УДК 004.021:056.55, 004.27

Білецький А.Я., Білецький О.А., Кандиба Р.Ю.
Національний авіаційний університет

Матричні аналоги протоколу Діффі-Хеллмана

Given by the comparative analysis of the effectiveness matrix of the known matrix protocols of secret encryption keys to open channels of communication. Proposed the new protocol, witch based on the use of irreducible polynomials and primitive matrices Galois and Fibonacci.

Keywords - protocol, encryption keys, irreducible polynomials, Galois matrix.

У статті наведено порівняльний аналіз відомих матричних протоколів передачі секретних ключів шифрування по відкритих каналах зв'язку. Запропоновані нові протоколи, що засновані на використанні незвідних поліномів та примітивних матрицях Галуа і Фібоначчі.

Ключові слова - протокол, ключі шифрування, незвідні поліноми, матриці Галуа.

Вступ

Опублікування в 1976 році Уітфілдом Діффі та Мартіном Хеллманом (Whitfield Diffie and Martin E. Hellman) статті «New Directions in Cryptography» [1] ознаменувало собою відкриття нового напряму в криптографії — *асиметричної криптографії*. Алгоритм Діффі-Хеллмана (DH) дозволяв двом абонентам комп'ютерної мережі (Алісі та Бобу) отримувати загальний секретний ключ шифрування K, використовуючи незахищений від прослуховування, але захищений від підміни відкритий канал зв'язку.

DH- алгоритм передбачає, що Алісі і Бобу відомі відкриті ключі p та q, причому $p-$ просте число, а $q-$утворюючий елемент. Абонент Аліса генерує випадкове велике число a, обчислює значення $A=q^a \bmod p$ и надсилає його Бобу. В свою чергу Боб генерує випадкове велике число b, обчислює значення $B=q^b \bmod p$ и надсилає його Алісі. Далі абонент Аліса піднесіть отримане від Боба число B в свою випадкову ступінь a і обчислює значення $K_a=B^a \bmod p=q^{ba} \bmod p$. Аналогічно поступає Боб, обчислюючи $K_b=A^b \bmod p=q^{ab} \bmod p$. Очевидно, що обидва абоненти отримують одне і теж число K, тому як $K_a \equiv K_b$. Це число K Аліса і Боб могут використовувати як секретний ключ, наприклад, для симетричного шифрування. Справа в тому, що супротивник, якій можливо перехопив числа A і B, зустрінеться з проблемою, яка є практично нерозв'язною, якщо числа a і b були обрані достатньо великими.

Головній недолік протоколу DH полягає в тому, що він не захищений від отакі «людина посередині». Тому в наступні роки були запропоновані інші варіанти протоколів, серед яких відзначимо так звані *матричні аналоги* алгоритму Діффі-Хеллмана. В статті наведено порівняльний аналіз відомих матричних аналогів протоколу Діффі-Хеллмана, а саме, алгоритмів Єроша-Скуратова [2], Мегрелішвілі [3] та *альтернативних алгоритмів* обміну таємними ключами шифрування по відкритих каналах зв'язку, що побудовано на основі незвідних поліномів та примітивних матрицях Галуа або Фібоначчі, пояснення до яких надано далі в тексті.

Протокол Ероша-Скуратова

Для обміну секретними ключами в системі автори пропонують використовувати протокол DH в циклічній групі матриць $\langle M \rangle$, причому матриця M вважається загальнодоступною.

Передбачається, що абонент A (Аліса) виробляє випадковий показник x, обчислює матрицю M^x і надсилає її абоненту B. В свою чергу абонент B (Боб) виробляє випадковий показник y, обчислює матрицю M^y та надсилає її абоненту A. Далі обидва абоненти підносять матриці, що отримані, у свої степені та обчислюють загальну матрицю (ключ шифрування) $M^{yx} = M^{xy}$. Тому як порядок матриць M, що пропонується, мусить бути не менш ніж 100, то злом ключа, як стверджують автори (доречи, без доказу), має перебірну складність. Разом з тим в [4] наведено, що протокол Єроша-Скуратова легко може бути зламаний за допомогою узагальненої китайської теореми о залишках.

