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

Криптозахист інформаційних об'єктів шляхом блокових перетворень із системи лишкових класів у позиційну систему числення

Для задач забезпечення конфіденційності інформаційних об'єктів автоматизованих систем запропоновано використання блокового криптографічного перетворення з умовної системи числення в лишкових класах у позиційну.

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

Вступ

Задача забезпечення конфіденційності та цілісності інформації [1–3] у сучасних інформаційно-телекомунікаційних системах є однією із вкрай важливих. Для її забезпечення в багатьох випадках криптографічне перетворення є чи не єдиним шляхом (з певною стійкістю до спроб розкриття її змісту — криптографічною стійкістю). На цей час широко відомими є велика кількість методів криптографічного закриття інформації, серед яких досить важливими є аналітичні матричні перетворення, що розглянуті, наприклад в роботах [1, 2], і до яких відносяться запропоновані авторами в роботах [3, 4] алгоритми криптографічного перетворення.

У цих алгоритмах, на відміну від відомих суто криптографічних перетворень [1, 2], запропоновано одночасне забезпечення не лише конфіденційності, але й цілісності інформаційних об'єктів при шифруванні — шляхом перетворення з позиційної системи числення (ПСЧ) у систему лишкових класів (СЛК), і при дешифруванні — шляхом перетворення із системи лишкових класів у позиційну систему числення. Показано також, що такі криптографічні перетворення (шифрування) вихідного тексту можна здійснити шляхом перемноження матриці-рядка, що отримана при представленні вихідного коду довжиною в k символів, і кодувальної матриці G з k рядків і k стовпців. Правила вибору чи формування її елементів виз-

начені в роботі [3]. Код, що отримано в результаті множення вихідного коду на кодувальну матрицю, є деяким криптографічним перетворенням вихідного коду.

Якщо механізм формування елементів кодувальної матриці є секретним, чи механізм формування елементів кодувальної матриці є загальновідомим, але при їхньому формуванні використовуються деякий секретний параметр — ключ, то зашифрований код має визначену криптографічну стійкість, тобто стійкість до спроб криптоаналітиків одержати із зашифрованого коду (часто з використанням певної частки відкритого вихідного тексту) ключ, чи власне вихідний код (текст). Така криптографічна стійкість є основною властивістю таких перетворень і досить часто визначається числом варіантів ключів.

Уважне ознайомлення з отриманими в [3, 4] результатами дає можливість стверджувати, що перетворення із ПСЧ у СЛК є можливим для будь-якої сукупності основ, які задовольняють відповідним вимогам. Отже, розглянуті методики дозволяють здійснити блокові криптоперетворення типу позиційна система числення → система лишкових класів з певною криптографічною стійкістю. Однак такі перетворення мають і певні вади, до яких можна віднести:

1) недостатню криптографічну стійкість, пов'язану з можливістю розкриття шифру, тобто визначення величин основ системи лишкових класів при достатньо тривалому спостереженні за блоками закритого тексту. Це є можливим завдяки тому, що максимальне значення лишків за певною основою p_i дорівнює $(p_i - 1)$, тобто визначення при тривалому спостереженні величини $(p_i - 1)$, однозначно визначає й p_i. Можна запропонувати способи запобігання цьому, але вони пов'язані з необхідністю додаткових операцій при перетворенні в систему лишкових класів;

2) велику надлишковість закритого тексту порівняно з відкритим. Останнє пояснюється тим, що збільшення криптографічної стійкості коду є можливим за рахунок використання значної кількості основ системи лишкових класів — взаємно простих чисел, величини яких перевищують (а при їхній великій кількості — значно перевищують) величину основи в позиційній системі числення. Тобто, якщо вихідний код потребує для запису (передавання, збереження та ін.) g розрядів, то кожен символ зашифрованого тексту — не менше ніж $(g + 1)$. Це, в свою чергу, призводить або до необхідності використання при запису кожного із символів системи лишкових класів подвійної розрядності (порівняно із символами в позиційній системі числення), або ж до необхідності здійснювати «переупаковку» зашифрованого тексту з метою його ущільнення (зі зворотною процедурою розущільнення), що вимагає значних затрат обчислювальних ресурсів.

У статті пропонуються, як альтернатива, кодові перетворення з деякої умовної системи умовних лишків у позиційну, котрі, на погляд авторів, є кращими від запропонованих у [3, 4].

