Журнал обчислювальної та прикладної математики **2014, № 1(115)** Journal of Computational & Applied Mathematics

УДК 517.9

ЗАСТОСУВАННЯ ГРУПОВИХ СТРУКТУР І ОПЕРАЦІЇ ЗСУВУ НА РОЗФАРБОВАНИХ ГРАФАХ ДО ПОБУДОВИ БЛОЧНИХ ШИФРІВ

Р. В. Скуратовський

Резюме. Встановлені достатні умови можливості побудови добутку операцій шифрування на бінарному розфарбованому графі дереві. Побудовано алгоритм. Зроблені оцінки складності прямого відновлення текста за отриманим шифром.

Вступ

Сьогодні на практиці частіше всього шифрування тексту відбувається симетричним алгоритмом, асиметричні ж шифри застосовуються для шифрування ключа [1], який передається отримувачу шифру чи цифрового підпису. Для швидкого шифрування тексту застосовують блочні симетричні шифри, саме такого типу шифр і розглянемо в роботі.

Інструментом для побудови такого шифра є розфарбовані графи. Розфарбовані графи це складний комбінаторний об'єкт, який може мати багато інтерпритацій та застосувань. Особливо цікаво вивчати групи автоморвізмів таких графів та їх сумісне використання з самими графами для побудови різних композицій шифрів. Різноманітні групові конструкції можуть бути застосовані для шифрування на графах та заслуговують особливого вивчення. При цьому певний конкретний колір відповідає певному блоку текста. Як відомо, граф дерево має експоненційну функцію росту. Саме це і дозволить зробити процес брутального підбору ключа обчислювально складною задачею.

Однією із загальноприйнятих сучасних вимог до блочних шифрів є їх обгрунтована стійкість відносно відомих на сьогоднішній день методів криптоаналізу, до яких, зокрема, належать алгебраїчні методи, що базуються на методах гомоморфізмів. Багато спеціалістів відносять ці методи до одних із перспктивних атак на сучасні симетричні системи шифрування. Представлений в роботі метод має обгрунтовані оцінки стійкості до деяких атак та є достатньо швидким, що є однією з переваг симетричного блочного шифрування. Стійкість блочних шифрів до методів криптоаналізу, що одержані в роботах К. Патерсона і Д. Вагнера [10] і які називаються методами гомоморфізму та групового криптоаналізу, як правило, визначається алгебраїчними властивостями різних груп підстановок. Саме вивченню таких властивостей і можливостей їх застосування присв'ячена дана робота. Вибір шифру з тими чи іншими властивостями диктується конкретною ситуацією [3]. Даний алгоритм блочного шифрування може при

довжині блока $n \leq 8$ бути застосовано у якості нелінійних перетворень, що є у s-блоках шифрів типу AES чи ГОСТ 28147-89.

Щоб досягти наявності всіх цих властивостей одночасно, доцільно застосувати композицію кількох шифрів або їх добуток. Завдяки рекурсивному принципу побудови шифру, що має залежність від відкритого тексту, досягається імітостійкость шифра, в данному випадку принцип його здійснення подібний до принципу гамування. Також цьому сприяє успішно реалізований завдяки спеціальній груповій консрукції блочний шифр заміни.

В роботі детально описана NP-повна задача, зроблено аналіз її складності. Дається підхід до знаходження відображення слова, за допомогою рекурсивно заданих групових конструкцій, побудовано композицію шифрів зсуву та підстановки. Описані операції на групах та на графах.

1. Означення і основні результати

Нагадаємо основні означення і технічні засоби. Нехай X — скінченний алфавіт. Позначимо через X^ω множину всіх нескінченних вправо послідовностей (слів) $x_1x_2\ldots$, де $x_i \in X$, аналогічно $X^{-\omega}$ — нескінченних вліво послідовностей над X а $X^{\mathbb{Z}} = X^\omega \sqcup X^{-\omega}$. В теорії блочного кодування і блочного шифрування часто зустрічаються поняття скінченного зсуву, простору зсуву [4].

Означення 1. Відображення $\sigma : X^{\mathbb{Z}}$ за правилом: $\sigma(X) = Y$, де $Y_i = X_{i+1}, i \in \mathbb{Z}$, називається зсувом.

Аналогічним є означення зсуву σ на просторі X^ω як відображення

$$\sigma(x_1x_2x_3,\ldots) = x_2x_3\ldots,$$

яке витирає першу літеру нескінченного вправо слова. Для будь-яких нескінченних слів $\omega_1 = x_1x_2x_3,\ldots,\omega_2 = y_1y_2y_3,\ldots \in X^\omega$ введено відстань $d(\omega_1,\omega_2) = \frac{1}{2^n}$, де n — довжина спільного початку слів ω_1 і ω_2.

