Применение генетических алгоритмов в задачах криптоанализа

Студент: Шестаков Дмитрий

Группа: 4241/1

Руководитель: доц. Пак В.Г

Содержание:

- Цели работы
- Введение. Криптоанализ –задача многомерной оптимизации
- Концепция генетических алгоритмов
- Криптосистемы атакованные генетическими алгоритмами
- Описание разработанного универсального генетического алгоритма.
- Отличия алгоритма от существующих реализации.
- Перспективность атак на современные криптосисетмы. Лавинный эффект.
- Итоги работы. Постановка направления дальнейшей деятельности.

Цели работы:

- Исследовать существующие работы по применению генетических алгоритмов в задах криптоанализа.
- Выделить криптосистемы для которых возможно эффективное применение генетических алгоритмов
- Изучить традиционные методы криптоанализа этих систем
- Разработать универсальный генетический алгоритм для криптоанализа выбранного ряда криптосистем
- Исследовать перспективность применения генетических алгоритмов для более современных типов криптосистем.
- Сравнить эффективность разработанного алгоритма с методом полного перебора.

Введение

• Задачи криптологии: задача криптографии и задача криптоанализа

• Криптоанализ - нахождении единственного настоящего секретного ключа среди множества всех возможных ключей

• Задача криптоанализа - задача поиска, при этом пространство поиска велико, и критерий «качества» найденного решения, как правило, не поддается строгой формализации

• Задача криптоанализа сводится к задаче многомерной оптимизации, где генетические алгоритмы зарекомендовали себя на сегодняшний день очень хорошо.

Концепция генетических алгоритмов

- Генетические алгоритмы – решают задачи оптимизации и используют механизмы, напоминающие механизмы естественной эволюции.
- Потенциальное решение представлено в виде особи.
- Особь кодируется с помощью полностью описывающего ее объекта хромосомы
- Популяция – совокупность особей.

Достоинства:

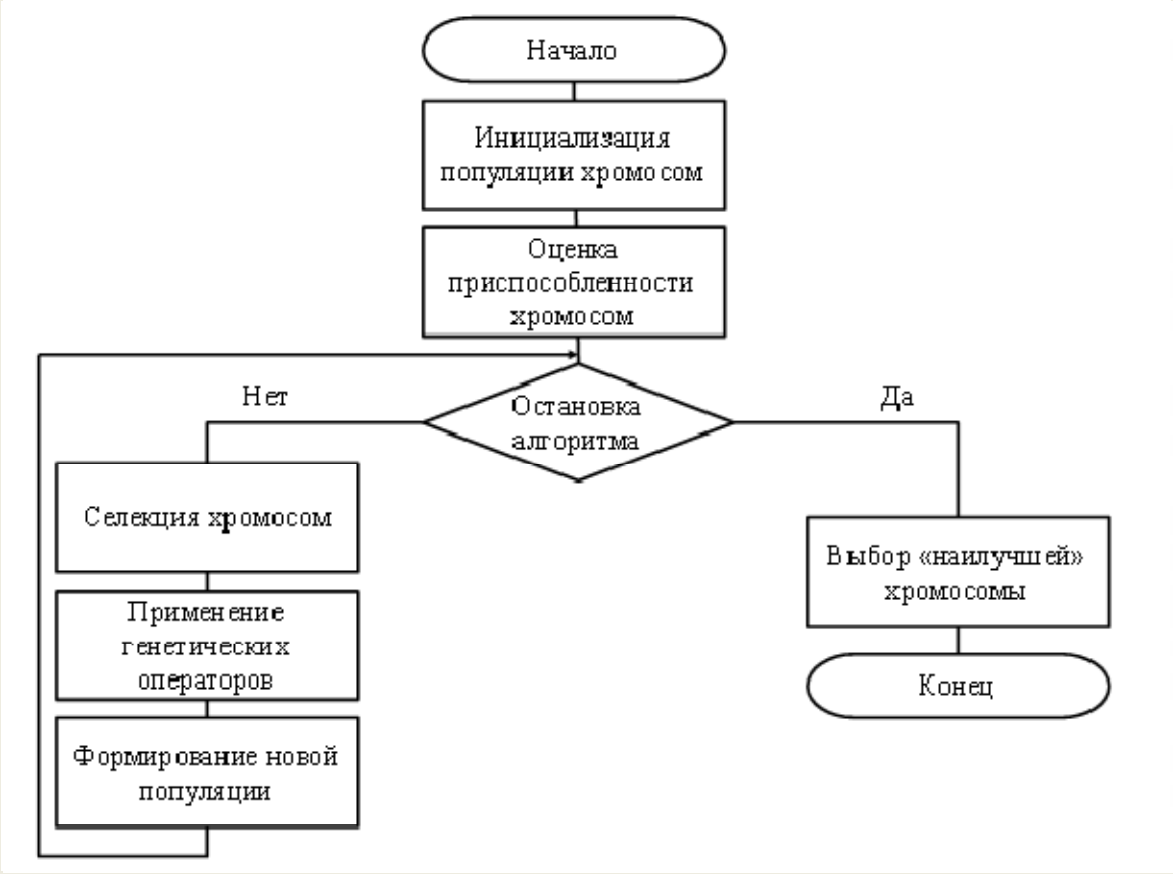
- Кодирование параметров
- Операции на популяции
- Рандомизация операций

