УДК 681.3
© А. Лагун[1], С. Лозинський[1], 2012

ДОСЛІДЖЕННЯ КРИПТОСИСТЕМИ МАК–ЕЛІСА ТА РОЗРОБКА АЛГОРИТМІВ ДЛЯ ЇЇ РЕАЛІЗАЦІЇ

В статті проведено дослідження криптосистеми Мак–Еліса і наведено блок–схеми алгоритму який реалізовує роботу даної системи шифрування. На основі проведеного дослідження різних кодів з виправленням помилок обрано алгеброгеометричні коди.

This article gives investigation of Mac–Eliece cryptosystem, block–schemas of algorithm of the crypto system realization have been provided. The algebraic – geometrical codes have been elected by theinvestigation of the different codes errors emendation.

1. ВСТУП

Для забезпечення високої якості переданої інформації необхідно вирішувати завдання протидії перешкодам як природнім, так і навмисним у каналах зв'язку, уникнути несанкціонованого доступу до інформації та усунути спроби нав'язування неправдивої інформації. Для цього при передачі інформації використовуються різні алгоритми завадостійкого кодування, шифрування та імітозахисту. Для забезпечення перерахованих вище вимог можливе використання алгоритму Мак–Еліса.

Перспективним є вивчення та використання кодових схем захисту інформації доказової стійкості для реалізації механізмів інтегрованого забезпечення достовірності і конфіденційності [1]. Основна ідея цих кодових схем полягає у «маскуванні» алгебраїчних блокових кодів під коди загального призначення. Ці схеми для реалізації односторонніх функцій спеціального перетворення даних використовують важко вирішувані завдання декодування випадкового коду. Стійкість кодових схем захисту інформації, побудованих на кодах БЧХ і кодах Ріда–Соломона, вважається недостатньою [2].

Для підвищення стійкості можна використовувати алгеброгеометричні коди які належать до кодових схем доказової стійкості [3]. Ці коди будуються по алгебраїчних кривих. Теорія побудови цих кодів узагальнює більшість відомих алгебраїчних кодів таких як коди Боуза–Чоудхурі–Хоквінгема, кодів Ріда–Соломона, альтернативних кодів, у тому ж числі кодів Гоппи. Використання алгебро геометричних кодів для передачі даних по дискретних каналах зв’язку дозволяє отримати суттєвий енергетичний виграш від кодування.

[1] Національний університет «Львівська політехніка»

2. ОГЛЯД СИСТЕМИ ВІДКРИТОГО ШИФРУВАННЯ МАК–ЕЛІСА

В 1978 році Роберт Мак Еліс розробив криптосистему з відкритими ключами на основі теорії алгебраїчного кодування [4]. Цей алгоритм використовує існування певного класу кодів виправляючих помилки, вони називаються кодами Гоппа. Мак–Елісом було запропоновано створити код Гоппа і замаскувати його під звичайний лінійний код.

В криптосистемі Мак–Еліса параметрами системи, загальними для всіх абонентів, є цілі числа k, n, і t. Для отримання відкритого і відповідного секретного ключа кожному з абонентів потрібно здійснити наступну послідовність дій [5]:

Вибрати породжуючу матрицю $G=G_{k\times n}$ двійкового (n, k) – лінійного коду, який виправляє t помилок, для якого відомий ефективний алгоритм декодування;

Випадково вибрати двійкову невироджену матрицю $S=S_{k\times k}$;

Випадково вибрати підстановочну матрицю $P=P_{n\times n}$;

Перемножити матриці $G'=S\cdot G\cdot P$;

Відкритим ключем є пара (G', t), секретним – трійка (S,G,P).