Методики блокових криптоперетворень типу система лишкових класів → позиційна система числення

Отже, розглянемо методики криптографічних перетворень за схемами: при шифруванні — перетворення із системи лишкових класів у позиційну систему числення; зворотне — перетворення із позиційної системи числення в систему лиш-

кових класів. З цією метою будемо уявляти всі символи вихідного блока для шифрування

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

незалежно від початкової системи числення (для визначеності в межах статті початкова система числення нехай буде позиційною), символами в деякій *умовній системі лишкових класів* — лишками за основами p_i (i = 1, 2, ..., k). Щоб символи початкової системи числення можна було вважати символами в умовній системі лишкових класів, значення основ цієї умовної системи лишкових класів p_i слід вибирати з умови

$$p_i > g^f, \tag{1}$$

де g — основа вихідної позиційної системи числення, а f — розрядність символів початкової системи числення. Ця вимога пов'язана з тим, що в системі лишкових класів значення основ є завжди більшими ніж значення лишків за цими основами (а це — значення символів початкової позиційної системи числення).

Методику блокових криптоперетворень типу система лишкових класів → позиційна система числення проілюструємо прикладами.

***Приклад* 1.** Нехай криптографічному перетворенню підлягає вихідне повідомлення, яке є еквівалентним двохрозрядному (m = 2) десятковому числу A = 17. Тоді g = 10, f = 1. *Вважаємо, що це число є числом в умовній системі лишкових класів* $A_{\text{слк}}$ = (1, 7). Визначимо основи цієї умовної системи лишкових класів. Виходячи з (1), такими основами можуть бути p_1 = 11 та p_2 = 13. При цьому для p_1 = = 11, p_2 = 13, діапазон представлення чисел у СЛК $P = \prod_{j=1}^{j=n} p_j$ у цьому випадку дорівнює:

$$P = \prod_{j=1}^{j=2} p_j = p_1 p_2 = 11 \cdot 13 = 143.$$

Ортогональні базиси такої системи числення мають значення B_1 = 78, B_2 = 66, а їхні ваги m_1 = 6, m_2 = 6. Тоді, з урахуванням попередніх результатів [3, 4], кодуючу та декодуючу матриці слід записати у вигляді:

$$G = \begin{pmatrix} 78 \\ 66 \end{pmatrix}, \quad G^{-1} = \begin{pmatrix} \{100\}_{11} & \{100\}_{13} \\ \{10\}_{11} & \{10\}_{13} \\ \{1\}_{11} & \{1\}_{13} \end{pmatrix} = \begin{pmatrix} 1 & 9 \\ 10 & 10 \\ 1 & 1 \end{pmatrix},$$

що надає змогу одержати перетворене в позиційну систему числення (зашифроване) число

$$A_{\text{псч}} = (1, 7) \times \begin{pmatrix} 78 \\ 66 \end{pmatrix} = (1 \cdot 78 + 7 \cdot 66) = (78 + 462) = (540)_{143} = 111_{10} = 1101111_2.$$

Звернемо увагу на ту обставину що *при переводі в позиційну систему числення операції слід здійснювати за модулем*, величина якого дорівнює діапазону представлення P (у цьому випадку за модулем $P = 143$), оскільки кінцевий результат ($A_{\text{псч}}$) не повинен перевищувати цей діапазон представлення. Це обмеження відповідає вимогам щодо криптографічних перетворень, згідно з якими при криптографічних перетвореннях довжина коду зашифрованого слова не повинна суттєво відрізнятися від довжини коду незашифрованого слова. З погляду зворотного перетворення ця вимога не є принциповою, але при її недотриманні слід розраховувати на збільшення коду зашифрованого числа. Так у розглянутому прикладі число $A_{\text{псч}} = 540$ (дев'ять двійкових розрядів) без урахування діапазону представлення ($P = 143$) і $A_{\text{псч}} = 111$ (сім двійкових розрядів) при представленні в діапазоні P. При більшій кількості символів вихідного коду ця різниця може бути значно більшою.

