Министерство образования Республики Беларусь
Учреждение образования
«Полоцкий государственный университет»

ИНФОРМАЦИОННО-КОММУНИКАЦИОННЫЕ ТЕХНОЛОГИИ: ДОСТИЖЕНИЯ, ПРОБЛЕМЫ, ИННОВАЦИИ (ИКТ-2018)

Электронный сборник статей
I Международной научно-практической конференции,
посвященной 50-летию Полоцкого государственного университета

(Новополоцк, 14–15 июня 2018 г.)

Новополоцк
Полоцкий государственный университет
2018

Информационно-коммуникационные технологии: достижения, проблемы, инновации (ИКТ-2018) [Электронный ресурс] : электронный сборник статей I международной научно-практической конференции, посвященной 50-летию Полоцкого государственного университета, Новополоцк, 14–15 июня 2018 г. / Полоцкий государственный университет. – Новополоцк, 2018. – 1 электрон. опт. диск (CD-ROM).

Представлены результаты новейших научных исследований, в области информационно-коммуникационных и интернет-технологий, а именно: методы и технологии математического и имитационного моделирования систем; автоматизация и управление производственными процессами; программная инженерия; тестирование и верификация программ; обработка сигналов, изображений и видео; защита информации и технологии информационной безопасности; электронный маркетинг; проблемы и инновационные технологии подготовки специалистов в данной области.

Сборник включен в Государственный регистр информационного ресурса. Регистрационное свидетельство № 3201815009 от 28.03.2018.

Компьютерный дизайн М. Э. Дистанова.

Технические редакторы: Т. А. Дарьянова, О. П. Михайлова.

Компьютерная верстка Д. М. Севастьяновой.

211440, ул. Блохина, 29, г. Новополоцк, Беларусь
тел. 8 (0214) 53-21-23, e-mail: irina.psu@gmail.com

ISBN 978-985-531-602-3

УДК 004.056.5

ПРИМЕНЕНИЕ ГЕНЕТИЧЕСКИХ АЛГОРИТМОВ В КАЧЕСТВЕ МЕТОДА КРИПТОАНАЛИЗА БЛОЧНОГО ПЕРЕСТАНОВОЧНОГО ШИФРА

Е.С. ЛЕМЕШОНОК, канд. физ.-мат. наук Е.И. КОЗЛОВА
(Белорусский государственный университет, Минск)

С развитием современных технологий защитить информацию от несанкционированного доступа становится все сложнее и сложнее. В какой-то момент нынешние алгоритмы шифрования и дешифрования могут исчерпать себя. Для решения данной проблемы необходимо найти новые подходы. Перспективным направлением является построение биологических моделей.

Если рассматривать криптоатаку как решение задачи поиска секретного ключа в пространстве ключей шифрования и при этом ввести в рассмотрение некоторый минимизирующий функционал, то данную задачу можно рассматривать как задачу оптимизации, которая и является основной для генетического алгоритма [1].

В данной работе рассматривается симметричный блочный перестановочный шифр. Открытый текст разбивается на блоки фиксированной длины N и над каждым из них выполняется перестановка по ключу. [2]

Задача: есть n открытых текстов на двоичном алфавите $Z_2 = \{0,1\}$, зашифрованных одной перестановкой, и n соответствующих открытых текстов. С помощью генетического алгоритма (ГА) необходимо найти ключ для дешифрования.

Для решения задачи проведем параллель между ее составляющими и составляющими генетического алгоритма.

Таблица. – Связь ГА и решаемой задачи

Хромосома	Искомая перестановка (ключ)
Ген	Элемент перестановки
Особь	Характеризуется одной хромосомой – ключом

Для фитнесс-функции использовалось такое понятие, как расстояние Хэмминга.

$$F = d(open, decrypt), \quad (1)$$

где $d(open, decrypt)$ – количество различающихся символов открытого текста и текста, расшифрованного найденным ключом.

Таким образом, если найдена правильная перестановка, то тексты совпадут и фитнесс-функция будет равна нулю.

Подробнее о шагах, которые имеют особенности.