Означення 2. Простором зсуву над алфавітом X називається підмножина $X_F \subseteq X^{\mathbb{Z}}$ така, що ніяке слово з F не входить у жодне нескінченне слово з X_F для деякого $F \subseteq X^*$, де F — множина заборонених слів.

Характерною властивістю простору зсуву X_F є σ-інваріантність підмножини X_F з множини $X^{\mathbb{Z}}$ [4].

Означення 3. Скінченний зсув називається N-зсувом, якщо існує $F \subseteq X^{N+1}$.

Означення 4. *Розфарбований граф* Γ в кольори 0 і 1 назвемо $\Gamma(0,1)$ графом, якщо виконується:

1) вершини i-го рівня піддерева графа з коренем на $(i-1)$-ому рівні мають різний колір;

2) з кореня кожного піддерева виходять ребра різних кольорів.

Надалі умова 1) може бути розширена так, що вершини i-го рівня мають усі наявні кольори.

Означення 5. Графом двоїстим до графа дерева $\Gamma(0,1)$ назвемо дерево

$$\widetilde{\Gamma}(0,1) := \bigcup_{i=0}^{\infty} \bigcup_{j=0}^{\infty} \acute{\Gamma}_{i_j}(0,1),$$

де $\acute{\Gamma}_{i_j}(0,1)$ — піддерево i-го рівня з коренем у j-тій вершині цього рівня. В підграфі $\acute{\Gamma}_{i_j}(0,1)$ відбулася інверсія кольорів крім випадків, коли колір вершини та ребра, що в нього входить співпадають.

Означення 6. Підмоножина $A : A \subseteq X^{\omega}$ називається *раціональною*, якщо існує скінченний орієнтований граф Γ з відміченою початковою вершиною v_0 і стрілками, що помічені елементами алфавіта X. При цьому мітки стрілок, що виходять з однієї вершини $v_i \in \Gamma$ попарно різні і множина усіх слів, які можна отримати послідовною конкатенацією міток на шляхах з початком у v_0, співпадає з A.

Граф, що фігурує в означенні 6 називається *детермінованим* автоматом, який розпізнає множину A. Зрозуміло, що простір односторонніх зсувів скінченного типу є раціональною множиною в X^{ω}.

Означення 7. Нескінченною геодезичною назвемо шлях в графі дереві T з вершини v_{i_0}, в одному з можливих напрямків, що являє собою послідовність попарно різних вершин $(v_{i_0}, v_{i_1}, v_{i_2}, \ldots)$, $\{v_{i_k}, v_{i_{k+1}}\} \in ET$, і ребер, що з'єднанують сусідні вершини.

Для побудови блочного шифру введемо скінченні геодезичні.

Означення 8. Назвемо скінченною геодезичною шлях в скінченному графі дереві з вершини v_{i_0} в одному з можливих напрямків послідовність попарно різних вершин $(v_{i_0}, v_{i_1}, v_{i_2}, \ldots)$, сусідні з яких з'єднані ребром. Висотою геодизичної назвемо кількість її ребер.

Природньо, що довжина блока дорівнює висоті геодизичної. Опишемо алгоритм шифрування на $\Gamma(0,1)$:

1. розбиваємо алфавіт $X = x_1 x_2 \ldots x_n$ на дві частини $X_1 = y_1 y_2 \ldots y_k$ і $X_2 = z_1 z_2 \ldots z_{n-k}$ так, щоб $X_1 \cap X_2 = \oslash$, $X_1 \cup X_2 = X$;
2. вводимо бієктивну відповідність $X_1 \longleftrightarrow 1$, $X_2 \longleftrightarrow 0$;
3. вхідне повідомлення розбивамо на блоки по n символів та шифруємо кожен блок окремо;
4. кожен блок шифруємо починаючи з кореня дерева однаковим алгоритмом незалежно від повереднього блока:
   (a) з нульового рівня дерева рухаємось по ребру, колір якого відповідає типу підалфавіта до якого належить перша літера;
   (b) у відповідність цій літері ставимо або наступну літеру цього ж підалфавіту, якщо колір вешини, в яку ми прийшли, та колір підалфавіту, до якого відноситься перша літера співпадаються, або літеру іншого підалфавіту з цим же порядковим номером у підалфавіті, якщо кольори різні.

Введемо позначення: $X_i = \{\sigma_{i_1}, \sigma_{i_2}, \sigma_{i_3}, \ldots\}$ тоді якщо $x_i \in X_j$, то $x_i = \sigma_{j_q}$ а зашифрований символ $c_i = E(x_i) = \sigma_{j_{(q+k_j)(mod|M_j|)}}$.

