УДК 004.056.2

О. Я. Матов[1], В. С. Василенко[2], М. Ю. Василенко[2]
[1]Інститут проблем реєстрації інформації НАН України
вул. М. Шпака, 2, 03113 Київ, Україна
[2]Національний авіаційний університет
вул. Космонавта Комарова, 1, 03058 Київ, Україна

Криптографічна стійкість методів шифрування на основі перетворень з використанням лишкових класів

Для задач забезпечення конфіденційності інформаційних об'єктів автоматизованих систем розглянуто підходи щодо оцінки криптографічної стійкості запропонованих криптографічних перетворень при використанні лишкових класів.

Ключові слова: *інформація, конфіденційність, криптографічні перетворення, лишкові класи, системи числення.*

Вступ

Однією із вкрай важливих для сучасних автоматизованих систем є проблема забезпечення конфіденційності інформації [1–3], для вирішення якої застосовуються ті чи інші методи, методики або алгоритми. Для забезпечення конфіденційності інформації у багатьох випадках використовуються криптографічні перетворення (з певною стійкістю до спроб розкриття її змісту — криптографічною стійкістю). На цей час теорія криптографічних перетворень розвинута досить широко, і для забезпечення конфіденційності інформаційних об'єктів можна застосувати різні алгоритми криптографічного перетворення. Для шифрування інформації серед інших можуть використовуватися і аналітичні перетворення [4, 5]. Із них найбільше поширення набули методи шифрування, що засновані на використовуванні матричної алгебри. Наприклад, аналітичні перетвореннях шифрування k-го блоку початкової інформації, представленого у вигляді матриці-рядка $A_k = \|a_j\|$, можуть здійснюватися шляхом перемножування цієї матриці-рядка на матрицю-ключ — кодувальну матрицю $G = \|g_{ij}\|$. У результаті перемножування виходить блок шифротексту у вигляді матриці-рядка $A_{шk} = \|a_{шi}\|$, де елементи матриці $A_{шk}$ визначаються з виразу:

$$a_{шi} = \sum_j g_{ij} a_i \ .$$

Розшифровка інформації у цьому випадку здійснюється шляхом послідовного перемножування матриці-рядка $A_{шк}$ і декодувальної матриці G^{-1}, яка є зворотною до матриці G. Операції під час кодування-декодування можуть здійснюватися за певним, визначеним відповідним алгоритмом модулем (наприклад, за модулем 2, за іншим модулем чи, навіть, за набором модулів з їхньої певної множини).

Одним із показників якості цих та інших криптографічних перетворень є їхня стійкість до розкриття — криптографічна стійкість. Надалі пропонується оцінка стійкості аналітичних криптографічних перетворень на основі переводу із позиційної системи числення в систему лишкових класів, а також із системи лишкових класів у позиційну систему числення [4, 5] з використанням матричної алгебри, коли операції здійснюються за набором модулів з їхньої певної множини.

Взагалі, процедура (алгоритм) аналітичного перетворення вихідного m-символьного цифрового коду (блоку відкритого тексту) A в n-символьний цифровий код (блок зашифрованого тексту) — $A_ш$ (на боці передавача інформації) і зворотного перетворення блоку зашифрованого тексту — числа $A_ш$ в блок відкритого тексту A (на боці одержувача інформації) зводиться до наступних операцій (функцій).

1. Формування за правилами відповідного криптографічного перетворення ключових наборів чи то матриць-ключів — кодувальної G (для прямого перетворення) та декодувальної (для зворотного перетворення) матриць G^{-1} (у [5] розглянуто варіанти та можливості визначення однієї із цих матриць при відомій іншій).