Кроссовер. Так как в качестве хромосом, характеризующих особь, выбраны перестановки, то получается, что гены хромосом зависят друг от друга. То есть в одной хромосоме каждый ген может повторятся только один раз, что противоречит стандартному ГА. Поэтому нужно ввести особенный оператор кроссовера, который будет учитывать этот момент. [3] Так же для того, чтобы улучшить сходимость ГА, при построении алгоритма работы оператора кроссовера были использованы понятия митоза и мейоза. В результате, если особь родитель имеет большую приспособленность, то одним из потомков будет абсолютная ее копия, что свойственно митозу. Если же особь родитель менее приспособлена, то потомок копия не создается, а происходит

скрещивание хромосом родителей с учетом уникальности генов в одной хромосоме. Таким образом обеспечивается как разнообразие генетического материала, так и его хорошее качество. [4]

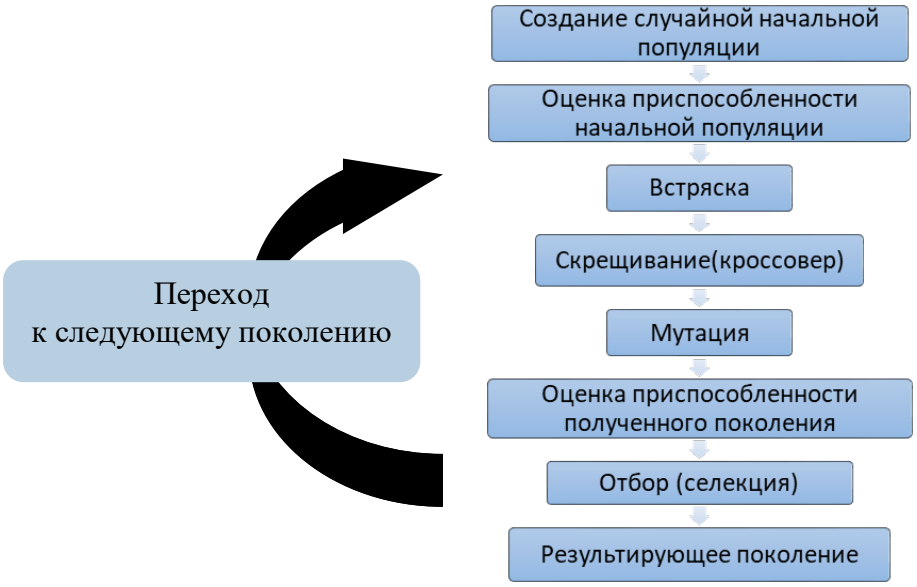


Рисунок 1. – Схема генетического алгоритма для решения поставленной задачи

Встряска. Для решения задачи возникла необходимость ввести данный процесс, так как какой-либо из найденных локальных минимумов фитнесс-функции начинал быстро заполнять всю популяцию и в результате дальнейшая работа алгоритма быстро переставала иметь смысл. Суть встряски заключается в том, чтобы из совокупности повторяющихся особей текущего поколения оставить только одну, а остальные уничтожить. Места уничтоженных особей занимают новые случайные особи. Это позволяет избежать ложной сходимости алгоритма, а также увеличить количество рассматриваемых вариантов решения задачи.

На работу алгоритма влияют несколько основных параметров, и их можно разделить на две группы: параметры, зависящие от алгоритма шифрования и параметры, зависящие непосредственно от ГА.

Параметры, зависящие от ГА:

– Количество особей в одном поколении и количество поколений

– Чем больше особей в поколении, тем быстрее находится ключ. Это обусловлено тем, что за одну итерацию рассматривается большее число различных решений.

– Оператор селекции.

Для сравнения были выбраны турнирная и элитная селекции. Из графиков видно, что турнирная селекция очень непостоянна в данном алгоритме и не может найти решение даже за большое число поколений, в то время как элитная срабатывает намного быстрее и находит нужный ключ.

Параметры, зависящие от алгоритма шифрования:

– Общая длина дешифровываемого текста.

Этот параметр сильно влияет на временные затраты на поиск ключа. Так же он влияет на качество найденной перестановки. Если тексты недостаточно длинные или пар текстов немного, то это приводит к нахождению ложной перестановки, т.к. несколько перестановок подходят к этим парам текстов и дают идеальный результат.

– Длина перестановки, использованной для шифрования текста.