Якщо $X = \{a, c, e, \ldots\} \bigcup \{c, d, \ldots\}$ і всі величини зсувів k_j однакові, то це шифр зсуву на k_j позицій.

Алгоритм дешифрування на $\Gamma(0,1)$:

1. Будуємо $\widetilde{\Gamma}(0,1)$ по заданому $\Gamma(0,1)$ дереву.

2. Виконуємо пункти c) і d) з перетворення шифрування але відповідність літера — колір будуємо дещо по-іншому. Якщо колір вершини, в яку ми прийшли та колір алфавіту до якого відноситься літера співпали, то ставимо у відповідність попередню літеру цього ж підалфавіту.

Означення 9. Позначимо $\hat{\Omega}_1 = \{x_i : i \equiv 0(mod 2), 1 \leq i \leq n, x_i \in X\}$, тобто літери з непарними номерами позицій в алфавіті X, $\hat{\Omega}_2 = \{x_i : i \equiv 1(mod 2), 1 \leq i \leq n, x_i \in X\}$.

Теорема 1. *Бінарне нескінченне дерево* $\Gamma(0,1)$ *визначає шифр 2-зсув (зсув на 2 позиції), якщо з кожної вершини* i*-го рівня* $i \in \mathbb{N} \bigcup 0$ *виходить лише одна нескінченна геодезична, в якій всі вершини і ребра зафабовані в колір* 0 *і лише одна нескінченна геодезична в якій всі вершини і ребра зафабовані в колір* 1 *та має місце розбиття* $X : X = \hat{\Omega}_1 \bigcup \hat{\Omega}_2$.

Доведення. З процесу дешифрування по $\Gamma(0,1)$ випливає: за умовою на $\Gamma(0,1)$ існує однокольорова геодизична, стартуючи з довільної вершини і рухаючись по такій геодезичній, ми для довільної літери не будемо виходити за межі підалфавіту, до якого вона відноситься, тобто рухаючись по кольору 0 або 1, ми прийдемо в вершину кольору 0 або 1 відповідно. Отже, ми будемо ставити у відповідність наступну літеру цього ж підалфавіту, яка має номер в алфавіті X на 2 більший. □

Модернізація графа $\Gamma(0,1)$: проіндексуємо кожну позицію блоку, тобто поставимо у відповідність деяке число $l_i \in \mathbb{N}$ відмінне від нуля. Отримаємо послідовність $\{l_1, l_2, \ldots, l_M\}, M \leq n$. Процес шифрування залишається тим же, але для кожної літери, що знаходиться на i-му місці в блоці, ми спускаємось по дереву не на один, а на l_i рівнів, при цьому отримаємо літеру з номером в X більшим на $2l_i$.

Розглянемо узагальнений підхід тут розфарбування графа довільне і теж є ключем. Наступну процедуру шифрування називатимемо $\Gamma(0,1)$-шифром для розбиття алфавіту $X = \sqcup_{i=1}^{t} X_i$, асоційованого з підстановкою π індексів множин розбиття алфавіту. Введемо відповідність між підалфавітами алфавіту X і кольорами:

$$X_i \longleftrightarrow C_i,$$

де під C_i маємо на увазі колір відповідного підалфавіту, також позначимо $C(v_i)$ — колір вершини v_i з Γ. Нехай $x_1 x_2 \ldots$ — блок відкритого тексту для шифрування. Розглянемо випадки:

Тип 1. Якщо $x_i \in X_j$, то до x_i застосовуємо шифр зсуву на k_j позицій в блоці X_j. Тоді компонентами ключа є: $X = \sqcup_{i=1}^{t} X_i$, та k_i — відповідні величини зсувів в підалфавітах X_i, $X_i = \{\sigma_{i_1}, \sigma_{i_2}, \ldots\}$. Шифрування: нехай

$x_i \in X_j$, позначимо його $x_i = \sigma_{j_q}$, $q < |X_j|$, як символ з j-го блоку, де діє зсув на k_j символів, тоді $E(x_i) = \sigma_{j_{q+k_j} mod|X_j|}$. Якщо $X = \{a, b, c, ...\} \cup \{b, d, f, ...\}$, де k_j всі однакові, то це зсув на k_j.

