АЛГОРИТМ РЕШЕНИЯ КУБИЧЕСКИХ УРАВНЕНИЙ В КОНЕЧНОМ ПОЛЕ И ЕГО ПРИМЕНЕНИЕ В ОТРИЦАЕМОМ ШИФРОВАНИИ

Д. С. Будчан

СПбГЭТУ «ЛЭТИ»

Одним из ключевых признаков современного общества является интенсивное развитие информационной области. При этом на первый план выходят проблемы, связанные с безопасностью личных, коммерческих и государственных данных. Защита информации достигается в том числе и путём применения различных алгоритмов шифрования. Существуют различные методы шифрования, среди которых в ряду новейших способов криптографического преобразования стоит отрицаемое шифрование.

В работе [1] предлагается способ отрицаемого шифрования, который заключается в генерации шифртекста в виде набора коэффициентов уравнений третьей степени в конечном поле, вида:

$$x^3 + Ax^2 + Bx + D \equiv 0 \; mod \; p \tag{1}$$

Алгоритм решения кубических уравнений в простом конечном поле $GF(p)$ состоит из нескольких этапов (упрощённый вид):

- переход к уравнению, свободному от квадрата неизвестного

$$x = z - \frac{A}{3} \bmod p \rightarrow z^3 + Pz + Q = 0 \bmod p, где P = B - \frac{A^2}{3} \bmod p, Q = \frac{2A^3}{27} - \frac{AB}{3} + D \bmod p \tag{2}$$

- вывод формулы для корней преобразованного кубического уравнения (2)

$$z = \alpha + \beta, \text{ где } \alpha\beta = -\frac{P}{3} \tag{3}$$

$$\alpha = \sqrt[3]{-\frac{Q}{2} + \sqrt{\frac{Q^2}{4} + \frac{P^3}{27}}}; \beta = \sqrt[3]{-\frac{Q}{2} - \sqrt{\frac{Q^2}{4} + \frac{P^3}{27}}}$$

- переход в поле $GF(p^2)$, в качестве которого берётся поле двоичных векторов

$$\vec{z}^3 + \vec{P}\vec{z} + \vec{Q} = (0,0), \vec{z} = \vec{a} + \vec{b} \tag{4}$$

- вычисление корней уравнения (4) и переход к корням уравнения (1) по формулам (2).

Результатом работы является алгоритм решения кубических уравнений в простом конечном поле. Алгоритм может быть использован для построения протокола отрицаемого шифрования, с целью применения в защищённых распределённых вычислениях, тайном электронном голосовании, защите от скупки голосов и др.

---

1. *Молдовян Н. А., Молдовян Д. Н., Вайчикаускас М. А. Генерация кубических уравнений как способ открытого шифрования // Вопросы защиты информации. 2015. №2. С. 3—7.*