УДК 681.3.05

В.Г. Красиленко, С.К. Грабовляк

Вінницький соціально-економічний інститут університету «Україна»

МОДИФІКАЦІЇ СИСТЕМИ RSA ДЛЯ СТВОРЕННЯ НА ЇЇ ОСНОВІ МАТРИЧНИХ МОДЕЛЕЙ ТА АЛГОРИТМІВ ДЛЯ ЗАШИФРУВАННЯ ТА РОЗШИФРУВАННЯ ЗОБРАЖЕНЬ

У статті розглядаються модифікації криптосистеми RSA для створення матричних моделей та алгоритмів криптоперетворень зображень. Запропоновано матричні моделі, що враховують специфіку зображень і можуть бути адаптованими до різних їх типів та форматів. Наведені формули та алгоритмічні кроки процедур зашифрування та розшифрування зображення розмірністю 128×128. Визначені переваги та продемонстровані можливості та таких модифікацій системи RSA для обробки зображень модельними експериментами у програмному середовищі Mathcad Professional.

Ключові слова: *криптографічні перетворення, модифікації, система RSA, матричні моделі, зашифрування, розшифрування, зображення, коригування.*

Вступ

Постановка проблеми. Бурхливий розвиток криптографії обумовлений стрімким розвитком інформаційних технологій та необхідністю забезпечення необхідного рівня захисту інформації державного, військового, комерційного та приватного змісту. Серед великого різноманіття криптографічних алгоритмів і протоколів [1, 2], що використовуються для захисту інформації лише незначна частина присвячена методам та алгоритмам орієнтованим на матричні моделі та матричні спеціалізовані алгоритми і засоби. Крім того, за декілька останніх років доля задач, в яких необхідно виконувати криптографічні перетворення над багатовимірними сигналами, серед яких важливе місце займають різноманітні напівтонові, кольорові зображення та двовимірні масиви. Так, наприклад, в біометричних системах, системах розпізнавання, ідентифікації об'єктів, інтелектуальному управлінні, при прийнятті рішень необхідно обробляти та передавати в зашифрованому вигляді велику кількість різноманітних зображень, наприклад, відбитки пальців, фотографії осіб, зображення рухомих об'єктів райдужної сітківки ока тощо. Оскільки ця інформація часто є конфіденційною, існує гостра необхідність в її криптографічних перетвореннях з метою захисту від несанкціонованого доступу. Актуальність проблеми створення високоефективних моделей, алгоритмів, протоколів та криптосистем для обробки та криптографічних перетворень зображень підтверджується і суттєвим зростанням долі робіт, що присвячені зашифруванню та розшифруванню зображень.

Аналіз останніх досліджень та публікацій. Огляд робіт присвячених проблемі криптоперетворень зображень, якому може бути присвячена окрема стаття, що виходить за рамки даної роботи, показав, що серед значної кількості робіт по цій тематиці і в Україні і за кордоном [3 – 15] можна виділити частину робіт, які концептуально відрізняються від більшої кількості тим, що вони зорієнтовані саме на матричні моделі, засоби та алгоритми. У роботах [9, 10] було запропоновано модифіковані та більш узагальнені матричні алгоритми криптографічних перетворень зображень і так звані матричні афінно-перестановочні алгоритми [12], що базуються на модифікації відомих афінних шифрів. Результати моделювання [11, 12] процесів криптоперетворень багатоградаційних та кольорових зображень на основі таких моделей та алгоритмів показали їх суттєві переваги у порівнянні з традиційними скалярними афінними асиметричними шифрами такі як: більша стійкість, збільшення швидкодії, можливість паралельно виконувати обчислювальні процедури та процеси та реалізовувати їх за допомогою паралельних проблемно-спеціалізованих засобів, матричних процесорів. У роботі [13] на основі матричних афінних шифрів запропонований алгоритм та процедура створення цифрового сліпого підпису (ЦСП) на текстографічні документи та наведені результати моделювання реально розробленої і практично перевіреної програми для формування та верифікації такого ЦСП. Такі матричні криптографічні моделі, алгоритми і криптосистеми на їх основі краще та ефективніше відображаються на повністю паралельні матричні обчислювальні засоби, оскільки описуються суто математичними матричними моделями, а це суттєво підвищує продуктивність обробки при криптоперетвореннях та зменшує час на їх виконання. Відомі також результати моделювання алгоритмів створення 2D ключа [14], суть яких полягає в узагальнені відомих протоколів створення та генерування ключів на матричний випадок і формуванні та описі цих протоколів за допомогою матричних моделей.

