Санкт-Петербургский государственный электротехнический университет им. В.И. Ульянова (Ленина)

Разработка алгоритма решения кубических уравнений в конечном бинарном поле и реализация протокола отрицаемого шифрования

Магистрантка 1 курса гр.2381: Будчан Дарья Сергеевна

Руководитель: д.т.н., профессор кафедры ИБ
Молдовян Николай Андреевич

Цель работы

Разработка алгоритма решения кубических уравнений в конечном поле с последующей имплементацией в протокол отрицаемого шифрования, стойкий к принуждающим атакам.

Задачи

- Уточнение алгоритма генерации кубического уравнения в виде набора коэффициентов уравнения, который будет лежать в основе шифрования сообщений.
- Разработка алгоритма решения кубического уравнения в конечном бинарном поле и обеспечение однозначности процедуры дешифрации.
- Модернизация способа отрицаемого шифрования, в основе которого будет разработанный алгоритм генерации и решения кубических уравнений.
- Реализация разработанного алгоритма.

Отрицаемое шифрование

- Защищённые распределённые вычисления.
- Системы тайного электронного голосования.
- Электронная цифровая подпись.
- Протоколы одноразовых паролей.

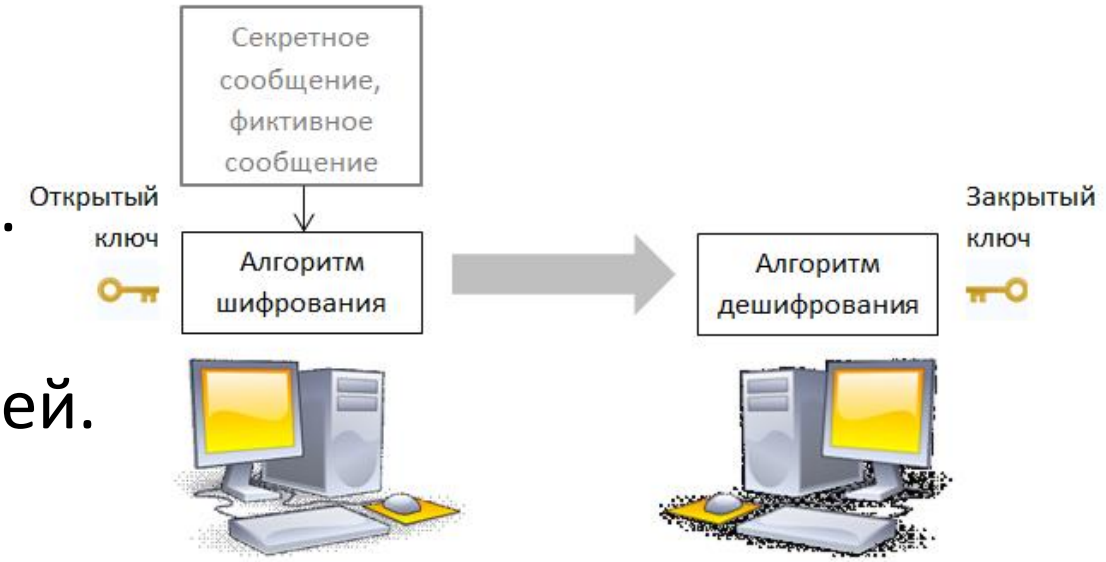


Рисунок 1 – Общая схема ОШ

Алгоритм решения уравнения

$$x^3 + Ax^2 + Bx + C = 0 \bmod p \quad (1)$$

$$z^3 + Pz + Q = 0 \bmod p \quad (2)$$

$$z = \alpha + \beta \quad (3)$$

$$\vec{z} = \vec{\alpha} + \vec{\beta} \quad (4)$$

Нахождение корней уравнения (4), переход к корням уравнения (3), обратная замена и вычисление корней уравнения (1).