Для кожного незвідного многочлена $g(x)$ над $GF(2^m)$ степеня t існує двійковий незвідний код Гоппа довжини $n=2^m$ і довжини $k \geq n–mt$, здатний виправляти t або менше помилок. Оскільки це лінійний код, він може бути описаний як $k\times n$ породжуюча матриця G. За допомогою випадкової невиродженої матриці S розміру $k\times k$ і перестановочної матриці P розміру $n\times n$ приховується структура матриці G:

$$G'=S\cdot G\cdot P. \tag{1}$$

Нова матриця G' є матрицею, яка генерує інші лінійні коди. Шифрування полягає в перемноженні інформаційного вектора довжини k–біт на матрицю G' і додавання за модулем 2 вектора помилок e вагою t:

$$c = m \cdot G' \oplus e. \tag{2}$$

Першим кроком розшифрування є множення c на P^{-1}. Тоді можна відновити $m\cdot S$ із:

$$c \cdot P^{-1} = (m \cdot S \cdot G) \oplus (e \cdot P^{-1}). \tag{3}$$

Повідомлення m відновиться після перемноження на S^{-1}.

Застосування кодів побудованих по просторових кривих для формування кодової схеми дозволяє отримати ще один додатковий параметр маскування коду та підвищити енергетичний виграш від кодування.

3. АЛГЕБРОГЕОМЕТРИЧНІ КОДИ НА ПРОСТОРОВИХ КРИВИХ.

Для побудови алгебро–геометричного коду потрібно взяти проективну алгебраїчну криву X над полем $FG(q)$ як сукупність розв'язків алгебраїчного рівняння [6]

$$f(x_0, x_1, x_2, x_3) = 0 \qquad (4)$$

Нехай $p_0(x_0, x_1, x_2, x_3)$, $p_1(x_0, x_1, x_2, x_3)$, …, $p_{N-1}(x_0, x_1, x_2, x_3)$ – N суміжних розв'язків рівняння (4) – точок просторової кривої X. Зафіксуємо дивізор D кривої X і множину раціональних функцій, що асоціюються з дивізором D, тобто множина, що складається з нуля і функцій $f \neq 0$, для яких (f) + D ≥ 0. Це еквівалентно набору генераторних функцій:

$F_0(x_0, x_1, x_2, x_3)$, $F_1(x_0, x_1, x_2, x_3)$, $F_2(x_0, x_1, x_2, x_3)$,..., $F_m(x_0, x_1, x_2, x_3)$

де $F_0, F_1, \ldots, F_m$ – форми однакового степеня і $F_0(x_0, x_1, x_2, x_3) \neq 0$.

Інакше кажучи, $\varphi(x) = (F_0(x), F_1(x), \ldots, F_m(x))$, як точка в P^m.

Нехай α – степінь класу дивізора, $\alpha > g-1$, тоді відображення $\varphi: X \to P^m$ задає породжуючу матрицю:

$$G = \begin{Vmatrix} F_0(p_0(x_0, x_1, x_2, x_3))...F_0(p_{n-1}(x_0, x_1, x_2, x_3)) \\ F_m(p_0(x_0, x_1, x_2, x_3))...F_m(p_{n-1}(x_0, x_1, x_2, x_3)) \end{Vmatrix} \qquad (5)$$

алгебро–геометричного коду, з конструктивними характеристиками

$$(n \leq N,\ k \geq \alpha - g + 1,\ d \geq n - \alpha).$$

Для формування кодового слова $(c_0, c_1, \ldots, c_{n-1})$ алгебро–геометричного коду на просторових кривих, заданого через породжуючу матрицю достатньо помножити інформаційний вектор $(i_0, i_1, \ldots, i_{k-1})$ на матрицю (5), тобто для всіх $j=0, \ldots, n-1$ виконати наступне перетворення

$$c_j = \sum_{i=0}^{m-1} i_i F(p_j(x_0, x_1, x_2, x_3)). \qquad (6)$$

Нехай $\alpha > 2g - 2$, тоді відображення $\varphi: X \to P^{m-1}$ задає перевіряльну матрицю

$$H = \begin{Vmatrix} F_0(p_0(x_0, x_1, x_2, x_3))...F_0(p_{n-1}(x_0, x_1, x_2, x_3)) \\ F_m(p_0(x_0, x_1, x_2, x_3))...F_m(p_{n-1}(x_0, x_1, x_2, x_3)) \end{Vmatrix}^T \qquad (7)$$