Нехай, наприклад, такі матриці мають вигляд (рис. 1).

$$\vec{G}=\begin{pmatrix} g_{11} & g_{12} & g_{13} & \cdots & g_{1m} \\ g_{21} & g_{22} & g_{23} & \cdots & g_{2m} \\ g_{31} & g_{32} & g_{33} & \cdots & g_{3m} \\ \cdots & \cdots & \cdots & \cdots & \cdots \\ g_{m1} & g_{m2} & g_{m3} & \cdots & g_{mm} \end{pmatrix},\ \vec{G}^{-1}=\begin{pmatrix} g_{11}^{-1} & g_{12}^{-1} & g_{13}^{-1} & \cdots & g_{1n}^{-1} \\ g_{21}^{-1} & g_{22}^{-1} & g_{23}^{-1} & \cdots & g_{2n}^{-1} \\ g_{31}^{-1} & g_{32}^{-1} & g_{33}^{-1} & \cdots & g_{3n}^{-1} \\ \cdots & \cdots & \cdots & \cdots & \cdots \\ g_{n1}^{-1} & g_{n2}^{-1} & g_{n3}^{-1} & \cdots & g_{nn}^{-1} \end{pmatrix}.$$

Рис. 1. Загальний вид кодувальної та декодувальної матриць

2. Представлення вихідного тексту у вигляді сукупності блоків A, B, C, ..., Z, які підлягають криптографічному перетворенню. При цьому кожен із таких блоків (рис. 2) розглядається у вигляді матриці-рядка розмірності $(1\times m)$.

$$T_{відкр}=\left(a_1 \quad a_2 \quad a_3 \quad \ldots \quad a_m\right);\ \left(b_1 \quad b_2 \quad b_3 \quad \ldots \quad b_m\right);$$
$$\left(c_1 \quad c_2 \quad c_3 \quad \ldots \quad c_m\right);\ldots;\left(z_1 \quad z_2 \quad z_3 \quad \ldots \quad z_m\right),$$
$$T_{шифр}=\left(a_{1ш} \quad a_{2ш} \quad a_{3ш} \quad \ldots \quad a_{nш}\right);\ \left(b_{1ш} \quad b_{2ш} \quad b_{3ш} \quad \ldots \quad b_{nш}\right);$$
$$\left(c_{1ш} \quad c_{2ш} \quad c_{3ш} \quad \ldots \quad c_{nш}\right);\ldots;\left(z_{1ш} \quad z_{2ш} \quad z_{3ш} \quad \ldots \quad z_{nш}\right)$$

Рис. 2. Загальний вид блоків вихідного (відкритого) та зашифрованого текстів

Тоді перша матриця-рядок складе перший блок вихідного тексту $A = (a_1, a_2, a_3, ..., a_m)$, друга матриця-рядок — блок вихідного тексту B і т.д.

3. Здійснення на боці передавача інформації криптографічного перетворення кожного із блоків відкритого тексту, наприклад, блоку A: $A_ш = A \times G$ і отримання при цьому зашифрованого тексту $A_ш$, який поблочно чи певним фрагментом (повідомленням, пакетом) передаються одержувачу. Тобто кожна із матриць-рядків, наприклад перша, шифрованого ($A_ш$) чи відкритого тексту (A) дорівнює:

$$A_ш = A \times \vec{G}, A = A_ш \times \vec{G}^{-1}. \quad (1)$$

4. Здійснення на боці одержувача інформації зворотного перетворення $A = A_ш \times G^{-1}$, $B = B_ш \times G^{-1}$, $C = C_ш \times G^{-1}$, …

Тобто, з урахуванням викладених у [4] підходів, криптографічні перетворення (шифрування) вихідного тексту (матриці відкритого тексту) здійснюються шляхом послідовного перемноження матриць-рядків A, B, C, … на кодувальну матрицю $\vec{G}$. Зворотне перетворення можна здійснити шляхом перемноження матриць-рядків шифрованого тексту $A_ш$, $B_ш$, $C_ш$, … на декодувальну матрицю $\vec{G}^{-1}$.

Нагадаємо також, що правила вибору чи формування елементів кодувальної та декодувальної матриць визначаються типом перетворення. Якщо механізм формування елементів цих матриць є секретним, чи механізм формування елементів кодувальної матриці є загальновідомим, але при їхньому формуванні використовуються деякий секретний параметр — ключ, то зашифрований код має певну криптографічну стійкість, тобто стійкість до спроб криптоаналітиків одержати з зашифрованого коду (часто з використанням певної частки відкритого вихідного тексту) ключ, кодувальну матрицю чи власне вихідний код (текст). Така криптографічна стійкість є основною властивістю таких перетворень і досить часто визначається кількістю варіантів ключів.