Недостатки:

- высокая трудоёмкость
- сложность оценки сходимости

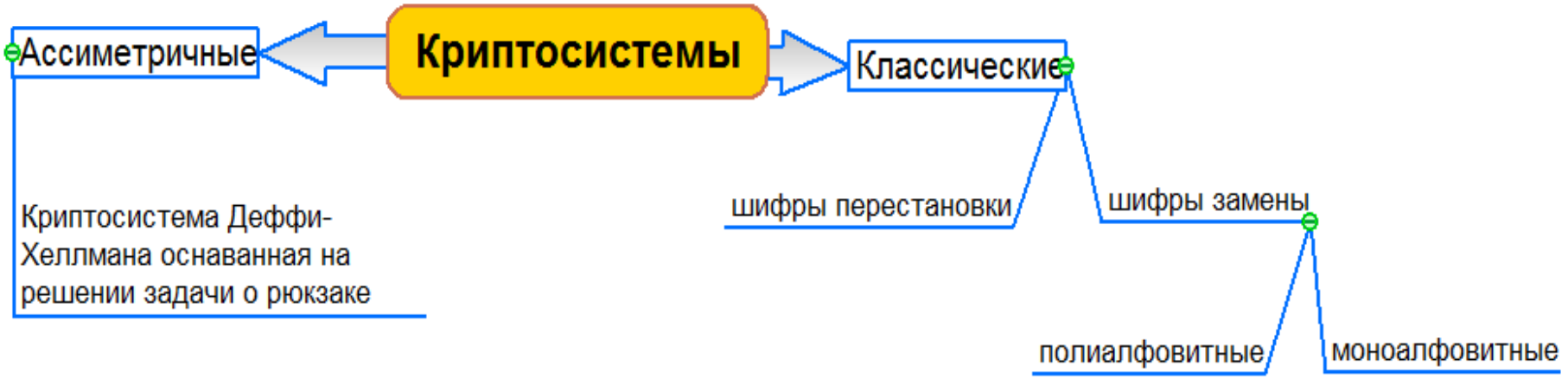
Концепция генетических алгоритмов

Блок-схема генетического алгоритма.



Шифры атакованные ГА

О эффективности применения ГА можно говорить только по отношению к классическим криптосистемам.



Описание разработанного ГА

- Особь популяции – потенциальный ключ для расшифровки. Строка символов или битов.
- Задаваемые параметры – размер популяции *pSize* и максимальная длинна ключа *kSize*.
- Начальная популяция – набор из *pSize* случайных строк символов длинной от 0 до *kSize*.

Описание разработанного ГА

Фитнесс-функция:

$$\mathrm{F(k)} = \frac{1}{f}\sum_{i=1}^{f} Fi(k)$$ - среднее значение трёх фитнесс функций F_1, F_2, F_3

- F_1 : функция вычисления ***индекса совпадения*** (ф-статистика)

$$\mathrm{f} = \sum_{i=0}^{n} pi(pi-1)$$ -формула вычисления индекса совпадения,
p_i – частота повторения i-ого символа алфавита в тексте.