Оцінимо величину простору ключів. Вона складається з кількості способів впорядкування і розбиття X на t блоків. Впрорядкувань є $n!$, крім того є C_{n-1}^{t-1} розбиттів алфавіту (хоча тут враховані не рівновеликі блоки), кількість розфарбувань вершин $2^n - 1$. Зсув можна вибрати $|X_i| - 1$ способами в i-ому блоці. Отже, простір всіх ключів зсуву містить $n! \prod_{i=1}^{t}(|X_i| - 1)$ можливостей вибору. Відмітимо, що для шифру підстановки на блоках вони повинні бути рівновеликі, тому надалі $|X_i| = [\frac{n}{t}] + 1$, інакше треба вносити додаткову інформацію, щоб відновити підстановку. Компонентом простору ключів також є вибір точної дії групи підстановок на множині $\mathbb{N}_n$. Тоді, якщо обмежитись дією спряження і φ-спряження, то кількість різних дій може бути оцінена знизу, кількістю дій (відображень), які дають різні набори класів $\mathfrak{R}(\Psi)$, де $\Psi : X \to X$, тобто класів Рademайстера в S_n на $\mathbb{N}_n$. Кількість таких підкручених спряжень, при фіксованому елементі g, що діє звичайним спряженням (коли немає підкрутки) і є компонентом ключової послідовності, випливає з $y = gxhg^{-1}h^{-1} = gx\varphi(g^{-1})$, визначається кількістю h, який можна вибрати $n!$ способами. Вкажемо існування взаємнооднозначної відповідності між елементами класів спряженості і підкрученої спряженості: маємо $y = gxhg^{-1}h^{-1}$ звідси $yh = gxhg^{-1}$, $yh = g(xh)g^{-1}$. Елементи yh і xh спряжені. Домноження x на h і є цим взаємно-однозначним перетворенням, що встановлює відповідність і задає нову циклову структуру класу подвійної спряженості.

Для розсіювання вибираємо поліалфавіт X_0, який є більшим ніж мінімально потрібний алфавіт X і застовуємо до кожного символа шифр багатозначної заміни (пропорційної заміни) Гауса, де образом x_i є множина символів (множина шифропозначень данного символа), величина якої пропорційна частоті появи x_i [10]. Це дасть розсіювання. Зауважимо, що $|X_0|$ має бути такою, щоб дія групи на X_0 була точною.

Тип 2. Якщо у $X_j \leftrightarrow k_j(\sigma_{j_s})$, k_j всі однакові і не виходимо за межі X_j, то це шифр циклічної підстановки степеня $[\frac{n}{t}] + 1$ або просто зсув не більше ніж на $[\frac{n}{t}] + 1$ символів, інакше це поліалфавітний шифр.

Тип 3. Перетворення-підстановка з областями імпримітивності — X_j, $1 \le j \le t$, де усі X_j рівновеликі за потужністю, помітимо, що фактично

$$\pi = \begin{pmatrix} X_1, & \dots & X_j, & \dots & X_t \\ X_{q_1}, & \dots & X_{q_j}, & \dots & X_{q_t} \end{pmatrix},$$

такі підстановки утворюють групу, яка діє імпримітивно.

Цю підстановку зручно записувати так:

$\pi = \begin{pmatrix} 1, 2, & \dots & j, & \dots & t \\ q_1, q_2, & \dots & q_j, & \dots & q_t \end{pmatrix}$

перетворення $\sigma_{j_s} \longleftrightarrow k(\sigma_{j_s})$.

Перетворення, що задає шифрування:

$$E(\sigma_{j_s}) = \sigma_{(q_j)_{s+k(\sigma_{j_s}(mod|X_{q_j}|))}}.$$

Частковим випадком є $k(\sigma_{j_s}) = 0$, тоді це шифр підстановки. У випадку, коли $k(\sigma_{j_s}) \neq 0$, $k(\sigma_{j_s}) = k$ всі однакові, то це добуток шифру підстановки та шифру зсуву на k позицій.

Тип 4: У випадку шифру Віженера π є циклом довжини t, при цьому всі X_i є рінопотужними, як і в попередньому випадку $\sigma_{j_s} \to k(\sigma_{j_s})$.

Перетворення, що задає шифрування:

$$E(\sigma_{j_s}) = \sigma_{(j_s)_{s+k_j(mod|\pi^{k_j}X_j|))}}.$$

3. Алфавіт X розбиваємо на

$$X = \sqcup_{i=1}^{t} X_i$$

Впорядкуємо букви підалфавіту X_i згідно з їх порядком у алфавіті X. Номером букви $x \in X_i$ є номер позиції цієї літери в такому розміщенні і позначимо $n_i(x)$. Тоді величина $|X_i|$ дорівнює номеру останньої букви у впорядкуванні літер з X_i. Символом $n_X(x)$ позначимо номер позиції x в усьому алфавіті X.