Але недоліком таких матричних афінних чи афінно-перестановочних алгоритмів є необхідність у використанні декількох великорозмірних матричних ключів, представлених у вигляді випадкових зобра-

жень певної розмірності. Для матричних афінних шифрів необхідно 2 ключі зашифрування та 2 ключі розшифрування [15], для афінно-перестановочних алгоритмів як мінімум 3-4 ключа, не кажучи вже про додаткові параметри β.

Постановка завдання. Метою роботи є пошук, розробка та моделювання матричних алгоритмів криптоперетворень зображень зі зменшеною кількістю матричних ключів при достатній їх стійкості. Вихідною гіпотезою для розробки такого матричного алгоритму криптоперетворень зображень з одним матричним ключем зашифрування та одним матричним ключем розшифрування є припущення про можливість таких відповідних модифікацій базової, широко відомої криптосистеми RSA та її теоретичних основ, які б при узагальнені на матричний випадок враховували специфіки зображень та матричної обробки. Теоретична сутність відомої (скалярної, за визначенням авторів) криптосистеми RSA полягає в тому, що створення ключів складається з таких операцій :

1. Вибираються два простих числа k і l
2. Обчислюється їхній добуток n = (k· l)
3. Вибирається довільне число e (e<n), таке, що НСД(e, Ψ(n)) = 1, де Ψ(n) = (k-1)(l-1), тобто e повинне бути взаємно простим із числом Ψ(n).
4. До числа e шукають обернене до нього за модулем Ψ(n) число d.
5. Два числа (e, n) – публікуються як відкритий ключ.
6. Число d зберігається в найсуворішому секреті – це і є закритий ключ, який дозволить читати всі послання, зашифровані за допомогою пари чисел (e, n).

Процес зашифрування за допомогою цих чисел виконується так :

1. Відправник розбиває своє повідомлення на рівні блоки по $k \equiv [\log_2(n)]$ біт, де квадратні дужки позначають узяття цілої частини від дробового числа. Таким чином кожен блок може бути інтерпретований як число з діапазону $(0;\ 2^k - 1)$.
2. Для кожного такого i-го числа-блока (назвемо його m_i) обчислюється $c_i(m_i)$ за виразом $c_i \equiv ((m_i)^e)_{\mathrm{mod}\, n}$. Блоки c_i і є зашифроване повідомлення Їх можна спокійно передавати по відкритому каналу, оскільки, операція піднесення в ступінь по модулю простого числа, є необоротною математичною задачею. Зворотна їй задача зветься «логарифмування в кінцевім полі» і є на кілька порядків більш складною задачею. Тобто навіть якщо зловмисник знає числа e і n, то по c_i прочитати вихідні повідомлення m_i він не може ніяк, крім як повним перебором m_i.

Процес розшифрування виконується так:

Для кожного отриманого i-го числа-блока криптограми c_i обчислюється $d_i(c_i)$ розшифроване число-блок за виразом $d_i \equiv ((c_i)^d)_{\mathrm{mod}\, n}$. Після конкатенації блоків отримують розшифроване повідомлення.

Виклад основного матеріалу

Допустимо, що сукупність чисел m_i є масив у вигляді матриці. Тоді аналогічно сукупності c_i та d_i також будуть матрицями з такою ж розмірністю N×M. Але, якщо раніше до всіх компонентів цих матриць в скалярному RSA застосовували один скалярний ключ e зашифрування та один скалярний ключ d розшифрування, то ми пропонуємо до кожного i-го компонента застосовувати свою i-пару взаємопов'язаних ключів (e_i, d_i), що вибираються з допустимої множини $(E,D) = \{e_1,\ldots e_{N\times M}, d_1,\ldots d_{N\times M}\}$ пар для даних вибраних чисел k і l у відповідності до відомих правил. У відповідності до нижче наведених результатів проведених досліджень назвемо ключі зашифрування та розшифрування відповідно **KEYP** та **OKEY**. Тоді процеси зашифрування та розшифрування можна представити у вигляді таких матричних моделей:

$$\mathbf{C} \equiv \mathbf{M}^{[\wedge]\mathbf{KEYP}}_{\mathrm{mod}\, n\cdot \mathbf{1}}; \qquad (1)$$

$$\mathbf{D} \equiv \mathbf{C}^{[\wedge]\mathbf{OKEY}}_{\mathrm{mod}\, n\cdot \mathbf{1}} \qquad (2)$$