$$x^3 - Ax^2 + Bx - C = 0 \bmod p$$

$$x = z + \frac{A}{3} \bmod p$$

$$z^3 + Pz + Q = 0 \bmod p$$

$$P = B - \frac{A^2}{3} \bmod p$$

$$Q = -\frac{2A^3}{27} + \frac{AB}{3} - C \bmod p$$

$$z = \alpha + \beta$$

$$\alpha = \sqrt[3]{-\frac{Q}{2} + \sqrt{\frac{Q^2}{4} + \frac{P^3}{27}}} \bmod p = \sqrt[3]{\frac{A^3}{27} - \frac{AB}{6} + \frac{C}{2} + \sqrt{\left(-\frac{A^3}{27} + \frac{AB}{6} - \frac{C}{2}\right)^2 + \left(\frac{B}{3} - \frac{A^2}{9}\right)^3}} \bmod p$$

$$\beta = \sqrt[3]{-\frac{Q}{2} - \sqrt{\frac{Q^2}{4} + \frac{P^3}{27}}} \bmod p = \sqrt[3]{\frac{A^3}{27} - \frac{AB}{6} + \frac{C}{2} - \sqrt{\left(-\frac{A^3}{27} + \frac{AB}{6} - \frac{C}{2}\right)^2 + \left(\frac{B}{3} - \frac{A^2}{9}\right)^3}} \bmod p$$