Протокол Мегрелішвілі

Сутність даного протоколу [3] зводиться до наступного. В якості відкритих ключів приймаються двійковий вектор ініціалізації V і примітивна матриця M. *Примітивною* будемо називати таку двійкову матрицю $n-$го порядку, послідовні степені якої в кільці залишків за $\mathrm{mod}\,2$ утворюють абелеву мультиплікативну групу ($m-$послідовність) порядку $L_n = 2^n - 1$. Абонент A виробляє випадковий показник x, обчислює вектор $V_a = V \cdot M^x$ і надсилає його абоненту B. В свою чергу абонент B виробляє випадковий показник y, обчислює вектор $V_b = V \cdot M^y$ та надсилає його абоненту A. Далі Аліса обчислює ключ $K_a = V_b \cdot M^x = V \cdot M^{y+x}$, а Боб – ключ $K_b = V_a \cdot M^y = V \cdot M^{x+y}$. Цілком зрозуміло, що по завершенню протоколу обміну даними обидва абоненти отримують однакові таємні ключі K, тому як $K_a \equiv K_b = K$.

Алгоритм формування матриць M в протоколі Мегрелішвілі достатньо простий і може бути пояснений наступною схемою обчислень:

$$M_1 = 1, \quad M_3 = \begin{bmatrix} 1 & 0 & 1 \\ 1 & 1 & 0 \\ 0 & 1 & 0 \end{bmatrix}, \quad M_5 = \begin{bmatrix} 1 & 0 & 1 & 0 & 1 \\ 1 & & & & 0 \\ 0 & & M_3 & & 1 \\ 1 & & & & 0 \\ 0 & 1 & 0 & 1 & 0 \end{bmatrix}, \quad \ldots \tag{1}$$

Як випливає з (1), матриці M є матрицями виключно непарного порядку, що може стати значною перешкодою щодо їх використання в криптографії. Вказаний недолік протоколу був усунутий за рахунок використання матриць M довільного порядку [5], що синтезуються на основі так званих узагальнених перетворень Грея [6], сутність яких зводиться до наступного.

Матрична форма прямих (для простоти позначимо їх цифрою 2) і зворотних (які позначимо цифрою 3) класичних перетворень (кодів) Грея представимо (обравши порядок матриць n, що дорівнює чотирьом) у вигляді:

$$2 := \begin{bmatrix} 1 & 1 & 0 & 0 \\ 0 & 1 & 1 & 0 \\ 0 & 0 & 1 & 1 \\ 0 & 0 & 0 & 1 \end{bmatrix}; \qquad 3 := \begin{bmatrix} 1 & 1 & 1 & 1 \\ 0 & 1 & 1 & 1 \\ 0 & 0 & 1 & 1 \\ 0 & 0 & 0 & 1 \end{bmatrix}; \tag{2}$$

Матрицям (2), які назвемо *матрицями лівостороннього перетворення Грея*, поставимо у відповідність *матриці правостороннього перетворення Грея*, що визначаються співвідношеннями:

$$4 := 121 = 2^T; \qquad 5 := 131 = 3^T, \tag{3}$$

де

$$1:=\begin{bmatrix}0 & 0 & 0 & 1\\ 0 & 0 & 1 & 0\\ 0 & 1 & 0 & 0\\ 1 & 0 & 0 & 0\end{bmatrix}, \qquad (4)$$

є матриця (оператор) інверсної перестановки.

Сукупність операторів (2)-(4) разом з оператором 0 або e (одиничною матрицею) утворюють повну групу *простих операторів (кодів) Грея* (табл. 1).

Таблиця 1.

Множина простих кодів Грея

Позначення оператора	Операція, що виконується
e (або 0)	Збереження вихідної комбінації
1	Інверсна перестановка
2	Пряме кодування по Грею лівостороннє
3	Зворотне кодування по Грею лівостороннє
4	Пряме кодування по Грею правостороннє
5	Зворотне кодування по Грею правостороннє

З елементів такої групи можливо сформувати так звані *складові коди Грея* (СКГ), що утворюються добутком простих (елементарних) кодів. Як приклад можна побачити СКГ 121 або 141, що наведені в формулах (3).

Як прості, так і складові коди Грея мають ряд особливих властивостей. По-перше, матриці, що їм відповідають, невироджені й тому виявляються зворотними. По-друге, існують достатньо прості алгоритми обернення СКГ. І, нарешті, по-третє, існують такі СКГ «криптографічного порядку», якім притаманні властивості примітивності. Приклади таких кодів наведено у табл. 2.

Таблиця 2.