При дешифруванні, тобто при *переводі в умовну систему лишкових класів операції слід здійснювати за заданим набором модулів* $p_1 = 11$, $p_2 = 13$, оскільки кінцевий результат — кожен лишок α_i з їхнього набору, яким запишуться складові шуканого числа A, не повинен перевищувати величини відповідної основи p_i. Це обмеження є принциповим. У цьому випадку

$$A = (111) \times \begin{pmatrix} 1 & 9 \\ 10 & 10 \\ 1 & 1 \end{pmatrix} = (\{12\}_{11},\ \{20\}_{13}) = (1, 7),$$

що відповідає вихідному числу 17, яке підлягало прямому (в позиційну систему числення) та зворотному (в умовну систему лишкових класів) перетворенням.

***Приклад* 2.** Нехай криптографічному перетворенню підлягає вихідне повідомлення, яке є еквівалентним дворозрядному десятковому вихідному слову $A = 17$ ($m = 2$), кожен символ якого представлено напівбайтами в двійковій системі числення. Тоді $g = 16$, а $f = 1$ (можна $g = 2$, $f = 4$). Вважаємо, що це число є числом в умовній СЛК $A_{\text{слк}} = (1, 7)$. Визначимо основи цієї умовної СЛК. Виходячи з (1), такими основами можуть бути $p_1 = 17$ та $p_2 = 19$. При цьому $p_1 = 17$, $p_2 = 19$, $m_1 = 9$, $m_2 = 9$, $B_1 = 171$, $B_2 = 153$, а діапазон представлення $P = \prod_{j=1}^{j=n} p_j$ у цьому випадку дорівнює: $P = \prod_{j=1}^{j=2} p_j = p_1 \cdot p_2 = 17 \cdot 19 = 323$. Тоді, з урахуванням попередніх результатів, кодуючу та декодуючу матриці слід записати у вигляді:

$$G = \begin{pmatrix} 171 \\ 153 \end{pmatrix},\ G^{-1} = \begin{pmatrix} \{256\}_{17} & \{256\}_{19} \\ \{16\}_{17} & \{16\}_{19} \\ \{1\}_{17} & \{1\}_{19} \end{pmatrix} = \begin{pmatrix} 1 & 9 \\ 16 & 16 \\ 1 & 1 \end{pmatrix},$$

а перетворене (зашифроване) в позиційну систему числення число буде таким:

$$A_{\text{псч}} = A_{\text{ш}} = (1, 7) \times \begin{pmatrix} 171 \\ 153 \end{pmatrix} = (1 \cdot 171 + 7 \cdot 153) = (171 + 1071)_{323} = (1242)_{323} = 273_{10}.$$

Звернемо увагу на те, що після кодування первинний код A при його представленні десятковими цифрами в межах кожного з двох напівбайтів (1, 7) має двійкове значення $A = (00010111)_2 = 23_{10}$, після перетворень — значення $A_{\text{ш}} = 273_{10} = (100010001)_2$, або через десяткові значення відповідних напівбайтів $A_{\text{ш}} = (1, 1, 1)$, що свідчить про здійснене криптографічне перетворення.

Зворотне перетворення матиме вигляд

$$A = (1, 1, 1) \times \begin{pmatrix} 1 & 9 \\ 16 & 16 \\ 1 & 1 \end{pmatrix} = (\{18\}_{17}, \{26\}_{19})) = (1, 7),$$

що відповідає вихідному числу 17, яке підлягало прямому (в позиційну систему числення) та зворотному (в умовну систему лишкових класів) перетворенням.

Неважко упевнитися, що криптографічне перетворення за такою схемою є вільним від викладених вище вад, оскільки:

1) представлення зашифрованого тексту в позиційній (особливо в двійковій) системі числення має, внаслідок властивостей позиційної системи числення, найвищу щільність упаковки. При цьому задачі ущільнення та розущільнення є зайвими;

2) зашифрований текст представляється в позиційній системі числення, тому розкрити шифр, тобто набір основ в умовній системі лишкових класів шляхом статистичного аналізу величин символів є неможливим (скоріше за все для цього потрібен лише прямий перебір усіх їхніх можливих варіантів).

Таким чином, варіант блокових криптоперетворень типу умовна система лишкових класів → позиційна система числення, порівняно із запропонованим у [3] варіантом криптоперетворень типу позиційна система → система лишкових класів, є більш досконалим.

1. *Чипига А.Ф.* Информационная безопасность автоматизированных систем. / А.Ф. Чипига: учеб. пособ. для студентов вузов. — 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.

.

Надійшла до редакції 13.07.2012