cdot m_2\}_{p_2} = \{4 \cdot 2\}_5 = 3$, $\alpha_3^{/} = \{\alpha_3 \cdot m_3\}_{p_3} = \{4 \cdot 6\}_7 = 3$;

при цьому $A_{ш} = 1,3,3$.

2. "маскування" сукупності основ – закритих ключів p_i шляхом визначення $\alpha_i^{/} = \{\alpha_i^{/}\}_{p_{\partial}} + [\alpha_i^{/} / p_{\partial}] \cdot p_l$ та кількості переходів через величину додаткової основи $k_{ni} = [\alpha_i^{/} / p_{\partial}]$; якщо як додаткову основу p_{∂} використати $p_{\partial} = 2$, то $k_{n1} = 0$, $k_{n2} = k_{p3} = 1$, $\alpha_{1\partial} = 1$, $\alpha_{2\partial} = \alpha_{3\partial} = 1$; Будемо вважати першою складовою зашифрованого блоку сукупність

$$A^1_{ш} = \alpha_{1\partial}, \alpha_{2\partial}, ..., \alpha_{n\partial} = 1, 1, 1;$$

3. тоді другою складовою зашифрованого блоку слід розглядати результати переводу в ПСЧ сукупності величин k_{ni}:

$$A^1_{ПСЧ} = \sum_{i=1}^{n} (k_{ni} \cdot p_{\partial}) \cdot B_i^{/} = 0 \cdot 2 \cdot 24 + 1 \cdot 2 \cdot 25 + 1 \cdot 2 \cdot 7 = 64;$$

4. отримання величини $d = 59$; $f = 1$, $\beta = 54$.

Результатом шифрування є сукупність $A_{ш} = 1, 1, 1, 64, 54, 1$.

Дешифрування.

1. Виконання алгоритму переводу зашифрованого числа з СЛК у ПСЧ відносно модифікованих значень $\alpha_i^{/}$, $B_i^{/}$ та $R^{/}$:

$$A^2_{ПСЧ} = \sum_{i=1}^{n} \alpha_{i\partial} \cdot B_i^{/} = 1 \cdot 24 + 1 \cdot 25 + 1 \cdot 7 = 56.$$

2. Додавання до отриманого значення $A^2_{ПСЧ}$ величини β:

$$A^2_{ПСЧ} = 56 + 54 = 110.$$

3. Отримання

$$A_{ПСЧ} = A^1_{ПСЧ} + A^2_{ПСЧ} = 64 + 110 = 174 .$$

4. Обчислення величини

$$c = f \cdot R^{/} = f \cdot (R - y) = 1 \cdot 135 = 135 .$$

5. Виконання операції обчислення за модулем R величини $A_{ПСЧ}$ шляхом віднімання від неї c:

$$A_{ПСЧ} = 174 - 135 = 39 .$$

Видно, що отримане значення $A_{ПСЧ}$ співпадає з отриманим внаслідок реалізації *базового алгоритму* і є шуканим розшифрованим блоком, тобто, в результаті виконання даної низки операцій отримується вихідне слово (слово для шифрування) А.

Окрім того, неважко переконатися і в роботоспроможності як другої, так і третьої модифікацій базового алгоритму. Автор упевнений, що розглянуті модифікації не є вичерпними.

VII Оцінка криптографічної стійкості запропонованих алгоритмів несиметричного кодування

При оцінці криптографічної стійкості першого з криптоалгоритмів на базі СУЛ (шифрують усі, розшифровує один) слід звернути увагу на те, що оскільки процес шифрування здійснювався з використанням випадкових величин, стійкість даного алгоритму, на погляд автора, визначається неможливістю визначення секретних параметрів іншим чином, окрім прямого перебору, тобто кількістю можливих варіантів ключів p_i (i = 1, 2, ..., n), та кількістю можливих варіантів випадкової величини x. При таких переборах для кожного із варіантів можливих закритих ключів (числа переборів як p_i , так і x) слід обчислити величини $(B_i + x)$, $(R - x)$ та порівняти їх із відкритими ключами. У разі вибору n ключів з їх наперед визначеної множини потужністю N (цей приклад забезпечує криптоаналітику-порушнику полегшення задачі умов підбору ключів) та вибору величини x при її розрядності в m двійкових розрядів кількість $N_{вк}$ варіантів ключів дорівнює добутку числа перестановок (розміщень) із N елементів по n на кількість можливих значень величини x:

$$N_{вк} = A^n_N \cdot 2^m .$$

При виборі основ СУЛ з розрядністю, яка з умови забезпечення восьмибітових умовних лишків є більшою 256 (наприклад, при виборі взаємно простих чисел з проміжку [257, ..., 1579]), величина N = 195. Якщо шифруванню підлягають слова із числом символів n = 32, то без урахування кількості варіантів секретної величини x: $A^{32}_{195} \approx 10^{73}$.