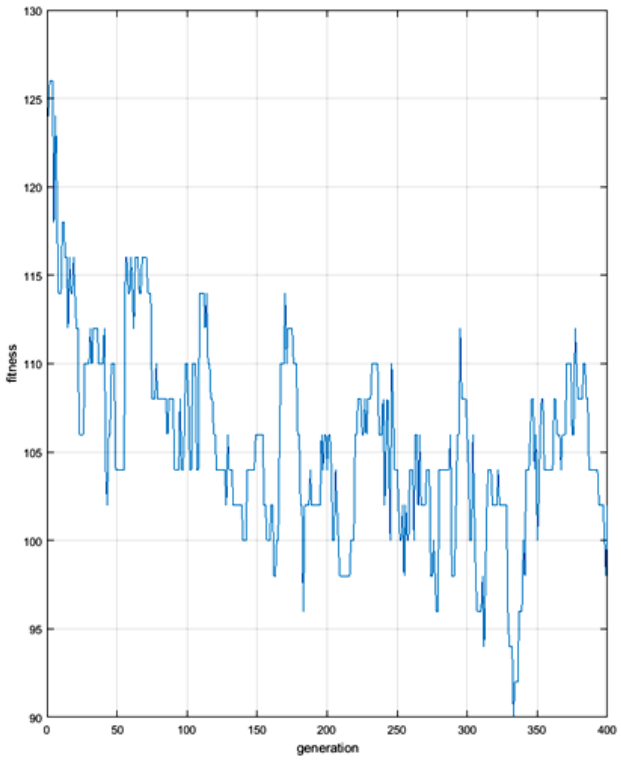
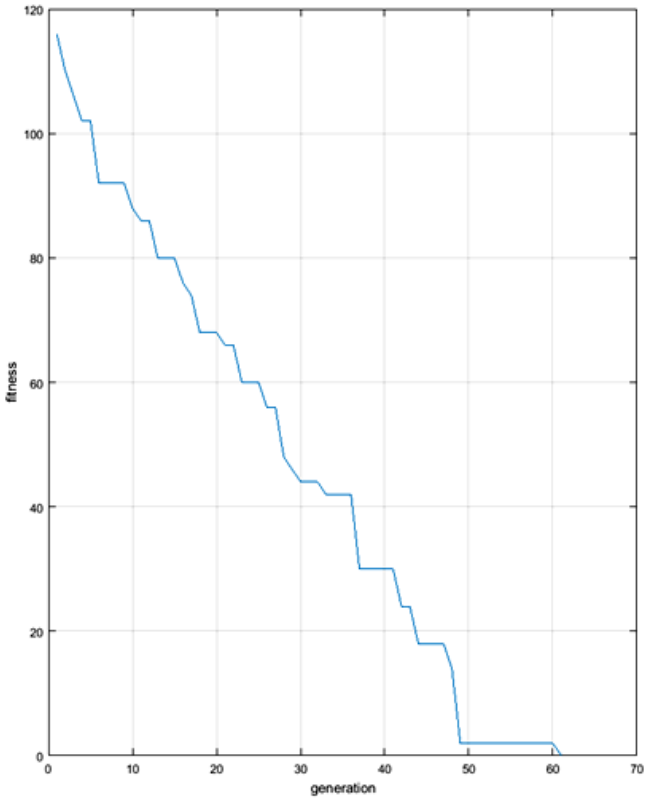


Рисунок 2. – Зависимость минимального фитнесса от числа поколений турнирная селекция



Длина ключа: 32
Длина текста: 320
Число особей: 200
Максимальное число поколений: 400

Рисунок 3. – Зависимость минимального фитнесса от числа поколений элитная селекция

Чем больше число перестановок, тем дольше работает ГА, и тем сложнее ему найти верные ключи. Аналогично и с длинами перестановок. Это происходит по следующей причине: если исходный тест зашифрован q перестановками и каждая перестановка имеет некоторую длину k, то число возможных решений задачи:

$$(k!)^q. \quad (2)$$

Рисунок 4. – График зависимости числа поколений от длины текста

Проанализировав разработанный алгоритм можно сделать следующие выводы:

- Преимущества:
  - Минимизация участия человека в процессе криптоанализа.
  - Возможность получить искомый ключ или близкий к нему.
- Недостатки
  - Требует большого количества временных и вычислительных ресурсов при решении сложных задач.
  - Необходимо иметь пары «исходный текст - шифрованный текст», а также знать длину ключей шифрования.
  - Недостаточно оптимальная фитнесс-функция для большего числа перестановок.
- При правильном выборе всех необходимых параметров можно получить достаточно сильный метод криптоанализа.

Литература

1. Катасев, А.С. Оценка стойкости шифрующих преобразований моноалфовитной замены с использованием генетического алгоритма / А.С. Катасев, Д.В. Катасева, А.П. Кирпичников // Вестн. технол. ун-та. – 2015. – Т. 18, №7. – 255 с.
2. Баричев, С.Г. Основы современной криптографии : учеб. пособие / С.Г. Баричев, Р.Е. Серов – М. : Горячая Линия – Телеком, 2006. – С. 8–22.
3. Городилов, А. Генетический алгоритм для определения длины ключа и дешифрования перестановочного шифра / А. Городилов, В. Морозенко // International Journal «Information Theories and Applications» – 2007. – 507 с.
4. Генетические алгоритмы [Электронный ресурс]. – Режим доступа: https://studopedia.org. – Дата обращения: 22.07.2015.