алгебро–геометричного коду з конструктивними характеристиками

$$(n \leq N,\ k \geq n - \alpha + g - 1,\ d \geq \alpha - 2g + 2).$$

Добуток прийнятого з помилками кодового слова

$c^* = \| c_0+e_0, c_1+e_1, \ldots, c_{n-1}+e_{n-1} \|$ на перевіряльну матрицю (7)

$$\left\| c_0^*, c_1^*, \ldots, c_{n-1}^* \right\| \cdot \begin{Vmatrix} F_0(p_0(x_0, x_1, x_2, x_3))...F_0(p_{n-1}(x_0, x_1, x_2, x_3)) \\ F_m(p_0(x_0, x_1, x_2, x_3))...F_m(p_{n-1}(x_0, x_1, x_2, x_3)) \end{Vmatrix}^T \qquad (8)$$

дає значення синдромного вектора

$$S = \| S_0, S_1, \ldots, S_{r-1} \|. \quad (9)$$

Значення синдромного вектора залежить тільки від вектора помилки e і не залежить від значення кодового слова c

$$S = c^* \cdot H + e \cdot H = e \cdot H, \quad (10)$$

де $c^* \cdot H = 0$.

Розкривши дужки у виразі (8) та з урахуванням (10), виразимо елементи синдромного вектора:

$$\begin{cases} S_0 = \sum_{i=0}^{n-1} e_i \cdot F_0(P_i) \\ S_1 = \sum_{i=0}^{n-1} e_i \cdot F_1(P_i) \\ \ldots \\ S_{r-1} = \sum_{i=0}^{n-1} e_i \cdot F_{r-1}(P_i) \end{cases} \quad (11)$$

Задача декодування кодового слова $\left\| c_0^*, c_1^*, \ldots, c_{n-1}^* \right\|$ алгебро–геометричного *(n, k, d)* коду над *GF(q)* полягає у знаходженні кодового слова c та вектора помилок e за відомим вектором c^* і обчисленими за допомогою перевіряльної матриці вигляду (7) елементами синдромного вектора (11).

Для однозначного знаходження вектора помилок вводиться многочлен локаторів помилок (МЛП):

$$\begin{aligned} \Lambda(x, y, z) = x^{u-2} + a_{t-3,1,0} \cdot x^{u-3} \cdot y + \cdots + a_{1,0,0} \cdot x + \\ + a_{0,1,0} \cdot y + a_{0,0,1} \cdot z + a_{0,0,0} \end{aligned} \quad (12)$$

розширеннями якого є локатори – такі набори точок, які перетворюють у нуль многочлен (12).

МЛП (12) однозначно задає розташування помилок у векторі

$$e = \| e_0, e_1, \ldots, e_{n-1} \|. \quad (13)$$

Знаходження коефіцієнтів $a_{i_x i_y i_z}$ МЛП $\Lambda(x, y, z)$ дозволяє однозначно вказати розташування виниклих при передачі кодового слова помилок, наприклад шляхом почергової підстановки всіх наборів (X_J, Y_J, Z_J) $J = 0, \ldots, n-1$ в многочлен $\Lambda(x, y, z)$ і перевірці його рівності нулю.

4. КРИПТОАНАЛІЗ

Відомі неповні атаки класифікуються за трьома категоріями:

Перша категорія включає атаки при яких намагаються вирахувати ключ або еквівалентні ключі. Проте існування еквівалентного коду Гоппа малоймовірно.

Другий тип атак спрямований на відновлення безпосередньо повідомлення m. Основна ідея полягає у виборі і розв'язуванні до n рівнянь із c і G'. Однією з особливостей є те, що контролюється вхідне і вихідне повідомлення. Іншою – те що j $(j>0)$ помилок є допустимими. Атака оптимізується по відношенню до j.

До третьої категорії можна віднести атаки на основі алгоритму ітераційної оптимізації, який дозволяє визначити кількість операцій коректування помилок як залежність від найбільшої ваги t, яка становить $20 \cdot n^3$. Ця атака не суперечить тому факту, що декодування для загального лінійного коду є NP– повною задачею, оскільки лише шаблонна помилка з вагою Хемінга ≤ t може бути виправлена.