Значения индекса для осмысленного текста и для случайного текста
Известны заранее $E_{случ.} = 0.0385N\ (N-1)$ и $E_{англ.} = 0.0668N\ (N-1)$
где N – длинна текста.

*Чем ближе значение индекса к значению для осмысленного текста тем выше **приспособленность** особи.*

Описание разработанного ГА

- F_2 – вычисление частот встречаемости **<u>биграмм</u>***:*
  - Биграмма – это две подряд идущие буквы в тексте
  - $W(T) = \sum_{ij} \left| T_{ij} - E_{ij} \right|$, где T_{ij} – частоты встретившихся в тексте T биграмм (ij), Eij – частоты биграмм для осмысленного текста.

  По шагам:
  - 1. Расшифровать зашифрованный текст S с использованием выбранного ключа P, в результате чего получим текст T .
  - 2. Подсчитать частоты Tij всевозможных биграмм (i j) в тексте T.
  - 3. Найти значение целевой функции W(T) по указанной выше формуле.

Чем ближе значение целевой функции к 0 тем выше ***приспособленность*** *особи.*

Описание разработанного ГА

- *F_3* – вычисление **расстояния Хэмминга***:*
  - Расстояние Хэмминга – метрика различия объектов одинаковой размерности.
  - Пример: *d(слнотацепрт, тлньеанелрт)* = 6 символов совпали

  По шагам:
  - 1. Расшифровать зашифрованный текст S с использованием выбранного ключа P, в результате чего получим текст T .
  - 2. Подсчитать расстояние Хэмминга для части текста T и заранее известной части исходного сообщения (длинны w).
  - 3. Найти значение целевой функции по формуле $F_{hd}(k) = i/w$, где i – расстояние Хэмминга.

Чем ближе значение целевой функции к 1 тем выше ***приспособленность*** *особи.*

Описание разработанного ГА

- **Селекция** хромосом:
  - 25% особей с наибольшей приспособленностью выбираются для формирования следующего поколения

  Следующее поколение :

  25% - выбранные особи без изменений

  50% - особи полученные путём скрещивания и мутации выбранных особей.

  25% - случайные особи, иммигрировавшие извне популяции.

  Иммиграция - потенциально вводит новый генетический материал.

  На всех этапах работы ГА все ***особи должны быть различны***.

Описание разработанного ГА

- **Мутация и скрещивание**

  1. Оператор **изменения размера**. Этот оператор случайным образом либо уменьшает размер особи, либо увеличивает.

  2. Оператор **замены**. Заменяет случайный символ в особи на случайный символ из алфавита.

  3. Оператор **единичной мутации**. Заменяет случайно выбранный символ особи на следующий или предыдущий по алфавиту.

  4. **Двухточечный кроссовер**.