Надалі вважатимемо, що у диз'юнктному розбитті алфавіту всі літери множин X_i впорядковані саме за таким правилом. Для $x \in X_i$ символом $\pi(x)$ позначимо букву із множини $\pi(X_i)$ номер якої дорівнює номеру літери x в X_i, тобто $n_i(x) = n_{\pi(X_i)}(\pi(x))$, або мовою алгебри, це образ елемента після дії підстановки $\pi(X_i)$, заданої на X_i.

Означення 10. Властивістю перемішування називається перетворення, де кожний символ шифро-тексту залежить від кожного символа відкритого текста і від кожного символа ключа для симетричного шифра (закритого ключа для асиметричного текста).

Означення 11. Нехай E_1, $E_2(x)\ldots$ — шифри зсуву такі, що E_1 це зсув на $\alpha(x)$, $E_2(x_1)$ це зсув на $\alpha_2(x_1, x_2)$ і т.д. Тоді вінцевим добутком цих шифрів називатимемо результат такого процесу шифрування: нехай $(x_1, ...)$ — буквенне повідомлення у алфавіті X; позначатимемо $(x_1, ...)^E$ — результат виконання процедури E до набору $(x_1, ...)$, аналогічно y^{E_i} — результат виконання процедури E_i до y, де i це номер раундового перетворення шифрування, тобто

$$(x_1, ...)^{[E_1,E_2,...]} = (x_1, ...)^E = (x_1^{E_1}, x_2^{E_2(x_1^{E_1})}, \ldots).$$

Це перетворення має структуру словарного автоморфізма [9], образ x_n залежить від образу усього кортежу з попередніх символів, тобто від: $x_n^{(x_1,\ldots,x_{n-1})^{E_{n-1}}} = x_n^{(x_1,\ldots,x_{n-1})g}$, де $(x_1, ..., x_{n-1}) = u \in X^{n-1}$. Позначимо $\overline{x}_n = (x_1, ..., x_{n-1})$. Для автоморфізма f і вершини $u \in X^*$ маємо новий автоморфізм $(u)f$, що називається секцією автоморфізма f у вершині u і однозначно задається рівнянням $(ux_n)^f = (u)^f(x_n)^{(u)f}$, $f \in G(\Lambda)$ або у запису через дію групи на підслові з префіксом $u \in X^{n-1}$ це $f(\overline{x}_n) = (f(x_1)f|_{x_1}(x_2), \ldots, f|_{x_1x_2\ldots x_{n_1}}(x_n))$. Якщо при цьому для $\forall u, u{\in}X^*$,

$\forall f \in G$ виконується $(u)f \in G$, то G самоподібна і автомат $\Lambda(G)$, що їй відповідає є скінченним. Побудований автомат Λ є обертовним, бо в кожному стані він виконує обертовне перетворення над прочитаною літерою x_i, це так оскільки у вершинах графа в процесі шифрування застосовуються лише зсуви та підстановки.

З метою класифікації зазначимо, якщо для $\forall i \in \mathbb{N}$ маємо $E(\overline{x}_{i-1}) = \alpha_i = \alpha(\overline{x}_{i-1})$, то такий вінцевий добуток називатимемо композицію шифрів, яка реалізує конструкцію вінцевого степеня, $E_1, E_2(x_1), ..., E_{i-1}(x_1, ..., x_{i-2})$. Частковим випадком вінцевого добутку є $\Gamma(0,1)$-шифр.

Зауважимо, що при дії на k-ту букву функція виходу $\lambda(\overline{x}, g)=\lambda(\overline{x}_i\omega_i, v_i)= = x_n^{(x_1,x_2,...,x_{n-1})g}$ автомата Λ, який відповідає цій групі $G(\Lambda)$, залежить лише від попередніх літер і від стану, тому вона не зміниться при заміні наступних після неї літер. Якщо на кожній ітерації фіксувати префікс $u \in X^k, k < n$ і брати різні продовження з $v_i \in X^*$, то неважко знайти оператор такого автоматного перетворення склавши систему рівнянь $uv_i = c(ux_i) = c(u)c_u(x_i)$, $x_i \in X$. Зокрема якщо брати кожний раз меншу частину префікса u, то система матиме матрицю трикутного вигляду, яка може бути легко розв'язана і тим самим оператор, що задає автоматне перетворення у цьому стані знайдено. Для уникнення властивості префіксності реалізуємо перемішування шляхом спряження перетворення ширування $c(X^n)$ цілого блока з X^n, щоб префікс шифру як і кожне символ залежав від символів усього блока відкритого тексту $u \in X^n$. Для цього пригадаємо, що автоматній групі $G(\Lambda) < AutX^\omega$ відповідає група автоморфізмів, які діють на словах: $(ux_n)^f = (u)^f(x_n)^{(u)f}, f \in G$ володіючи властивістю префіксності, скінченна $G(\Lambda)$ може бути задана вінцевою рекурсією $f_i = (f_{i0}f_{i1}...f_{id-1})\sigma_i$.