5. ЗАСТОСУВАННЯ АЛГОРИТМУ МАК–ЕЛІСА ДЛЯ ЕЛЕКТРОННИХ ЦИФРОВИХ ПІДПИСІВ

З проведеного дослідження алгоритму Мак–Еліса встановлено, що цей алгоритм може використовуватися для реалізації електронного цифрового підпису (ЕЦП). При використанні алгоритму Мак–Еліса для ЕЦП абонент А може послати абоненту В секретне повідомлення М з підписом Р. Для цього потрібно виконати наступний протокол:

1) Абонент В бере закритий ключ – матриці (S, G, P).

2) Абонент В обчислює відкритий ключ (генеруючу матрицю) $G_{PJ(N\times K)} = SGP$, і публікує пару $(G_{PJ(N\times K)}, t_J)$ у довіднику відкритих ключів мережі.

3) Абонент А бере з довідника відкриті ключі абонента В, вибирає випадковий вектор e, який має довжину n, вагу $t \le t_j$, і потім обчислює кодове слово C за формулою, $C = MG_{pj} + e$, де М–секретне повідомлення, яке буде передане абоненту В. Тут вектор e відіграє роль цифрового підпису абонента A.

4) Отримуючи кодове слово С, абонент В виконує декодування з використанням матриць (S, G, P), після цього отримує секретне повідомлення M. Таким чином, без передачі секретного ключа між абонентами в мережі абонент А послав абоненту В секретне повідомлення зі своїм підписом, а абонент В відкрив дане повідомлення. Можна порахувати цифровий підпис абонента А за формулою $e = CM_{pj}$ для того щоб переконатись в його достовірності.

6. РОЗРОБЛЕННЯ АЛГОРИТМІВ ТА ПРОГРАМНОГО ЗАБЕЗПЕЧЕННЯ ДЛЯ РЕАЛІЗАЦІЇ КРИПТОСИСТЕМИ МАК–ЕЛІСА

Зашифрування

Для зашифрування повідомлення, воно переводиться в бітовий вигляд і множиться на відкритий ключ. Даний процес було реалізовано в методі Encryption_Text, структура алгоритму якого зображена на рис. 1.

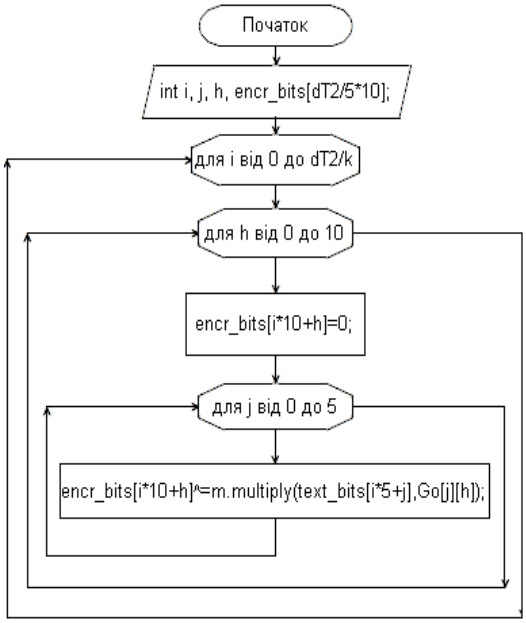

Рис. 1. Структура алгоритму зашифрування (Encryption_Text)

Значення змінних та функцій:

– dT2 – довжина масиву послідовності вхідних бітів;
– k – розмір кодового слова;
– encr_bits – масив зашифрованих бітів;
– text_bits – масив вхідних бітів;
– Go – матриця з відкритим ключем;
– multiply – функція, яка здійснює множення в полях Галуа.
– Розроблений алгоритм містить три цикли:
– цикл нижнього рівня вкладеності здійснює перебір всієї послідовності вхідних бітів;

– цикл першого рівня вкладеності здійснює перебір всіх стовпців матриці відкритого ключа;

– цикл другого рівня вкладеності перебирає рядки матриці відкритого ключа.

Результати множення по стовпцях матриці відкритого ключа додаються за допомогою операції виключне АБО.

Як приклад, для зашифрування задається відкритий текст у графічному вікні, що зображено на рис. 2.