З урахуванням кількості варіантів секретної величини x кількість $N_{ВК}$ варіантів ключів суттєво збільшується навіть при відносно малих розрядностях x. В таблиці для порівняння наведено кількість варіантів ключів для відомих механізмів формування цифрового підпису (за стандартом ГОСТ 34.310 – 94), та криптографічного перетворення (за стандартом ГОСТ 28147-89), а також запропонованого механізму без врахування кількості варіантів секретної величини x (колонка 4) та з врахуванням такої кількості (при m = 10, чи 2m ≈ 103 – колонка 5):

$$N_{ВК} = A^{32}_{195} \approx 10^3 \cdot 10^{73} \approx 10^{76} .$$

Як видно із таблиці, запропонований механізм забезпечує кількість варіантів ключів, яка є близькою, або навіть перевищує кількість варіантів ключів відомих механізмів, і за цим показником має, відповідно, вищу імітостійкість. У наведених прикладах кількість варіантів ключів наближається до вимог гарантованого криптозахисту

. Таблиця – Кількість варіантів ключів для різних механізмів перетворень

Довжина ключа (байти)	Кількість варіантів ключів				
	ГОСТ 34.310 – 94	ГОСТ 28147-89	ЛУ – код		
1	2	3	4	5	6
32	-	10^{76}	$>10^{73}$	$>10^{76}$	$>10^{79}$
64	$9{,}45 \cdot 10^{65}$	-	$>10^{136}$	$>10^{139}$	$>10^{1429}$
128	$9{,}45 \cdot 10^{156}$	-	$>> 10^{260}$	$>> 10^{263}$	$>> 10^{266}$

Примітка. Для другої та третьої колонок таблиці використано дані Інституту Інформаційних Технологій Харківського технічного університету радіоелектроніки (в другій колонці, виходячи з обсягу обчислень в $3 \cdot 10^5$ та $3 \cdot 10^{12}$ міпсороків відповідно).При оцінці криптографічної стійкості **першого варіанту** криптоалгоритму на базі СУЛ (шифрує один, розшифровують усі) слід звернути увагу на те, що серед елементів відкритого ключа є константи СЛК (величина діапазону представлення R, модифіковані ортогональні базиси $B_i^{/} = B_i /(m_i \cdot p_j) = R/(p_i \cdot p_j)$, які надають можливість досить просто (шляхом розкладання їх на множники) отримати сукупність основ p_i – основних констант СЛК. Це, в свою чергу, полегшує криптоаналітику можливість розкриття закритих ключів сукупності $p_i^{/} = p_j (i, j = 1, 2, ..., n)$ – величин, які, з метою підвищення криптографічної стійкості перетворення, випадковим чином вибрані із сукупності основ p_i так, що $i \neq j$. Це полегшення полягає в тому, що знання повного набору основ p_i та їх скорочених наборів, з яких обраховується кожен модифікований ортогональний базис $B_i^{/}$, дозволяє для кожного із них визначити пари p_i та p_j, які є відсутніми в даному базисі. Внаслідок цього задача криптоаналітика зводиться до визначення (тепер уже шляхом прямого перебору) з сукупності з *n* таких пар лише одного правильного варіанту (набору) ключів $p_i^{/} = p_j$ (i = 1, 2, ..., n). Неважко упевнитися в тому, що кількість варіантів ключів складає $N_{BK} = 2^n$, наприклад, при n =32 $N_{BK} = 2^{32}$. Звідсіля слід зробити висновок про <u>недостатню криптографічну стійкість даної модифікації криптоалгоритму на базі СУЛ</u>.

При оцінці криптографічної стійкості ***базового варіанту*** криптоалгоритму на базі СУЛ (шифрує один, розшифровують усі) слід звернути увагу на те, що в зв'язку із можливістю розкриття закритих ключів шляхом "статистичного" аналізу слід також зробити висновок про <u>недостатню криптографічну стійкість базового криптоалгоритму на базі СУЛ</u>.

При оцінці криптографічної стійкості будь-якої із запропонованих ***модифікацій базового варіанту*** криптоалгоритму на базі СУЛ (шифрує один, розшифровують усі) слід звернути увагу на те, що в зв'язку із неможливістю розкриття закритих ключів шляхом "статистичного" аналізу чи іншим чином, слід зробити висновок про необхідність застосування для розкриття ключів лише механізму прямого перебору з кількістю варіантів ключів, яка за рахунок більшої кількості секретних величин, ніж в алгоритмі **першого варіанту** криптоалгоритму на базі СУЛ, визначається згідно з даними колонки 6 таблиці, а отже, про <u>достатньо високу криптографічну стійкість базового криптоалгоритму на базі СУЛ,</u> яка не поступається стійкості відомих криптографічних алгоритмів.

Література: ***1.*** *Василенко В. С., Горицький В. М. Варіант завадостійкого криптографічного перетворення // "Современные проблемы телекоммуникаций", збірка доповідей на 6-ій міжнародній науково-технічній конференції, 19 – 22 серпня 2003 р. (ч. 1) // Одеська національна академія зв'язку ім. А. С. Попова – с. 71 – 73.* ***2.*** *Василенко В. С. Варіант завадостійкого криптографічного перетворення // Правове, нормативне та метрологічне забезпечення системи захисту інформації в Україні, вип.. 8, 2004 р. – с. 101 – 108.* ***3.*** *Коржов В. Асимметричные криптоалгоритмы. // Открытые системы. № 7– 8/2002.*

УДК 621.391

АНАЛИЗ СЛОЖНОСТИ *MAP*, *MAX LOG MAP* И *LOG MAP* АЛГОРИТМОВ ДЕКОДИРОВАНИЯ ТУРБОКОДОВ ПРИ ДЕКОДИРОВАНИИ БИТА ИНФОРМАЦИИ

Сергей Ливенцев, Сергей Зайцев, Борис Горлинский
Специальный факультет СБ Украины ВИТИ НТУУ "КПИ"

Аннотация: **Произведен анализ сложности Map, Max Log Map и Log Map алгоритмов декодирования турбокодов с учетом нормализации при вычислении основных функций, а также количества проверочных символов с выхода компонентного рекурсивного систематического сверточного кода кодера турбокода. В результате анализа получены аналитические выражения, определяющие количество алгебраических операций для основных алгоритмов декодирования турбокодов.**
Summary: **In the article the analysis of complication of the Map, Max Log Map and Log Map decoding**