Спрягаючи автоморфізми $f \in G(\Lambda)$, що діють на словах з X^n і які мають вигляд: $f(x_1, \ldots, x_n) = (f(x_1)f|_{x_1}(x_2)f|_{x_1x_2}(x_3), \ldots, f|_{x_1x_2...x_{n_1}}(x_n))$, з цієї групи досягнемо потрібного перемішування. Але слід врахувати, що спряження слід робити не одним і тим самим елементом g для усіх $x_n^{(x_1,...,x_{n-1})f}$ а вибрати обертове перетворення $g \in G(\Lambda)$, тоді перетворення прийме вигляд

$$\phi(\overline{x}_n) = g^{-1}(\overline{x}_n)f(x_1, x_2, \ldots, x_n)g(\overline{x}_n)$$

Таким чином отримаємо автоморфізм $\phi(\overrightarrow{x_n})$, який вже не має властивості префіксності завдяки принципу перемішування і великому порядку групи $G(\Lambda)$ твірними якої є автоморфізми з $AutX^\omega$, важливо також щоб перетворення $g(\overrightarrow{x_n})$ не потрапляло в просту підгрупу скінченнозаданої групи бо там проблема слів а значить і проблема спряженості є розв'язною.

Зрозуміло, що вибір таких компонентів ключа як розбиття алфавіту і простої поліалфавітної підстановки $x \to y, n_i(x) = n_j(y), x \in X_i, y \in X_j$, яка діє у випадку не співпадіння кольорів, перетворення E_n як словарного автоморфізму, впливає на результат — весь шифротекст завдяки цьому маєм гарне перемішування [1, 5]. При цьому проста підстановка, при якій

$n_i(x) = n_j(y)$ легко узагальнюється до $n_i(x) \neq n_j(y), 0 < i, j < \frac{n}{t}$. Для зручності позначатимемо $k(\sigma_{q_s})$ як $k_{\sigma_{q_s}}$. Перемішування задаємо нелінійним алгебраїчним перетворенням — підстановками і зсувами.

Довготерміновим ключем є розбиття на підалфавіти, група, яка діє підстановками на літерах і розфарбування вершин, яке можна зробити $2^{n+1}-1$ способами. Раундовим ключем є підстанока, яка обчислюється через дію композиції групових перетворень, або відповідна величина зсуву, яка також визначається в залежності від літери і підалфавіту. У випадку поліалфавітного розбиття на t алфавітів маємо $n!$ відповідних впорядкувань і підстановки рангу $[n/t]+1$. Потужність простору ключів визначається кількістю зсувів з композиції шифрів $E_1, E_2(x_1), E_3(x_1, x_2), \ldots, E_n(x_1, \ldots, x_{n-1})$.

Образ довільного $x \in X_i$ позначимо $\pi(x)$, літерою з множини $\pi(X_i)$, номер якої дорівнює номеру x як букви із X_i, тобто це образ $x \in X_i$ при дії підстановки $\pi(X_i)$ і тому $n_i(x) = n_{\pi(X_i)(\pi(x))}$.

Теорема 2. *Вінцевий добуток шифрів* $E_1, E_2(x_1), E_3(x_1, x_2), \ldots, E_n(x_1, \ldots, x_{n-1})$ *є шифром типу* $\Gamma(0,1)$ *для розбиття алфавіту* $X = \sqcup_{i=1}^{t} X_i$ *асоційованого з підстановкою на областях імпримітивності* X_i

$$\pi = \begin{pmatrix} X_1, & \ldots & X_j, & \ldots & X_t \\ X_{q_1}, & \ldots & X_{q_j}, & \ldots & X_{q_t} \end{pmatrix},$$

які є елементами диз'юнктного розбиття алфавіту X *тобто множинами* $X_1, \ldots, X_t$. *Частковим випадком цього шифру є шифр на* $\Gamma(0,1)$.

Образ рекурсивно визначається через усі попередні символи і елементи групи: $\alpha_2(x_1, x_2) = k(\pi(x_2) + \alpha_1(x_1)), \ldots,$

$\alpha_\beta(x_1, ..., x_\beta) = \sum_{i=1}^{\beta_k} (\pi(x_i) + \alpha_{i-1}(x_1, ..., x_{i-1}))$, *з початковою умовою* $\alpha_0 = 0$.

