УДК 004.056.55 DOI: 10.12737/3505

Исследование возможности применения бионических методов пчелиных колоний для реализации криптоанализа классических шифров перестановок*

Ю. О. Чернышёв, А. С. Сергеев, Е. О. Дубров, А. Н. Рязанов

Рассматривается возможность применения алгоритмов пчелиных колоний для реализации криптоанализа шифров перестановок. Данная задача является классической оптимизационной задачей, для решения которой применяются известные методы пчелиных колоний, относящихся к сравнительно новому классу биоинспирированных оптимизационных методов. Показано, что данная задача является частным случаем задачи о назначениях и может быть решена с помощью алгоритма пчелиных колоний, основу поведения которых составляет самоорганизация, обеспечивающая достижение общих целей роя. На первом этапе с помощью пчёл-разведчиков формируется множество перспективных областей-источников, на втором этапе с помощью рабочих пчёл-фуражиров осуществляется исследование окрестностей данных областей. При этом основная цель колонии пчёл — найти источник, содержащий максимальное количество нектара. Рассмотрены методы представления решения (позиции в пространстве поиска), приведена формула для определения значения целевой функции (количества нектара). Показано, что целью поиска является определение оптимальной комбинации символов с максимальным значением целевой функции. Приводится описание основных этапов алгоритма пчелиных колоний, а также пример его работы.

Ключевые слова: *криптоанализ, задача о назначениях, биоинспирированные методы, алгоритм пчелиных колоний, рабочие пчёлы (фуражиры), пчёлы-разведчики, шифр перестановки.*

Введение. В последние годы интенсивно разрабатывается новое научное направление под названием «природные вычисления», объединяющее математические методы, в которых заложен принцип природных механизмов принятия решений. Как отмечено в [1], научное направление «природные вычисления» объединяет такие разделы, как эволюционное программирование, нейросетевые вычисления, алгоритмы роевого интеллекта, муравьиные и генетические алгоритмы. В моделях и алгоритмах эволюционных вычислений ключевым элементом является построение начальной модели и правил, по которым она может изменяться (эволюционировать). В течение последних лет были предложены разнообразные схемы эволюционных вычислений, в том числе генетические алгоритмы, генетическое программирование, эволюционные стратегии, эволюционное программирование. Общие концепции и методологический подход к построению эволюционных вычислений, основанных на природных системах, а также основные гипотезы, закономерности и положения концепции эволюционных вычислений отмечены в [2, 3]. В настоящее время известны применения генетических алгоритмов для оптимизации широкого круга задач, в том числе задач криптоанализа. В [4–9] авторами рассматривались методы организации криптографических атак на традиционные симметричные криптосистемы, использующие шифры перестановки и замены, а также на блочные криптосистемы с использованием биоинспирированных методов. Следует заметить, что задачи такого типа относятся к переборным задачам с экспоненциальной временной сложностью. Побудительным мотивом для разработок новых алгоритмов являются возникшие потребности в решении задач большой размерности [10]. Анализ исследований показывает, что наиболее успешными в данных условиях являются методы, в которых заложены принципы природных механизмов принятия решений. Недостатком генетических алгоритмов является наличие «слепого» поиска, что приводит к увеличению времени поиска, генерации большого количества одинаковых и плохо приспособленных решений, что может привести к попаданию в локальный оптимум [11]. Поэтому представляет интерес применение эвристических мето-

* Работа выполнена при финансовой поддержке РФФИ (проект 12-01-00474).

дов, инспирированных природными системами, в которых осуществляется поэтапное построение решения задачи (то есть добавление нового оптимального частичного решения к уже построенному частичному оптимальному решению). Одной из последних разработок в области роевого интеллекта является алгоритм пчёл, который довольно успешно используется для нахождения экстремумов сложных многомерных функций [10].

Первые публикации, посвящённые пчелиным алгоритмам для нахождения экстремумов сложных многомерных функций, относятся к 2005 году [12, 13]. В [14] рассмотрена суть этого алгоритма, приведено сравнение алгоритма пчёл с генетическим алгоритмом и алгоритмом, моделирующим поведение муравьев. Описание алгоритма, основанного на поведении колонии пчёл, приводится в [15, 16, 17]. Исследование пчелиных алгоритмов для решения комбинаторных теоретико-графовых задач (задача разбиения графа, раскраска графа, сравнение с другими «биоинспирированными» методами) приводится в [18, 19]. Можно отметить также работы [20, 21], посвящённые рассмотрению алгоритма решения задачи размещения на основе моделирования поведения пчелиной колонии, основным принципам работы простого пчелиного алгоритма, улучшенного пчелиного алгоритма, алгоритма колонии пчёл, моделирующих поведение пчёл в живой природе в поисках нектара. Алгоритм разложения составных чисел на простые сомножители с использованием пчелиных колоний, используемый при криптоанализе алгоритма RSA, описан авторами в [22, 23]. Обзор актуальных алгоритмов и методов роевого интеллекта (муравьиных, пчелиных алгоритмов, метода роя частиц), их отличительные особенности, достоинства, недостатки и возможности практического применения приведены в [24].