Одним із шляхів створення загроз конфіденційності (загроз розкриття змісту інформаційних об’єктів) з боку порушників є використання *можливо недостатньо високої* криптографічної стійкості застосованого перетворення й отримання ключів (механізмів) перетворення шляхом здійснення криптографічного аналізу фрагменту (фрагментів) відкритого тексту певної довжини та фрагменту (фрагментів) закритого (зашифрованого) тексту, який є відповідним відкритому. Таке розкриття змісту інформаційних об’єктів є можливим як з використанням відомих способів лінійного, диференційного та інших криптографічних аналізів, так і з використанням відповідної криптографічної слабкості власне запропонованих механізмів криптографічних перетворень. На погляд авторів, запропоновані ними перетворення з використанням відповідних систем числення (зокрема системи лишкових класів) і матричних операцій з погляду криптографічної стійкості можуть мати власні недоліки.

Тому в статті не аналізуються відомі підходи щодо криптографічного аналізу, а розглядаються деякі з можливих аспектів криптографічного аналізу запропонованих у [4, 5] блокових матричних перетворень, що пов’язані з використанням

відповідної криптографічної слабкості цих механізмів криптографічних перетворень, та шляхи підвищення, у разі необхідності, такої криптографічної стійкості.

Можливості із забезпечення стійкості криптографічних блокових перетворень

Запропоновані в [4, 5] механізми блокових матричних перетворень інформаційних об'єктів дають змогу здійснювати суто криптографічні перетворення, завадостійкі криптографічні перетворення (завадостійка криптографія) та завадостійке кодування (з використанням коду умовних лишків).

З початку розглянемо можливості із забезпечення стійкості тих типів блокових суто криптографічних перетворень, які викладено в [5]: позиційна система числення (ПСЧ) → система лишкових класів (СЛК) та система умовних лишків (СУЛ) → ПСЧ. Із попереднього розділу зрозуміло, що для забезпечення стійкості блокових криптографічних перетворень необхідно створити умови, коли, по-перше, виключена можливість визначення ключів перетворення з використанням «статистичного» аналізу величин елементів (лишків по наборам основ — елементів ключового набору) із фрагментів зашифрованого тексту, і, по-друге, коли обрахування (чи взагалі існування) зворотних матриць $\vec{A}^{-1}$ та $\vec{A}_{ш}^{-1}$ з тих чи інших причин є неможливим.

Відмітимо, що можливостей статистичного аналізу при перетворенні типу СУЛ → ПСЧ не існує, іншими словами, таке перетворення є стійким щодо статистичного аналізу. Це пов'язано з тим, що елементи відкритого тексту розглядаються лише як умовні лишки (без будь-яких модифікацій цих елементів), а величини власне основ системи числення залежать від цих елементів тільки через нерівність $p_i > (g - 1)$, де p_i — i-та основа СУЛ, а g — це та загально відома основа системи числення, в якій представлено елементи відкритого тексту (наприклад, $g = 256$ при байтовому представленні елементів вихідного тексту). Тобто по значенням відкритого тексту неможливо визначити таємні елементи ключа перетворення. При цьому результат криптографічного перетворення є наперед невідомим числом у позиційній системі числення, за яким визначити елементи ключа перетворення також неможливо.

При перетвореннях же із ПСЧ у СЛК величини отриманих при цьому лишків знаходяться в інтервалі $[0, (p_i - 1)]$, що за наявності достатньої статистики дає змогу визначати всі величини елементів ключа $p_i (i = 1, 2, ..., n)$.