або

$$c_{i,j} = (m_{i,j})^{keyp_{i,j}}_{\mathrm{mod}\, n};\ d_{i,j} = (c_{i,j})^{okey_{i,j}}_{\mathrm{mod}\, n},$$

де $\mathbf{M} = \begin{bmatrix} m_{11} & m_{12} & \ldots & m_{1N} \\ m_{21} & m_{22} & \ldots & m_{2N} \\ \ldots & \ldots & \ldots & \ldots \\ m_{M1} & m_{M2} & \ldots & m_{MN} \end{bmatrix};$

$$\mathbf{C} = \begin{bmatrix} c_{11} & c_{12} & \ldots & c_{1N} \\ c_{21} & c_{22} & \ldots & c_{2N} \\ \ldots & \ldots & \ldots & \ldots \\ c_{M1} & c_{M2} & \ldots & c_{MN} \end{bmatrix};$$

$$\mathbf{D} = \begin{bmatrix} d_{11} & d_{12} & \ldots & d_{1N} \\ d_{21} & d_{22} & \ldots & d_{2N} \\ \ldots & \ldots & \ldots & \ldots \\ d_{M1} & d_{M2} & \ldots & d_{MN} \end{bmatrix};$$

$$\mathbf{KEYP} = \begin{bmatrix} keyp_{11} & keyp_{12} & \ldots & keyp_{1N} \\ keyp_{21} & keyp_{22} & \ldots & keyp_{2N} \\ \ldots & \ldots & \ldots & \ldots \\ keyp_{M1} & keyp_{M2} & \ldots & keyp_{MN} \end{bmatrix};$$

$$\mathbf{OKEY} = \begin{bmatrix} okey_{11} & okey_{12} & \ldots & okey_{1N} \\ okey_{21} & okey_{22} & \ldots & okey_{2N} \\ \ldots & \ldots & \ldots & \ldots \\ okey_{M1} & okey_{M2} & \ldots & okey_{MN} \end{bmatrix};$$

$$\mathbf{1} = \begin{bmatrix} 1 & 1 & \ldots & 1 \\ 1 & 1 & \ldots & 1 \\ \ldots & \ldots & \ldots & \ldots \\ 1 & 1 & \ldots & 1 \end{bmatrix}.$$

[^]– операція поелементного піднесення у степінь за модулем.

Таким чином можна модифікувати відомий математичний апарат, що лежить в основі криптосистеми RSA, на матричний випадок. Крім того, наше припущення полягає в тому, що потужності множин отриманих матричних ключів **KE** та взаємопов'язаних з ними ключів **KD** за відповідною процедурою та правилами, навіть при знанні цих процедур та правил, буде настільки значною, що дозволить успішно використовувати такий підхід при формуванні необхідної пари матричних ключів. Останні, до речі, теж будуть по суті матрицями з розмірністю N×M.