Складові коди Грея, які завдають двійковим матрицям властивості примітивності

Порядок матриці (n)			
32	64	128	256
2244424	22533435	2425535	22533435
2442224	22534335	2433534	22534335
12242253	24334225	2435334	24334225
12242443	25224334	22524224	25224334
12252242	222524424	22533334	2222535224

Нехай M є примітивна двійкова матриця, що породжена СКГ G. Відносно таких матриць можна легко доказати (методом безпосередньої перевірки) наступне:

Твердження. *Примітивність матриць M інваріантна до групи лінійних перетворень* Ω *над СКГ G, що утворюють матриці M, і перетворень подібності* П *над цими матрицями.*

До складу Ω-групи входять оператори: циклічного зсуву, обернення, інверсії і сполучення, а також довільні комбінації цих операторів. Перетворенням П формується матриця M_p, подібна до M, яка визначається співвідношенням

$$M_p = P \cdot M \cdot P^{-1},$$

де P – матриця перестановки.

Коротко пояснимо суть перетворень, що входять у вище позначену Ω-групу. Введемо (табл. 3) символіку для операторів, що належать цій групі.

Таблиця 3.

Символічне позначення операторів Ω-перетворень

Позначення оператора	Тип перетворення
$\vec{1}_k$, $\overleftarrow{1}_k$	Циклічний зсув
2	Обернення
3	Інверсія
4	Сполучення

Стрілки оператора циклічного зсуву вказують напрямок прокрутки СКГ G, а нижній індекс k визначає число розрядів зсуву. Наприклад, $\overleftarrow{1}_3$ означає, що СКГ піддається циклічному прокручуванні за годинниковою стрілкою на три розряди (символи) коду. Якщо G – простий або складений оператор Грея, то перетворення над G будемо записувати у загальному вигляді як $P\{G\}$. Наприклад, $P = 3$, або $P = 2 \cdot \vec{1}_2$ та ін.

Альтернативні протоколи

В даному розділі пропонуються два варіанти альтернативних матричних протоколів обміну секретними ключами по відкритих каналах зв'язку. Процедура формування ключа шифрування K в *першому варіанті протоколу* засновується на використанні двох відкритих та по одному закритому ключу в обох абонентах мережі. В якості відкритих ключів обирають двійковий вектор ініціалізації V n – го порядку і довільний незвідний поліном (НП) φ_n ступеня n. Закритими ключами являються примітивні (утворюючі) елементи ω поля Галуа $GF(2^n)$ над НП φ_n, на основі яких абоненти Аліса і Боб формують примітивні секретні матриці перетворень G_{φ_n, ω_a} і G_{φ_n, ω_b} відповідно. Елемент ω поля $GF(2^n)$ примітивний над НП φ_n, якщо мінімальний показник e, при якому $(\omega^e \equiv 1) \bmod \varphi_n$, приймає значення $e = 2^n - 1$.

Алгоритм синтезу матриць $G_{\varphi, \omega}$, які будемо називати *матрицями Галуа*, пояснимо на числовому прикладі. Нехай НП $\varphi_8 = 100101101$, а утворюючий елемент (УЕ) абонента Аліса $\omega_a = 111$. Отримуємо

$$A = G_a = \begin{bmatrix} 1 & 1 & 1 & 1 & 0 & 1 & 1 & 1 \\ 1 & 1 & 1 & 0 & 1 & 1 & 0 & 1 \\ 1 & 1 & 1 & 0 & 0 & 0 & 0 & 0 \\ 0 & 1 & 1 & 1 & 0 & 0 & 0 & 0 \\ 0 & 0 & 1 & 1 & 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 & 1 & 1 & 0 & 0 \\ 0 & 0 & 0 & 0 & 1 & 1 & 1 & 0 \\ 0 & 0 & 0 & 0 & 0 & 1 & 1 & 1 \end{bmatrix}. \qquad (5)$$

Згідно з (5), заповнення матриці G_a відбувається за такою схемою. Спочатку УЕ ω_a розміщується в нижньому рядку матриці. Елементи цього рядка матриці, що розташовані зліва від елементів УЕ, заповнюються нулями. Наступні рядки матриці (за напрямом знизу вгору) утворюються зсувом попередніх рядків. Якщо при цьому лівий елемент рядка, що зсувається, дорівнює 0, то виконується циклічний зсув на один розряд вліво (кругова прокрутка за годинниковою стрілкою). В тому випадку, коли лівий елемент рядка, що зсувається, дорівнює 1, то

виконується звичайний зсув рядка на один розряд вліво, а в правий елемент рядка, який звільняється, записується 0. Розрядність подібних рядків стають на одиницю більше порядку матриці. Вектори, які відповідають таким рядкам, приводяться до залишку за модулем НП φ_n, що повертає їм розрядність, яка співпадає з порядком матриці n. Аналогічним чином формує матрицю Галуа $B = G_b$ абонент Боб, використовуючи при цьому свій примітивний УЕ ω_b.