Для виключення можливості такого «статистичного» криптоаналізу елементів фрагменту зашифрованого тексту в СЛК при перетвореннях типу ПСЧ → СЛК є достатнім «спотворення» цих елементів шляхом, наприклад, порозрядного додавання за модулем 2 (існують і інші можливості «спотворень») до відповідного блоку такого блоку (матриці-рядка), який «спотворює» перетворений текст і є таємним для порушника (в даному випадку — криптоаналітика), але є відомим як відправнику, так і одержувачу повідомлення. Цей блок (матриця-рядок), який «спотворює», може складатися, наприклад, із ключових елементів. Зрозуміло, що такий блок криптоаналітик може сформувати лише шляхом прямого перебору. При зворотному перетворенні перед виконанням усіх необхідних операцій з та-

кими блоками (матрицями-рядками) достатньо здійснити ще одне порозрядне додавання за модулем 2 до цього блоку такого ж самого «спотворюючого» блоку (матриці-рядка) і зняти, тим самим, попереднє спотворення. Таким чином, стійкість і останнього перетворення щодо «статистичного» аналізу забезпечується досить просто.

Перед розглядом умов обрахування (чи взагалі існування) зворотних матриць $\vec{A}^{-1}$ та $\vec{A}_{ш}^{-1}$ нагадаємо [5], що при використанні перетворень типу ПСЧ → СЛК і СЛК → ПСЧ для забезпечення однозначності перетворень необхідно узгодити діапазони представлення вихідних і перетворених чисел (під числом тут і надалі будемо розуміти цифровий еквівалент відповідного коду — вихідного блоку A чи зашифрованого блоку $A_ш$), тобто необхідно забезпечити виконання умови $g^{m-1} \le P$, де g — основа системи числення, яка використана для подальших математичних операцій над цими цифровими кодами ($g = 2$ — для двійкового, $g = 10$ — для десяткового представлення, $g = 256$ — для байтового представлення та т.п.); m — кількість символів вихідного блоку; $P = \prod_{j=1}^{m} p_j$ — діапазон представлення («робочий» діапазон) СЛК. Окрім того, для забезпечення можливостей блокових матричних перетворень слід узгодити й розміри матриць (довжини блоку — розмірність матриці вихідної інформації (m) і розмірність кодувальної матриці (n), а також розмірності блоку зашифрованого тексту та розмірності декодувальної матриці). Остання вимога призводить до необхідності якимось чином забезпечити рівність $m = n$, що, зрозуміло, може здійснюватися, залежно від умов, шляхом збільшення чи то m, чи то n.

З урахуванням цих зауважень відзначимо, що умовами для неможливості обрахування чи існування певних матриць при перетвореннях типу ПСЧ → СЛК є наступні.

1. Наявність у матрицях однакових (наприклад, нульових) рядків чи стовпців, коли виконується умова, зя якої визначник матриці дорівнює нулю ($\det\vec{A} = 0$), що має своїм наслідком відсутність зворотних матриць. У [5] наведено умови здійснення блокових криптографічних перетворень з використанням лишкових класів (перетворення типу ПСЧ → СЛК). Показано, що під час шифрування при $m < n$ згадане вище узгодження може здійснюватися, наприклад, шляхом доповнення блоків початкового тексту, який підлягає перетворенню (збільшення розміру матриці початкового блоку розмірності $1 \times m$) до розмірності $1 \times n$. Це забезпечується тим, що вихідні блоки (матриці-рядки) $A = (a_1, a_2, ..., a_i, ..., a_m)$ можуть доповнюватися потрібною кількістю нулів ($s = n - m$) на місцях старших розрядних коефіцієнтів. У цьому випадку матриці-рядки A набувають вигляду $A = (0, 0, \ldots, a_1, a_2, ..., a_i, ..., a_m)$. Зрозуміло, що при зворотному перетворенні (дешифруванні) результат дешифрування також буде мати таку ж кількість нулів (нульових стовпців чи рядків). Звідси витікає, що, по-перше, для створення умов, коли $m < n$, як основи системи числення в лишкових класах слід вибирати взаємно прості числа, починаючи із найменших. Тоді створюються умови для забезпечення $n > m$. По-друге, в разі неможливості забезпечення умови $m < n$ за рахунок вибору малих

значень основ СЛК, їхню кількість можна збільшити штучно. За цих умов отримати зворотні матриці $\vec{A}^{-1}$ та $\vec{A}_{ш}^{-1}$ із фрагментів відкритого та відповідного йому закритого текстів неможливо.