Спочатку необхідно вибрати таких два простих числа, щоб їхній добуток якнайближче знаходився до числа, що представляє максимальну інтенсивність пікселя зображення, що підлягає зашифруванню або до максимального числа, що представляється не одним байтом, а двома, трьома чи більшою кількістю байтів. Для випадку кодування чорно-білих багато градаційних зображень, оскільки кожен піксель кодується байтом, один з можливих варіантів це вибір чисел k=11, l=23, тоді їх добуток буде дорівнювати kl=253, а функція Ейлера від kl, тобто число взаємно простих з ним чисел буде визначатись за відомою формулою Ψ(kl)=(k-1)· (l-1) і буде дорівнювати для нашого випадку 220. Це означає, що для кожного ij-го пікселя матричного ключа, що формується, лише 220 значень (чисел) можуть бути використані. Це необхідно для того, щоб до кожного скалярного значення цього ij-ого пікселя ключа можна було знайти обернене число за модулем Ψ, тобто сформувати скалярний ключ розшифрування ij-ого пікселя або для нашого матричного випадку це означає сформувати матричний ключ (матрицю) розшифрування **OKEY**, кожен ij-ий елемент якої буде відповідати необхідній вимозі, а значить також буде лежати у множині таких чисел, які менші ніж множина всіх допустимих значень градацій зображення. На відміну від традиційної криптосистеми RSA, в якій числа k і l зберігаються в таємниці, а стійкість забезпечується складністю задачі факторизації числа kl, тобто пошуку невідомих співмножників k і l, в нашому випадку не обов'язково, як буде підтверджено далі, зберігати ці числа в таємниці. Це пояснюється тим, що навіть при невеликій кількості (220, дивись вище) можливих значень якби мікроключів, тобто скалярних піксельних ключів, з яких складається матричний ключ, множина матричних ключів є дуже значною (залежить від розмірності матриць, а вони як мінімум 64×64), а тому множина створюваних ключів є досить великою і її можна оцінити. Але у зв'язку з тим, що не всі значення яскравості зображення, що відповідає такому ключу допустимі необхідно проводити так звану процедуру коригування значень пікселя такого ключа зашифрування. Спочатку, за відомими протокольними процедурами або відомими методами генерування випадкових чисел формується випадкове зображення **G2** (матриця), кожен ij-й елемент якої є випадкове число a∈0:255, що представляється байтом двійкового коду. Якщо це зображення вибрано як ключ двома сторонами, то цей ключ повинен бути ними узгоджений відомими підходами та конкретними протоколами. Один з найпростіших це просто вибране спільно одне із зображень. Якщо ж це зображення згенеровано шляхом того чи іншого протоколу обміну, наприклад, протоколу Діффі-Хеллмана модифікованого на матричний випадок для створення 2D ключа, то в цьому випадку це зображення або цей сесійний ключ створюється у відповідності до протоколу без необхідності зустрічі сторін і не потребує знання тих випадкових матриць зображень, які випадковим чином вибирались і тою і іншою стороною при формуванні таким протоколом 2D ключа. В будь-якому разі таке створене і гарантовано випадкове зображення **G2** може стати необхідним ключем для зашифрування (чи розшифрування) лише при необхідному коригуванні. Суть останнього полягає у відкиданні чи заміні в зображенні **G2** тих пікселів, які мають значення з недопустимої множини чисел у відповідності до правил системи RSA. Нами пропонується коригування, яке полягає в тому, що до кожного числового значення пікселя добавляється одиниця до тих пір поки необхідна умова буде забезпечена. А оскільки доля недопустимих значень пікселя для нашого варіанту вибраних чисел k і l складає всього 253-220=33, то границі між допустимими значеннями є відносно малими, а тому буквально за 1 чи 2 кроки додавання одиничної яскравості утвориться необхідний ключ. Ці несуттєві відмінності в матрицях зображення **G2** та **KEYP** візуально непомітні.

У зв'язку з тим що кожен елемент матриці **S1**, що відповідає текстографічному документу (ij-ий піксель зображення), що підлягає зашифруванню може мати значення, які перевищують вибране число kl, то необхідно цю матрицю (зображення) також відкоригувати. Таке коригування полягає у заміні значень, що перевищують чи дорівнюють числу kl чи зменшеними на 1 чи на відповідну кількість таких 1. Для нашого випадку лише три значення не підходять у матриці зображень, це 253, 254, 255. Ймовірність появи в реальних зображеннях таких значень інтенсивностей пікселів незначна, а відносна зміна цих яскравостей практично не помітна візуально, тому це не впливає на сприйняття текстографічних документів. Крім того можна передбачити і розробити алгоритми, які б після розшифрування зображення могли враховувати процес коригування і здійснювати процес декоригування зображень.

Оскільки матричний ключ зашифрування **KEYP** (хоч і таємний) відомий для обох сторін, то кожна з них при необхідності в момент зміни сесійного ключа шукає для нього обернений ключ. Цей ключ є матриця чисел, кожне з яких для ij-ого елемента матриці є числом оберненим за модулем Ψ до числа, що відповідає ij-ому елементу ключа.