Матрицям Галуа, що введені, притаманні деякі цікаві властивості. По-перше, добуток матриць комутативний, тобто $A \cdot B = B \cdot A$. В той же час, по-друге, якщо хоча б один з УЕ не являється примітивним елементом поля Галуа над НП φ_n, то властивість комутативності матриць A і B втрачається. І, нарешті, по-третє, якщо, наприклад, піднести деяку матрицю G_a, що утворена на основі УЕ ω_a, до ступеня x (операція виконується в кільці залишків за $\bmod 2$), то це буде відповідати створенню примітивної матриці $G_a^{'}$, яка відповідає УЕ $\omega_a^{'} = (\omega_a)^x \bmod \varphi_n$.

Виходячи з наведених властивостей матриць Галуа, пропонується такий протокол обміну ключами. Вважаємо відомими вектор ініціалізації V и НП φ. Абонент Аліса обирає таємний примітивний УЕ ω_a, на основі якого синтезує матрицю A, примітивну над НП φ. Аналогічним чином абонент Боб обирає таємний примітивний УЕ ω_b і синтезує примітивну матрицю B. Далі Аліса обчислює вектор $V_a = V \cdot A$ і надсилає його абоненту Бобу. В свою чергу абонент Боб обчислює вектор $V_b = V \cdot B$ і надсилає його абоненту Алісі. Після цього обидва абоненти помножують вектори, що отримали від партнера, на свої таємні матриці Галуа. Тим самим буде сформований однаковий таємний загальний ключ K. Це відбувається завдяки тому, що добуток примітивних матриць Галуа над одним і тим же НП є комутативним, а з цього випливає тотожність

$$K_a = V_b \cdot A = V \cdot B \cdot A \quad \equiv \quad K_b = V_a \cdot B = V \cdot A \cdot B. \tag{6}$$

Тому як матриці A і B комутативні, то з (6) маємо, що

$$K_a \equiv K_b \equiv K. \tag{7}$$

Замість матриць Галуа G з рівним успіхом в протоколі обміну ключами можуть бути використані *матриці Фібоначчі* F, які пов'язані з матрицями Галуа співвідношенням

$$F \xleftrightarrow{\perp} G \quad \text{або} \quad F = G^{\mathrm{T}}; \quad G = F^{\mathrm{T}},$$

де $\perp$ – оператор *правостороннього транспонування*, тобто транспонування відносно допоміжної діагоналі матриці.

Слід зазначити, що термін «матриця Галуа», як і «матриця Фібоначчі», мають походження з літературних джерел (наприклад: [7], [8]), що присвячені лінійним регістрам зсуву з лінійними зворотними зв'язками за схемами Галуа або Фібоначчі відповідно.

В *другому варіанті альтернативного протоколу* секретний ключ K обчислюється за два раунди. В першому раунді, який повторює варіант протоколу, що розглянутий вище, формується секретний спільний для обох абонентів мережі бінарний вектор n – го порядку, якій ми позначимо V_p. На підставі цього вектора Аліса і Боб обчислюють секретну сумісну матрицю перестановки P. Можна запропонувати різні способи побудови матриць P. Розглянемо один з них. Нехай $n = 8$ і N є десятковий еквівалент вектора V_p. Задача полягає в тому, щоб по значенню N скласти матрицю перестановки P_8 восьмого порядку. Оберемо той чи інший спосіб нумерації елементів матриці P_8 від 0 до 63. Обчислимо значення $n_8 = N \bmod 64$ и запишемо 1 в тому елементі матриці P_8, номер якого дорівнює n_8. Після цього викреслимо з матриці P_8 той рядок і стовпець, що містять 1. Отримаємо матрицю сьомого порядку, елементи якої перенумеруємо від 0 до 48. Знаходимо значення, яким однозначно визначається місце розташування 1 в матриці P_7 і, відповідно, в

матриці P_8. Дотримуючись методики, що запропоновано, можна досить просто побудувати матрицю перестановки будь-якого порядку.