2. Розміри фрагментів відкритого та відповідного йому зашифрованого тексту є недостатніми для побудови матриць $\vec{A}$, $\vec{A}_{ш}$. Зрозуміло, що така можливість існує, коли кількість блоків у згаданих фрагментах є меншою, ніж n. Слід зазначити, що при цьому розв'язання відповідних матричних рівнянь дає безліч рішень.

Примітка. Забезпечити останнє можливо за умови зміни матриць перетворення (чи сеансових ключів для їхнього формування) з періодичністю, яка відповідає шифруванню/дешифруванню не більше ніж (n – 1) блоків зашифрованого тексту.

Тобто при дотриманні умов, розглянутих вище, здійснення криптоаналізу перетворення ПСЧ → СЛК через отримання кодувальних чи декодувальних матриць шляхом перетворення фрагментів відкритого та зашифрованого текстів стає неможливим.

При перетвореннях типу СУЛ → ПСЧ для створення умов, коли обрахування (чи взагалі існування) зворотних матриць $\vec{A}^{-1}$ та $\vec{A}_{ш}^{-1}$ з тих чи інших причин є неможливим, слід враховувати наступне. Для забезпечення можливості такого перетворення усі символи вихідного блока для шифрування

$$A = \alpha_1, \alpha_2, \ldots, \alpha_m,$$

слід [5] уявляти символами в деякій умовній СЛК — лишками за основами p_i (i = = 1, 2, ..., m). Щоб символи початкової системи числення можна було вважати символами в умовній СЛК значення основ цієї умовної СЛК p_i потрібно вибирати з умови

$$p_i > g^f,$$

де g — основа вихідної (позиційної) системи числення, а f — розрядність символів початкової системи числення. Ця вимога пов'язана з тим, що в СЛК значення основ є завжди більшими ніж значення лишків (а це — значення символів початкової системи числення) за цими основами. За рахунок цього завжди виконується умова $g^{m-1} \le P = \prod_{j=1}^{m} p_j$. Таким чином, кількість лишків у такій умовній СЛК завжди дорівнює числу символів у блоці вихідного коду. Звідси витікає, що для підвищення криптографічної стійкості перетворень типу ПСЧ → СЛК слід штучно вводити r додаткових основ (r = 1, 2, …) і збільшувати до $n = m + r$ розмірності матриць-рядків блоків вхідного та перетвореного текстів, а також кодувальної та декодувальної матриць. При цьому, як і для перетворення ПСЧ → СЛК, *здійснення криптоаналізу через отримання кодувальних чи декодувальних матриць шля-*

хом перетворення фрагментів відкритого та зашифрованого текстів стає неможливим.

Таким чином, обидва варіанти запропонованих блокових криптографічних перетворень забезпечують високу криптографічну стійкість, причому варіант криптоперетворень типу умовна система лишкових класів → позиційна система числення, порівняно з варіантом криптоперетворень типу позиційна система → система лишкових класів, є більш досконалим.

1. *Чипига А.Ф.* Информационная безопасность автоматизированных систем: учеб. пособ. для студентов вузов / А.Ф. Чипига. — М.: Гелиос АРВ. — 2010. — 336 с.

2. *Ростовцев А.Г.* Теоретическая криптография / А.Г. Ростовцев, Е.Б. Маховенко. — М.: Изд-во «Профессионал», 2005. — 490 с.

3. *Василенко В.С.* Варіант завадостійкого криптографічного перетворення / В.С. Василенко // Правове, нормативне та метрологічне забезпечення системи захисту інформації в Україні. — 2004. Вип. 8. — С. 101–108.

4. *Матов О.Я.* Матричні завадостійкі криптографічні перетворення / О.Я. Матов, В.С. Василенко, М.Ю. Василенко // Реєстрація, зберігання і оброб. даних. — 2011. — Т. 13, № 4. — С. 39–51.

5. *Матов О.Я.* Криптозахист інформаційних об'єктів шляхом блокових перетворень із позиційної система числення в систему лишкових класів / О.Я. Матов, В.С. Василенко, М.Ю. Василенко // Реєстрація, зберігання і оброб. даних. — 2012. — Т. 14, № 1. — С. 66–74.

Надійшла до редакції 27.10.2012