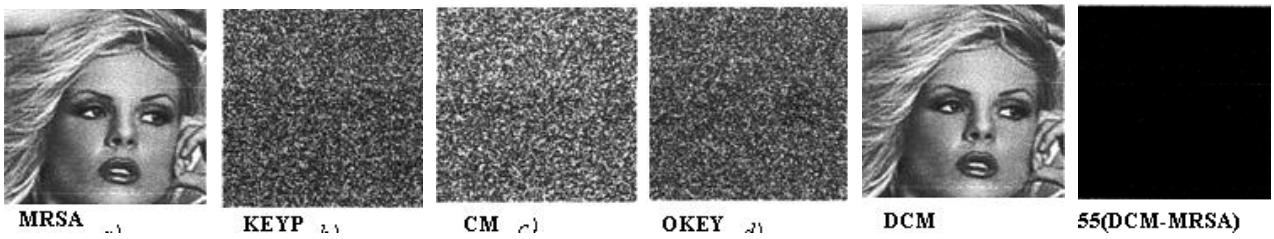

Рис. 1. Результати зашифрування та розшифрування зображення на базі модифікованої системи RSA: а – вхідне відкориговане зображення; б – ключ зашифрування; в – криптограма; г – ключ розшифрування; д – розшифроване зображення; е – різницеве зображення

Алгоритм процесу зашифрування та розшифрування зображення

Отже, розглянемо процес зашифрування та розшифрування зображень використовуючи модифікацію системи RSA у вигляді програмних алгоритмічних блоків, які створюються у програмному середовищі MathCad. Для того щоб здійснити зашифрування та розшифрування зображення потрібно виконати такі етапи:

1. Вибираються два простих числа k, l, обчислюється їх добуток і за допомогою функції Ейлера знаходиться кількість взаємно простих з kl чисел:

$$k := 11 \quad l := 23 \quad kl := k \cdot l \quad kl = 253$$

$$\Psi := (k-1)\cdot(l-1) \quad \Psi = 220$$

2) Формулюються ключі таким чином:

- методом генерування випадкових чисел формується випадкове зображення **G2** для створення ключа.

$$G2_{i,j} := \mathrm{round}(\mathrm{rnd}(201), 0)$$

Зазначимо, що замість 201 можна обирати інше максимальне значення діапазону, яке повинно бути менше kl.

- виконується коригування ключа: до зображення **G2** додаємо одиничну яскравість доти, поки необхідна умова не буде забезпечена і таким чином отримаємо ключ зашифрування **KEYP** (рис. 1, б):

$$KEYP_{i,j} := \left| \begin{array}{l} s \leftarrow G2_{i,j} \\ \text{while } \mathrm{csd}(s,\Psi) \neq 1 \\ \quad s \leftarrow s + 1 \end{array} \right.$$

- визначається ключ розшифрування **OKEY** (рис. 1, г), в якому елементи є оберненими до елементів ключа **KEYP**:

$$OKEY_{i,j} := \left| \begin{array}{l} s \leftarrow 0 \\ \text{while } \mathrm{mod}\left[\left(KEYP_{i,j}\right)\cdot s, \Psi\right] \neq 1 \\ \quad s \leftarrow s + 1 \end{array} \right.$$

2. Процес зашифрування зображення виконується так:

- перед зашифруванням вхідне зображення **S1** коригується з метою заміни значень, що перевищують чи дорівнюють числу kl і в результаті формується зображення **MRSA** (рис. 1, а):

$$MRSA_{i,j} := \left| \begin{array}{l} s \leftarrow S1_{i,j} \\ \text{while } S \geq kl \\ \quad s \leftarrow s - 1 \end{array} \right.$$

- зображення **MRSA** кодується ключем **KEYP** в результаті чого отримується криптограма **CM**, яка надсилається призначеному адресату (рис. 1, в).

$$CM_{i,j} := \left| \begin{array}{l} l \leftarrow 1 \\ s \leftarrow MRSA_{i,j} \\ \text{while } l < KEYP_{i,j} \\ \quad \left| \begin{array}{l} s \leftarrow \mathrm{mod}\left(MRSA_{i,j}, kl\right) \\ l \leftarrow l + 1 \end{array} \right. \\ s \end{array} \right.$$