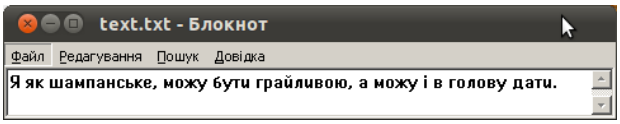

Рис. 2. Вхідні дані

Результати зашифрування заносяться у інший файл і зберігаються у вигляді бітової послідовності, що показано на рис. 3.

Розшифрування

Щоб розшифрувати повідомлення потрібно перемножити зашифроване повідомлення на закритий ключ, тобто матриці: P^T, S^{-1}.

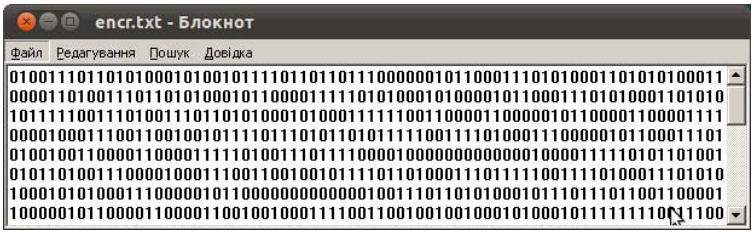

Рис. 3. Зашифровані дані

Множення зашифрованого повідомлення на транспоновану перестановочну матрицю здійснюється в методі De_Permutation, блок–схему якого зображено на рис. 4.

Значення змінних та функцій:

de_P – масив бітів зашифрованого повідомлення перемножених на матрицю зворотної перестановки;

add – функція що здійснює додавання в полях Галуа;

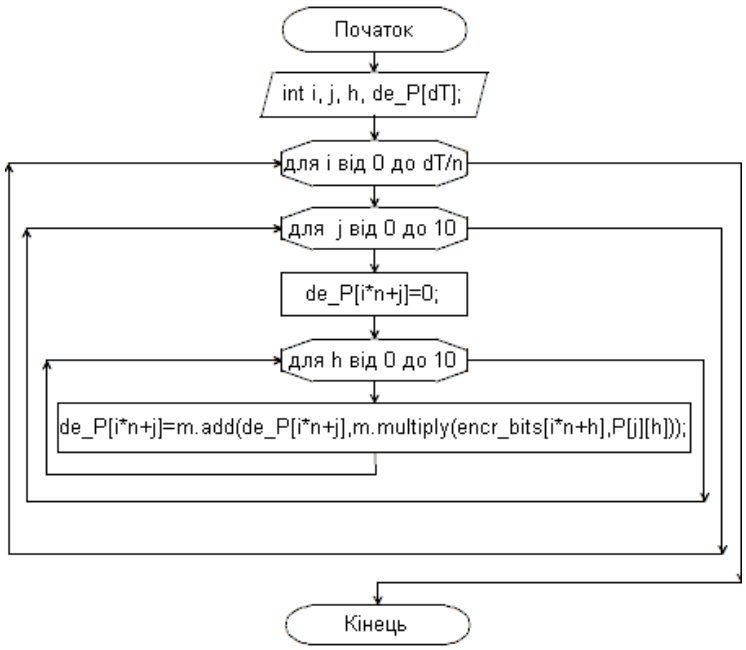

Рис. 4. Блок–схема методу De_Permutation

В цьому методі перемножуються біти зашифрованого повідомлення на стовпці матриці перестановки, і додаються до значень отриманих при перемножуванні на попередні стовпці. Зашифроване повідомлення розбивається на послідовності з 10 біт для почергового перемноження на матрицю розміру 10x10. Всі ці дії виконуються в полях Галуа.

Метод de_S множить одержане з попереднього методу повідомлення на обернену матрицю S; блок–схему зображено на рис. 5.

Значення змінних та функцій:

decrypt_bits – масив бітів розшифрованого повідомлення

Inverce_Matrix – функція яка знаходить обернену матрицю;

S2 – обернена матриця S;

На даному етапі перемножуються значення отримані з попередніх обчислень на обернену матрицю S. Результатом цих дій є послідовність біт розшифрованого повідомлення, які записуються у файл у вигляді байтової послідовності.