Доведення. Легко бачити, що $x_1^{E_1} = x_1 + k_{\sigma_{q_s}}$ (позначаємо $x_{1+k_{\sigma_{q_s}}}$ як $x_1 + k_{\sigma_{q_s}}$), тому $\alpha_1(x_1) = k(\sigma_{q_s})$, де $s = n_1(x_1)$, $(x_1, x_2)[E_1, E_2] = (x_1^{E_1}, x_2^{E_2(x_1^{E_1})}) =$ $= (x_1 + k_{\sigma_{q_s}}, \pi(x_2) + k_{\sigma_{q_s}})$, $\sigma_q = \pi(x_2) + \alpha_1(x_1)$, $\pi(X_{q_1}) = X_q$, бо $\pi(q_1) = q$. Тому

$$\alpha_2(x_1, x_2) = k(\pi(x_2) + \alpha_1(x_1)).$$

Ітеруючи цей процес, нарешті отримаємо

$$(x_\beta)_{\beta\in\mathbb{N}}^{E_1, E_2, \ldots} = (x_\beta)_{\beta\in\mathbb{N}}^{E_\beta(x_1^{E_1}, \ldots, x_{\beta-1}^{E_{\beta-1}(x_1, \ldots, x_{\beta-2})})} = (\pi(x_\beta) + k_{\sigma_{q_s}}),$$

де $\sigma_q = \pi(x_\beta) + \alpha_{(\beta-1)}(x_1, \ldots x_{\beta-1})$. □

Зауважимо, що закон перетворення шифрування це залежність, яка забезпечує гарне перемішування та високу імітостійкість. Залежність має вигляд $C(v_i) = f(\vec{x}_{i-1}, C(v_{i-1}))$, де $1 \leq i \leq n$, x_i — i-ий символ відкритого тексту, c_i — i-ий символ шифротексту, $\vec{x}_{i-1} = (x_1, x_2, ..., x_{i-1})$, $\vec{v}_{i-1} = (v_1, v_2, ..., v_{i-1})$, причому $c_i = F(\vec{x}_i, E_1, E_2, ..., E_{i-1}, \pi_1, ..., \pi_{i-1}, C(\vec{v}_{i-1}))$.

Твердження 1. *Довільний* $\Gamma(0,1)$ *шифр для розбиття алфавіту* $X = \sqcup_{i=1}^{t} X_i$ *асоційованого з підстановкою* π *буде вінцевим добутком шифру зсуву* E_1 *на* $k_{\sigma_{q_s}}$ *позицій, що застосовується до* $\pi(x_1)$, *шифру зсуву*

$E_2(x_1)$ на $k_{\sigma_{q_{s_2}}}$ позицій, що застосовується до $\pi(x_2)$, і т.д., для шифру зсуву $E_\beta(x_1, ..., x_{\beta-1})$ на $k_{\sigma_{q_{s_\beta}}}$ позицій, що застосовується до $\pi(x_\beta)$.

Доведення. Розглянемо деякі шифри зсуву $E_1, E_2(x_1) \ldots$ на $\alpha_1(x_1)$ $\alpha_1(x_1, x_2)$ позицій відповідно. Виразивши $k(\sigma_q)$ через $\alpha_1(x_1)$, отримаємо шифр типу 3, який задовольняє умови твердження. □

Наслідок 3. Нехай $\Gamma(0,1)$ — шифр для розбиття алфавіту $X = \sqcup_{i=1}^{t} X_i$, де $X_1 = \{x \in X : n_X(x) \equiv 1(mod 2)\}$ і $X_2 = \{x \in X : n_X(x) \equiv 0(mod 2)\}$, тобто номер символа x в X є парним числом, асоційованим з транспозицією $(1,2)$ і буде вінцевим добутком шифрів зсуву E_1, $E_2(x_1)$, де E_1 є шифром зсуву на 1-ну позицію, $E_2(x_1)$ — на 2 позиції.