3. Для розшифрування криптограми **CM** використовується сформований ключ **OKEY**, який дає можливість отримати розшифроване зображення **DCM** (рис. 1, д):

$$DCM_{i,j} := \left| \begin{array}{l} l \leftarrow 1 \\ s \leftarrow CM_{i,j} \\ \text{while } l < OKEY_{i,j} \\ \quad \left| \begin{array}{l} s \leftarrow \mathrm{mod}\left(s\cdot CM_{i,j}, kl\right) \\ l \leftarrow l + 1 \end{array} \right. \\ s \end{array} \right.$$

На рис. 1 показано результати моделювання запропонованим алгоритмом у програмному середовищі MathCad, в якому всі матриці, що використовувались були розмірністю 128 × 128.

Різницеве зображення між вхідним зображенням та розшифрованим (рис. 1, е) підтверджує правильну роботу запропонованого алгоритму для зашифрування та розшифрування зображень.

Висновки

Запропоновано модифікації криптосистеми RSA для створення матричних моделей та алгоритмів криптоперетворень зображень. Розроблена математична модель алгоритму зашифрування та розшифрування зображень, які краще відображаються на паралельні апаратні засоби їх реалізації та проведені модельні експерименти в середовищі MathCad. Показано, що такі розроблені моделі та алгоритми мають такі переваги як: високу швидкодію при обробці зображень великої розмірності, при цьому час криптоперетворення в модельних експериментах не перевищує декількох секунд, підвищену криптос-

тійкість, широкі функціональні можливості при криптоперетвореннях багатоградаційних та кольорових зображень представлених в різних форматах, значні резерви підвищення швидкодії та продуктивності запропонованих моделей та алгоритмів при їх апаратній реалізації. Запропоновані матричні моделі є узагальненням скалярних моделей, враховують специфіку зображень і можуть бути адаптованими до різних типів та форматів, легко реалізуються в сучасних програмних середовищах типу MathCad, MathLab та відображаються на апаратні засоби, мають перспективи подальшого їх вдосконалення.

Список літератури

1. Ємець В. Сучасна криптографія: Основні поняття [Текст] / В. Ємець, А. Мельник, Р. Попович. – Львів: БаК, 2003. – 144 с.

2. Хорошко В.О. Методи та засоби захисту інформації [Текст]: навч. посібник / В.О. Хорошко, А.О. Четков. – К.: Юніор, 2003. – 502 с.

3. Ковальчук А. Підвищення стійкості системи RSA при шифруванні зображень [Текст] / А. Ковальчук // Технічні вісті. – 2009. - № 1-2. – С. 70-71.

4. Рашкевич Ю.М. Афінні перетворення в модифікаціях алгоритму RSA шифрування зображень [Текст] / Ю.М. Рашкевич, А.М. Ковальчук, Д.Д. Пелешко // Автоматика. Автоматизация. Электротехнические комплексы и системы. – 2009. – № 2 (24). – С. 59-66.

5. Chin-Chen Chang. A new encription algorithm for image cryptosystems [Text] / Chin-Chen Chang, Min-Shian Hwang, Tung-Shou Chen // The Journal of Systems and Software. – 2001. – No. 58. – PP. 83-91.

6. Deergha Rao K. A New and Secure Cryptosysyem for Image Encryption and Decryption [Text] / K. Deergha Rao, K. Praveen Kumar, P.V. Murali Krishna // IETE Journal of research. – 2011. – Vol. 57. – Issue 2. – PP. 165-171.

7. Han Shuihua. An Asymmetric Image Encryption Based on Matrix Transformation [Text] / Han Shuihua, Yang Shuangyuan // Ecti transactions on computer and information technology. – 2005. – Vol.1, No.2. – PP. 126-133

8. Krasilenko V.G. A noise-immune cryptographic information protection method for facsimile information transmission and the realization algorithms [Text] / V.G. Krasilenko, V.F. Bardachenko, A.I. Nikolsky, et. al., // Proc.SPIE, 2006. - Vol. 6241. – P. 316-322.