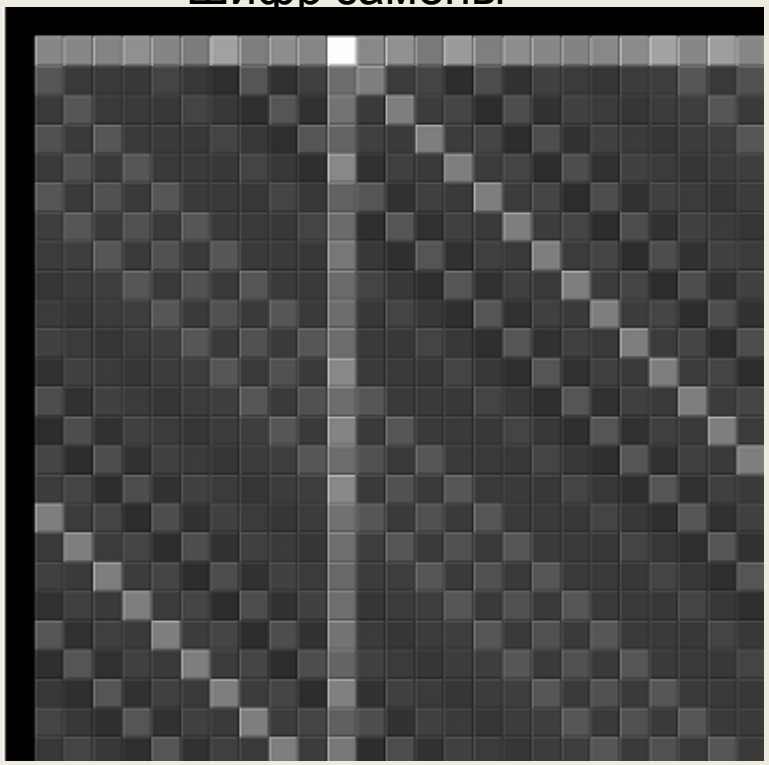
Уникальность алгоритма

- Универсальность алгоритма
- Фитнесс функция объединяет методы поиска ключа и поиска длинны ключа.
- Система селекции с иммиграцией
- Уникальные операторы мутации

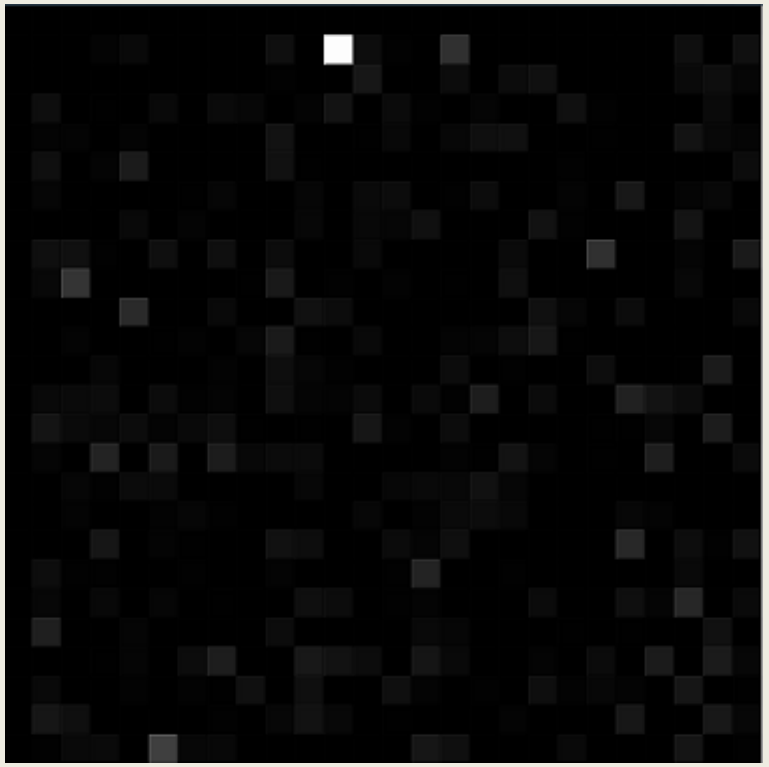
Устойчивость современных криптосистем

- Лавинный эффект – изменение одного символа входной последовательности изменяет в среднем половину битов выходной последовательности.

Шифр замены



16 раунд шифра DES



Ключ = ‘ka’

Итоги

- Были изучены существующий работы по применению генетических алгоритмов в криптоанализе
- Выявлены криптосистемы к криптоанализу которых могут применяться ГА наиболее эффективно.
- Были исследованы традиционные методы атак на эти криптосистемы.
- Была разработана концепция универсального ГА для криптоанализа классических криптосистем.
- Исследована возможность применения ГА подхода для современных криптосистем.

Направления дальнейшей деятельности

- Программная реализация алгоритма
- Тестирование на шифрах замены: шифре Виженера, смешанном шифре Виженера, шифре с автоключом;

  и на перестановочных шифрах.
- Сравнение эффективности ГА и метода полного перебора по выбранным метрикам.
- Исследования возможности модификации алгоритма с целью эффективного применения для современных криптосистем.
- Исследовать возможность распараллеливания разработанного ГА с целью увеличения эффективности.

Достижения

- Первые результаты исследований по это теме были представлена на XXXVIII «Неделе науки СПбГПУ»

БЛАГОДАРЮ ЗА ВНИМАНИЕ