Теорема 3. *Застосування операції вінцевого добутку до перетворень, які є поліалфавітними шифрами, дає поліалфавітний шифр.*

Доведення. Виходячи з означення поліалфавітного шифру (це шифр, що ставить у відповідність кожній літері повідомлення літеру з певної множини за наперед визначеним правилом), ми маємо, що при вінцевому добутку кожній літері повідомлення ставиться у відповідність літера з певної множини за наперед визначеним правилом, яке залежить від типу шифра. □

Теорема 4. *Алгоритм шифрування для вінцевого добутку шифрів E_1 та $E_2(x_1)$ є вінцевим добутком алгоритмів шифрування.*

Доведення. У нашому випадку кожна i-та літера блоку X шифрується з допомогою деякого поліалфавітного шифру, причому кожен з цих шифрів має свій алгоритм (зсуву, підстановки або їх суперпозиції). Ці алгоритми можуть повторюватися і результат наступного рекурсивно залежить від дії на його аргумент попереднього перетворення. Тому при шифруванні таким способом ми отримуємо для наших алгоритмів конструкцію вінцевого добутку, що була описана вище. А тому загальний алгоритм буде вінцевим добутком алгоритмів. Порядок групи, яка йому відповідає і сама є вінцевим добутком групових перетворень циклічних зсувів $(x_\beta)_{\beta\in\mathbb{N}}^{E_1,E_2,\ldots}$, експоненційно зростає з ростом β, що забезпечує стійкість до перебору. □

Теорема 5. *Обчислювальна складність повного перебору для алгоритму шифрування на розфарбованому графі $\Gamma(0,1)$ оцінюється як $O(2^{n+1})$.*

Доведення. Нехай ми маємо повідомлення довжини n. Тоді процес шифрування (дешифрування) цього повідомлення нашою криптосистемою полягая в наступному. На першому кроці ми вибираємо один з двох напрямів руху, на другому кроці перед нами постає вибір з чотирьох шляхів, бо маємо 2^2 гілок, на третьому ще більше — вісім шляхів (2^3),..., на n-тому кроці — 2^n шляхів. Таким чином, на кожному k-ому кроці, у найгіршому випадку, ми маємо перевірити 2^k шляхів. Тому загальна кількість операцій які ми робимо, буде дорівнювати $2+4+8+... = 2^1+2^2+2^3+... = \sum_{k=1}^{k=n} 2^k = 2^{n+1}-2$. Таким чином, за означенням оракула O-великого, складність алгоритму буде дорівнювати $O(2^{n+1})$. □

1. Висновок.

В роботі ефективно використаний добуток двох шифрів, один з яких є поліалфавітним. Доведена висока стійкість до прямого підбору ключа. Вдосконалено метод поліалфавитного шифрування буквенного текста з використанням ключового слова, яке у шифрі Віженера використовувало шифрувальний шаблон, тепер же зі зміною кольору ребра графа змінюється величина зсуву та алфавіт. Залежність для обчислення шифрованого тексту задається складною груповою конструкцією, де рекурсивно обчислюється відповідна підстановка на символах алфавіту. Для розсіювання, яке не забезпечується підстановками і зсувами, застосовано шифр багатозначної заміни, зокрема пропорціойної заміни на більшому алфавіті. Можливим шляхом вдосконалення шифру є урізноманітнення методів вибору розподільника підстановок для шифровеличин [7] та переобчислення розфарбування C вершин $AutX^*$ як раундового ключа для кожного блоку X^n.

Література

1. Бабаш А. В., Шанкин Г. П. Криптография. — М., Солон-Р, 2002. — 511 с.
2. Василенко О. Н. Теоретико-числовые алгоритмы в криптографии. — М.: МЦНМО, 2003. — 328 с.
3. Вербицкий О. В. Вступление в криптологию. — Львов: Издательство научно-техничной литературы. 2005. — 300 с.
4. Douglas Lind, Brian Marcus. An introduction to symbolic dynamics and coding. — Cambridge University Press, 1995. — 490 p.
5. N. Koblitz. Algebraic aspects of cryptography. Vol. 3, Algorithms and Computation in Mathematics. — Springer-Verlag, Berlin, 2004. — 207 p.
6. Диффи У. Первые десять лет криптографии с открытым ключом // Труды института инженеров по электронике и радиотехнике. — 1988. — Т. 76, № 5. — С. 54–74.
7. Барычев С. В. Криптография без секретов. — М.: Наука. — 1998. — 120 с.
8. Задирака В. К., Олексюк О. А. Компьютерная арифметика многоразрядных чисел. — Тернопіль: Вища Школа, 2003. — 502 с.
9. Laurent Bartholdi, Rostislav I. Grigorchuk. Branch Groups. Handbook of algebra, V. 3. — North-Holland, Amsterdam, 2005. — P. 989–1112.
10. Wagner D. X. Generalized birthday problem // CRYPTO'02. Lect. Notes Comput. Sci. — 2002. — V. 2442. — P. 288–303.

Факультет кібернетики, Київський національний університет імені Тараса Шевченка, вул. Володимирська, 64, Київ, 01601, Україна.

Надійшла 01.02.2014