9. Красиленко В.Г. Моделювання матричних алгоритмів криптографічного захисту [Текст] / В.Г. Красиленко, Ю.А. Флавицька // Вісник НУ «Львівська політехніка». «Комп'ютерні системи та мережі». – 2009. – № 658. – С. 59-63.

10. Красиленко В.Г. Моделювання матричних афінних алгоритмів для шифрування кольорових зображень [Текст] / В.Г. Красиленко, К. Огородник, Ю. Флавицька // Комп'ютерні технології: наука і освіта. Тези доповідей V Всеукр. наук.-пр. конф. – Київ, 2010. – С. 120-124.

11. Красиленко В.Г. Оцінювання стійкості та часу зламування у матрично-перестановочних алгоритмах криптоперетворень [Текст] / В.Г. Красиленко, С.К. Грабовляк // Наука і навчальний процес: науково-методичний збірник матеріалів науково-практичної конференції ВСЕІ Університету "Україна". – Вінниця, 2012. – С. 173-174.

12. Красиленко В.Г. Моделювання матричного афінно-перестановочного алгоритму для криптоперетворень зображень [Текст] / В.Г. Красиленко, С.К. Грабовляк // Наука і навчальний процес: науково-методичний збірник матеріалів науково-практичної конференції ВСЕІ Університету "Україна". – Вінниця, 2012. – С. 171-172.

13. Красиленко В.Г. Матричні афінні шифри для створення цифрових сліпих підписів на текстографічні документи [Текст] / В.Г. Красиленко, С.К. Грабовляк // Системи обробки інформації. – 2011. – № 7 (97). – С.60-63.

14. Красиленко В.Г. Моделювання модифікованого алгоритму створення 2-D ключа в криптографічних застосуваннях [Текст] / В.Г. Красиленко, О.І. Нікольський, О.О. Лазарєв // Науково-методичний збірник науково-практичної конференції «Наука і навчальний процес». – Вінниця, 2008. – С. 107-109.

15. Красиленко В.Г. Матричні афінно-перестановочні алгоритми для шифрування та дешифрування зображень [Текст] / В.Г. Красиленко, С.К. Грабовляк // Системи обробки інформації. – 2012. – № 3 (101). – С. 53-61.

Надійшла до редколегії 5.10.2012

Рецензент: д-р техн. наук, проф. В.М. Лисогор, Вінницький національний аграрний університет, Вінниця.

МОДИФИКАЦИИ СИСТЕМЫ RSA ДЛЯ СОЗДАНИЯ НА ЕЕ ОСНОВЕ МАТРИЧНЫХ МОДЕЛЕЙ И АЛГОРИТМОВ ДЛЯ ШИФРОВАНИЯ И РАСШИФРОВАНИЯ ИЗОБРАЖЕНИЙ

В.Г. Красиленко, С.К. Грабовляк

В статье рассматриваются модификации криптосистемы RSA для создания матричных моделей и алгоритмов криптопреобразования изображений. Предложено матричные модели, которые могут учитывать специфику изображений и быть адаптированы к различным их типам и форматам. Приведенные формулы и алгоритмические шаги процедур шифрования и расшифрования изображения размерностью 128 × 128. Определенные преимущества и продемонстрированы возможности таких модификаций системы RSA для обработки изображений модельными экспериментами в программной среде Mathcad Professional.

Ключевые слова: *криптографические преобразования, модификации, система RSA, матричные модели, шифрование, расшифровка, изображения, корректировки.*

MODIFICATION OF RSA TO CREATE ON ITS BASIS MATRIX MODELS AND ALGORITHMS FOR ENCRYPTION AND DECRYPTION IMAGES

V.G. Krasilenko, S.K. Grabovlyak

In the article the modified RSA cryptosystem to generate matrix models and algorithms of cryptographic transformation of images. Proposed a matrix model that can be tailored to specific images, and be adapted to different types and sizes of. Presented formulas and algorithmic procedures steps encryption and decryption image dimension 128 × 128. Advantages and demonstrated capabilities and such modifications of RSA imaging model experiments programmed in Mathcad Professional.

Keywords*: cryptographic transformation, modification system RSA, matrix models, encoding, decoding, image, adjustments.*