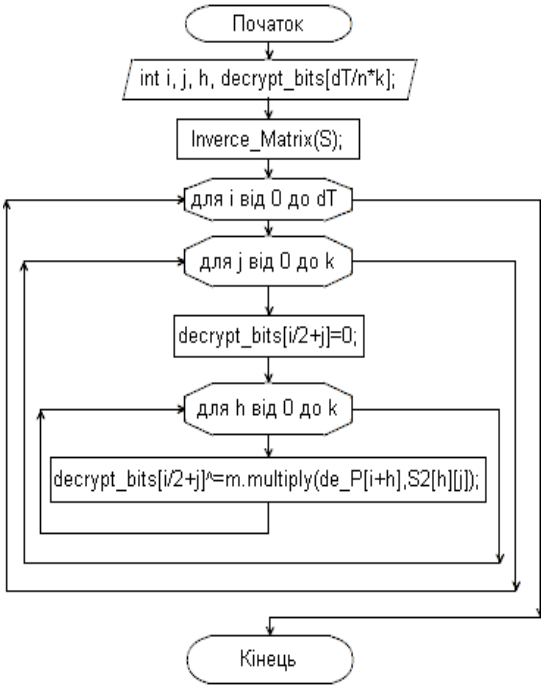

Рис. 5. Блок–схема методу de_S

Результати розшифрування зображено на рис. 6.

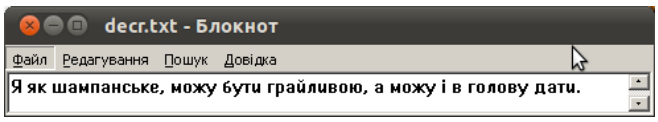

Рис. 6. Розшифровані дані

7. ВИСНОВКИ

Криптосистема Мак–Еліса є перспективною, через те що вона не потребує складних обчислювальних потужностей, а це дозволяє її реалізацію на малопотужних комп'ютерах.

Встановлено, що суттєвим недоліком криптосистеми є значний обсяг переданих даних. Проте останнім часом кількість переданих даних через великі обчислювальні потужності інформаційних систем відходить на другий план, а важливішою стає стійкість до зламу.

Система шифрування Мак–Еліса має певні переваги над іншими криптосистемами даного сегменту, а саме системами з відкритим клю-

чем. В порівнянні з системою RSA перевагами криптосистеми Мак–Еліса є менші вимоги до «заліза»; швидкість здійснення шифрування; коректуючи здібності кодування; краща криптостійкість за умови використання певних кодувань та «маскування»; можливість визначення стійкості.

Встановлено, що система шифрування Мак–Еліса, попри недоліки, залишається перспективною через зростання обчислювальних здатностей комп'ютерів і завдяки застосуванню нових алгоритмів кодування.

Розроблений алгоритм та програмне забезпечення реалізує дану криптосистему. З множини існуючих систем кодування вибрано алгебро–геометричні коди через їх актуальність, зокрема здатність маскувати код під випадковий. Параметри програми: довжина інформаційного вектора k = 5; довжина кодового слова n = 10; кількість штучно введених помилок t = 1.

1. В. Грабчак, З. Грабчак, І. Пасько, П. Трофіменко Кодові схеми захисту інформації доказової стійкості на просторових кривих Сумський державний університет, Суми, 2001. 2. Ф.Дж. Мак–Вильямс, Н. Дж. А. Слоэн Теория кодов, исправляющих ошибки: М.: Связь, 1979. 3. В. І. Грабчак Синтез каскадних кодів з алгебро–геометричними кодами на зовнішній ступені. – Львів, 2009. 4. Hung–Min Sun Enhancing the Security of the McEliece Public–Key Cryptosystem Journal of information science and engineering 16 799–812 (2000), Taiwan. 5. P.Loidreau, N.Sendrier Weak keys in the McEliece public–key cryptosystem B.P. 105 78 153 Le Chesnay CEDEX, France, 2000. 6. В. В. Золотарёв Г. В. Овечкин Помехоустойчивое кодирование. Методы и алгоритмы: Справочник М.: – Телеком, 2004.