$$\alpha\beta = -\frac{P}{3} = \frac{A^2}{9} - \frac{B}{3}$$

Алгоритм шифрования

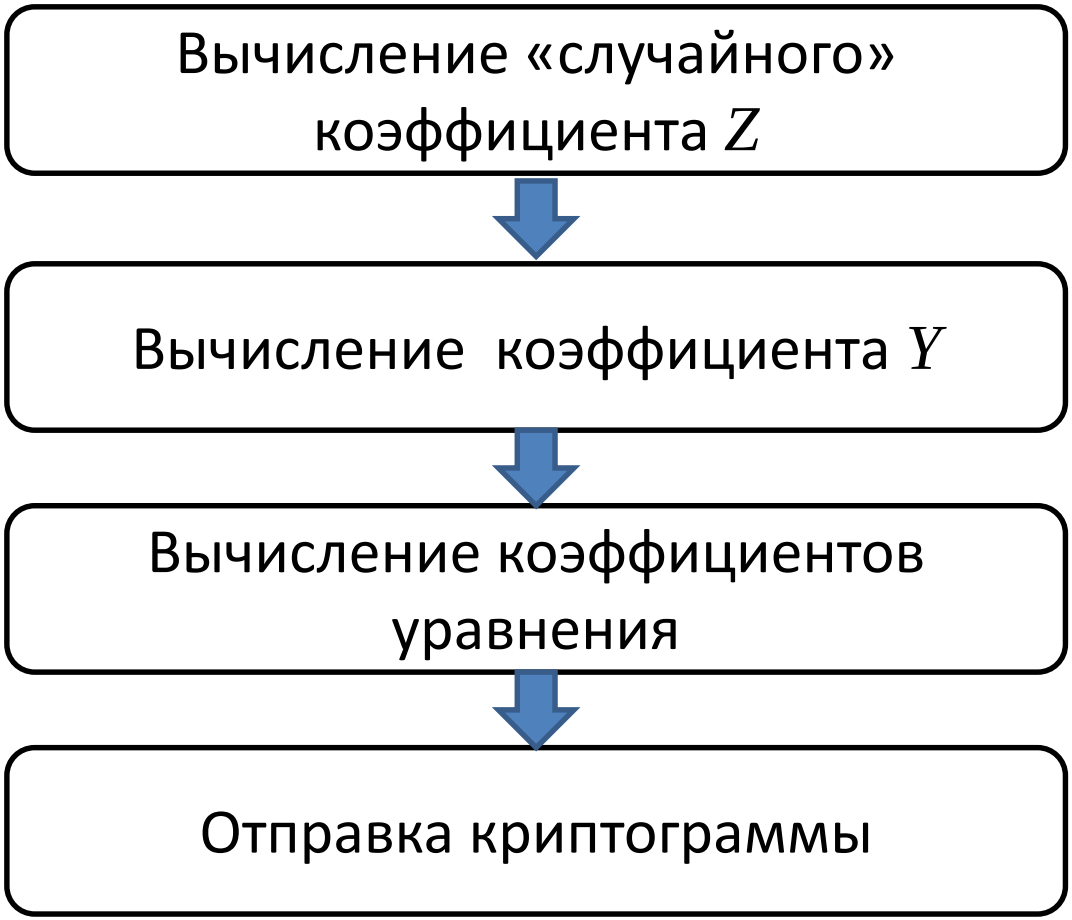


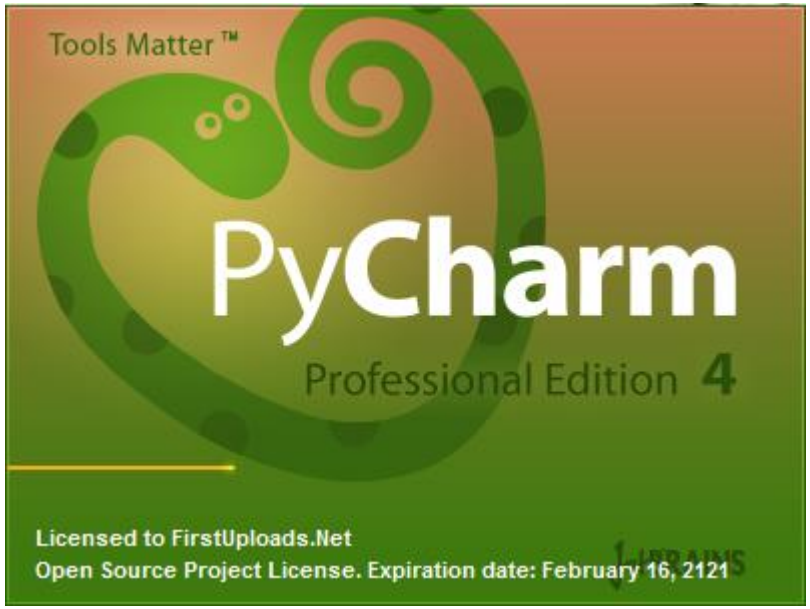
Рисунок 2 – Схема алгоритма ОШ

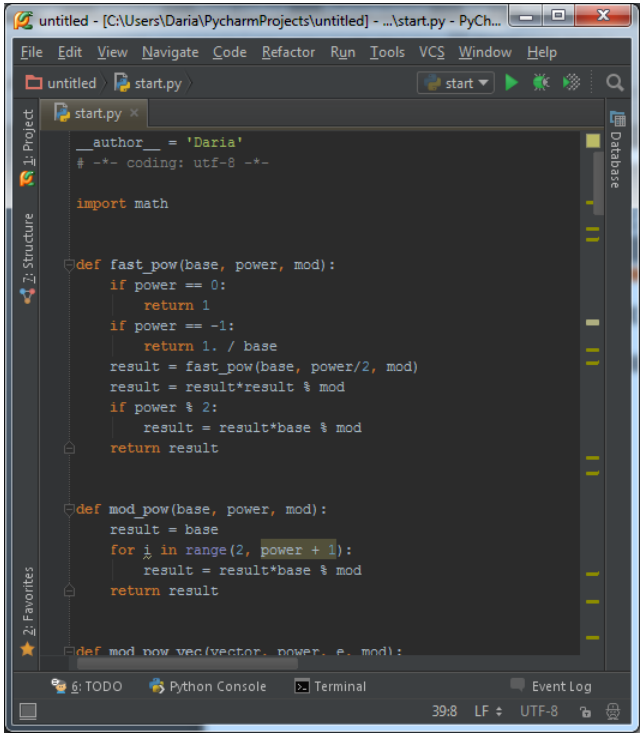
Алгоритм дешифрования

Рисунок 3 – Схема алгоритма дешифрования

Реализация алгоритма

- Язык программирования: Python версии 3
- Среда разработки: PyCharm





Список использованных источников

- Глуско Кр.Л., Титов С.С. Арифметический алгоритм решения квадратных уравнений в конечных полях характеристики два / Доклады ТУСУРа, № 1 (25), часть 2, июнь 2012– 5 с.
- Геут К.Л. Нормальные базисы в конечных полях и их приложения / Диссертация, Екатеринбург 2015 – 111 с.