Переходимо безпосередньо до викладу другого альтернативного варіанту протоколу обміну ключами шифрування. У цьому варіанті протоколу використовуються два відкритих ключа, якими є вектор ініціалізації V і незвідний поліном φ, а також по два закритих ключа, в якості яких оператори Аліса і Боб генерують (незалежно один від другого) випадкові примітивні над НП φ утворюючи елементи ω і υ. Протокол виконується за два раунди. У першому раунді на підставі відкритих ключів V, φ і секретних УЕ ω оператори мережі обчислюють сумісну матрицю перестановки P. Другий раунд виконується в такій послідовності. Аліса обирає примітивний над φ УЭ υ_a, формує спочатку матрицю Галуа A_υ, а потім подібну їй матрицю $A_p = P \cdot A_\upsilon \cdot P^{-1}$, обчислює вектор $V_a = V \cdot A_p$ і надсилає його Бобу. Відповідним чином поступає і оператор Боб. Після цього обидва абонента перемножують вектори, які отримані від партнерів, на свої секретні подібні матриці Галуа. Тим самим буде утворений спільний ключ K в силу того, що матриці A_p і B_p зберігають властивості як примітивності, так і комутативності первинних матриць A_υ і B_υ відповідно. Алгоритм формування спільного ключа K можна відобразити такою послідовністю математичних перетворень:

$$K_a = V_b \cdot A_p = V \cdot (P \cdot B_\upsilon \cdot P^{-1}) \cdot A_p = V \cdot P \cdot B_\upsilon \cdot (P^{-1} \cdot P) \cdot A_\upsilon \cdot P^{-1} = V \cdot P \cdot (B_\upsilon \cdot A_\upsilon) \cdot P^{-1}; \quad (8)$$

$$K_b = V_a \cdot B_p = V \cdot (P \cdot A_\upsilon \cdot P^{-1}) \cdot B_p = V \cdot P \cdot A_\upsilon \cdot (P^{-1} \cdot P) \cdot B_\upsilon \cdot P^{-1} = V \cdot P \cdot (A_\upsilon \cdot B_\upsilon) \cdot P^{-1}. \quad (9)$$

Тому як добутки матриць, що розміщені в дужках наприкінці співвідношень (8) та (9), комутативні, то з цього випливає тотожність (7), що як раз і потрібно для нормального функціонування протоколу обміну ключами шифрування.

Висновки

В даній роботі викладені основи побудові нових матричних протоколів обміну секретними ключами шифрування по відкритому каналу зв'язку. Незважаючи на те, що перший варіант протоколу, якій запропоновано, має ту ж саму кількість відкритих і закритих ключів, що і протокол Мегрелішвілі, криптографічна стійкість альтернативного протоколу імовірно вище за аналог. Справа в тім, що протокол Мегрелішвілі успадковує деякі риси протоколу Єроша-Скуратова. В зв'язку з цим питання щодо його криптостійкості залишається відкритим. Відносно альтернативних протоколів можливо висунути гипотезу, що єдиною атакою для них (крім атаки «людина посередині», яка притаманна всім протоколам, подібним DH протоколу) залишається лобова атака.

Література

1. Diffie W. New Directions in Cryptography /Diffie W.,Hellman M.E. // IEEE Transactions on Information Theory, v. IT-22, no. 6, Nov. 1976, p. 644-654. 2. Ерош И.Л. Адресная передача сообщений с использованием матриц над полем GF(2) / ЕрошИ.Л., Скуратов В.В. //Проблемы информационной безопасности. Компьютерные системы. 2004, №1. – С. 72-78. 3. Мегрелишвили Р.П. Однонаправленная матричная функция – быстродействующий аналог протокола Диффи - Хеллмана. / Мегрелишвили Р.П., Челидзе М.А., Бесиашвили Г.М. – Збірник матеріалів 7-й МК «Інтернет – Освіта – Наука - 2010». – Вінниця: ВНТУ, 2010. – С. 341-344. 4. Ростовцев А.Г. О матричном шифровании (критика криптосистемы Ероша и Скуратова). Ел. ресурс: www. ssl.stu.neva.ru/psw/crypto/rostovtsev/Erosh_Skuratov.pdf 5. Белецкий А.Я. Однонаправленная матричная функция / Белецкий А.Я., Мегрелишвили Р.П. - Праці Міжнародної Міжнародної молодіжної школи «Питання оптимізації обчислень». – Крим, Кацівелі, 2011. – С. 21-22. 6. Лидл Р. Конечные поля / Лидл Р., Нидеррайтер Г. – Т. 1. – М.: Мир, 1988. – 432 с. 7. Поточные шифры. Результаты зарубежной открытой криптологии Ел. ресурс: http://padabum.com/d.php?id=2669 8. Иванов М.А. Теория, применение и оценка качества генераторов ПСП / Иванов М.А., Чугунков И.В. – М.: «КУДИЦ-ОБРАЗ», 2003. – 240 с.