## Алгоритм шифрования на базе полиномиальных отображений

* Теоретической основой выпускной квалификационной работы послужили исследования, представленные в работе *«*Арыков Н. Е., Кренделев С. Ф. Разработка white-box криптографической системы и ее применение для безопасного хранилища данных //Безопасность информационных технологий. – 2014. – Т. 21. – №. 3.*»*

В основе работы алгоритма лежит биективное отображение, .т. е. взаимно однозначное отображение конечного множества в себя или перестановки элементов этого множества, где в нашем случае множество – это конечное поле, а его элементы – это перестановочные многочлены.

Как уже было сказано одночлен является перестановочным над полем , если его степень взаимно проста с . Обратным отображением к будет , где обратный элемент в кольце p-1. Найти обратный элемент будет очень сложно,т. к. мы не знаем число .Комбинируя эти отображения, используя обратимое аффинное преобразование , мы увеличиваем число многочленов, где – прямая на плоскости и .

Получаем, что перестановочный многочлен может быть описан как суперпозиция отображений таких, что:

,

где p, и p-1. Такие отображения назовем элементарными.

Учитывая выше сказанное, предлагается следующая схеме шифрования:

1. Выбираются простые числа с помощью Теста Миллера-Рабина
2. Для каждого их выбираются элементарные полиномы над и вычисляется их суперпозиция
3. После раскрытия скобок в получается биективный полином
4. Вычисляется F(x) с помощью китайской теоремы об остатках:

=

1. Объявляется открытый ключ:

,

где – произведение

1. Объявляется приватный ключ:

(, )

Пример работы алгоритма на малых параметрах.

* + 1. Пусть . Модуль
    2. Выбираются элементарные полиномы для каждого простого числа:
* Для : . Вычисляется их суперпозиция и биективный полином:

=

* Для : . Вычисляется их суперпозиция и биективный полином:

=

* Для : . Вычисляется их суперпозиция и биективный полином:

=

* Получаем, что полином имеет вид

,

где , т. к. во всех биективных полиномах они отсутствуют. Тогда полином будет иметь вид:

.

Для получения коэффициентов необходимо решитьдля каждого из них китайскую теорему об остатках. Коэффициент будет равен:

,

где , , и .

Отсюда , , . Для каждого применяется расширенный алгоритм Евклида для нахождения обратных к ним элементов и вычисляются. В нашем случае . Следовательно, коэффициент

Таким образом находим все остальные коэффициенты и получаем

* + 1. Взаимно однозначный полином и объявляются публичным ключом, а биективные полиномы для каждого простого числа и сам набор простых чисел – приватным ключом.