UDC 65

METHOD OF PROTECTION OF THE CONFIDENTIAL INFORMATION WITH USE OF PERMUTABLE FUNCTIONS

Stella G. Spirina

Krasnodar branch of Russian state trade and economic university
St. Karyakinf, 10, ap.35, Krasnodar, 350072, Russia
PhD (Law), Assistant Professor
E-mail: stella_spirina@mail.ru

In work it is offered recurenting a method of construction of permutable whole functions in fields Galua GF from (p) to the set degree on the basis of basic as question of protection of the confidential information.

Keywords: confidential information, permutable function.

Защита информации предполагает разработку системы организационно-технических мероприятий, обеспечивающих требуемую надежность хранения данных. Во многих криптографических системах защиты информации используются те или иные типы шифров перестановок. Зависимость вида ключей таких шифров от длины открытого текста создаёт значительные неудобства в использовании шифра. Поэтому был предложен ряд частных шифров перестановок, которые можно применить для зашифрования текстов любой длины.

В работе приводится алгоритм генерации перестановок числовых эквивалентов элементарных сообщений с помощью целых перестановочных функций заданной степени в явном виде. При программной реализации данного метода необходимо учитывать, что все перестановки генерируются с помощью так называемых базисных перестановочных целых функций заданного конечного поля. [2, С. 286]

Пусть F_q – поле Галуа порядка $q = p^l$, $l \geq 1$ и $x_1, x_2, \ldots, x_q$ – все его различные элементы, где p – простое число и представляет собой харак-теристику составного поля F_q.

Обозначим через $S=[x,g(x)]=\begin{pmatrix} x_1 & x_2 \ldots x_q \\ g(x_1) & g(x_2) \ldots g(x_q) \end{pmatrix}$ – подстановку элементов поля F_q, порождённую функцией $g(x) \in F_q[x]$. Назовём функцию g (x) перестановочной функцией поля F_q [1].

Перестановочные функции индуцируют перестановки элементов конечного поля F_q и, следовательно, соответствуют элементам симметрической группы S_q – группы всех подстановок на множестве из q элементов. Причём, если перестановочные функции f(x) и g (x) поля F_q задают подстановки $\mathbf{S}_f$ и $\mathbf{S}_g$ соответственно, то композиция **f(g(x))** этих функций – также перестановочная функция в F_q, которой соответствует новая подстановка $S = S_f \cdot S_g$. В частности, для функции $f(x) = g(g \ldots (g(x)) \ldots)$ существует наименьшее целое положительное число t такое, что подстановка $\mathbf{S^t = [x, x]} = E$ – тождественная подстановка. Здесь функция g(x) является базисной, на основе которой строится тождественная подстановка.

Отметим, что для некоторых значений q достаточно легко найти все перестановочные функции заданного поля F_q, а для других – невозможно [1].

Следуя работе [2], соответственно, назовём полином g(x) степени m ≥ 1 из кольца $F_q[x]$: $g(x) = \sum_{u=0}^{m} g_u x^u$ перестановочным полиномом поля F_q, если соответствующая ему полиномиальная функция g(x): $F_q \to F_q$, отображающая элемент $x_i \in F_q$ в элемент $g(x_i) \in F_q$, является перестановкой элементов поля F_q. Отметим, что полиномы такого вида существуют для любого конечного поля F_q, так как любое отображение такого поля F_q в себя можно задать с помощью некоторого полинома степени не более q – 1.

Здесь приведем лишь алгоритм генерации всех перестановок длины p, где p – характеристика поля Галуа. Алгоритм генерации всех перестановок длины p.

Вход. Длина перестановки p (p – простое число, характеристика поля).

Выход. Перестановки степени p.

Метод: а) Найти все значения $\mathbf{k_i}$ такие, что $(k_i, p-1) = 1$. б) Выписать все $\varphi(p-1)$ базисные перестановочные функции $f_1(x), f_2(x), \ldots, f_\varphi(x)$, для которых степени равны соответственно $\mathbf{k_i}$. Здесь $\varphi(x)$ – функция Эйлера. в) Найти все возможные композиции $\mathbf{g(x) = f_i(f_j(x))}$ для всех базисных функций. Каждой подстановке $S=\begin{pmatrix} 1 & 2 \ldots p \\ g(1)\ g(2) \ldots g(p) \end{pmatrix}$ применить функцию $\mathbf{g(x) = f_1(f_j(x))}$ для генерации очередной перестановки. г) Результатом является то, что все n! перестановки имеют длину p.

Отметим, что данный способ задания перестановок может найти практическое применение при программной реализации алгоритмов генерации поточного преобразования, а также в задачах, использующих различные варианты шифров перестановок в криптографических системах безопасной передачи информации.

Примечания:

1. Лидл Р., Нидеррайтер Г. Конечные поля. М., 1988.

2. Осипян В.О., Спирина С.Г., Подколзин В.В. Моделирование перестановок на основе перестановочных целых функций. // Материалы X Межд. н/п конф. «Современные проблемы математики, информатики и управления», г. Алматы, 2–3 октября 2008 г. С. 284-286.

УДК 65

МЕТОД ЗАЩИТЫ КОНФИДЕНЦИАЛЬНОЙ ИНФОРМАЦИИ С ИСПОЛЬЗОВАНИЕМ ПЕРЕСТАНОВОЧНЫХ ФУНКЦИЙ

Стелла Георгиевна Спирина

Краснодарский филиал Российского государственного торгово-экономического университета
350072, Россия, г. Краснодар, ул. Карякина 10, кв. 35
Кандидат юридических наук, доцент
E-mail: stella_spirina@mail.ru

В работе предлагается рекурентный метод построения перестановочных целых функций в полях Галуа GF от (p) заданной степени на основе базисных, для защиты конфиденциальной информации.

Ключевые слова: конфиденциальная информация, перестановочная функция.