В настоящей работе рассматривается метод криптоанализа классических шифров перестановок, основанный на применении к данной задаче отмеченного выше известного метода моделирования поведения пчелиной колонии и относящегося к сравнительно новому классу биоинспирированных оптимизационных методов.

Понятие шифров перестановок. В качестве первичного признака, по которому производится классификация шифров, используется тип преобразования, осуществляемого с открытым текстом при шифровании. Если буквы открытого текста при шифровании только меняются местами друг с другом, то данный шифр относится к классу *шифров перестановок* [25, 26]. Результатом применения данного класса шифров к открытому тексту является строка символов (криптограмма), получаемая путём перестановки символов открытого текста в определённом порядке.

Таким образом, полученная криптограмма включает только те символы, которые составляют открытый текст. Отсюда следует, что задача определения открытого текста заключается в определении позиций для назначения символов криптограммы таким способом, при котором целевая функция, определяющая оптимальность исходного текста, достигает экстремума. То есть данная задача криптоанализа, по сути, является частным случаем задачи о назначениях, цель которой — определить экстремум затрат, необходимых для обмена ресурсами между всеми объектами.

Как и в предыдущих работах [8, 27], для решения задачи криптоанализа определим $X_{ij} = 1$, если объект *i* назначен в пункт *j*, и $X_{ij} = 0$ в противном случае. Предположим, что C_{ij} — вероятность того, что за символом в позиции *i* должен следовать символ в позиции $i + 1$. Кроме этого, введём параметр Q_i, показывающий, насколько фрагмент текста из *i* символов носит осмысленный характер, то есть совпадает с словарным запасом языка. В этом случае оптимизационная модель будет иметь вид:

$$R = \sum_{i=1}^{n} \sum_{j=1}^{n} Q_i C_{ij} X_{ij} \longrightarrow \max. \qquad (1)$$

Элементы C_{ij} задаются в виде матрицы размерности *n* x *n* (*n* — число символов текста). Отметим, что таблицы частот биграмм русского языка приведены, например, в [26].

Таким образом, множество вариантов решений определяется числом перестановок $P = n!$ без повторений n символов, входящих в шифртекст в n позициях. Даная задача имеет комбинаторный характер, что приводит к необходимости использования метаэвристических алгоритмов.

Алгоритм решения. Основу поведения пчелиного роя составляет самоорганизация, обеспечивающая достижение общих целей роя при двухуровневой стратегии поиска. На первом уровне с помощью пчёл-разведчиков формируется множество перспективных областей-источников, на втором уровне с помощью рабочих пчёл-фуражиров осуществляется исследование окрестностей данных областей. При этом основная цель колонии пчёл — найти источник с максимальным количеством нектара [10].

В алгоритме каждое решение представляет собой позицию в пространстве поиска, содержащую определённое количество нектара. При этом данное количество нектара определяет значение целевой функции в этой точке. Решение задачи криптоанализа представляет собой последовательность символов алфавита $x_1, x_2, ..., x_k$, пройденных при перемещении агента-пчёлы в пространстве поиска. Целью поиска является определение оптимальной комбинации (последовательности прохождения) символов с максимальным значением R. Значение целевой функции R определяется комбинациями символов, пройденных агентами-пчёлами, в соответствии с (1).

Таким образом, итерационный процесс поиска решений при реализации алгоритма заключается в последовательном перемещении агентов-пчёл в новые позиции в пространстве поиска.

Основная идея пчелиного алгоритма заключается в том, что все пчёлы на каждой итерации будут выбирать как элитные участки для исследования, так и участки в окрестности элитных, что позволяет разнообразить популяцию решений, а также увеличить вероятность обнаружения решений, близких к оптимальным [21].

Таким образом, в соответствии с [10, 21] общую структуру пчелиного алгоритма представим в следующем виде.

1. Формирование пространства поиска.
2. Оценка целевой функции (ЦФ) пчёл в популяции.
3. Поиск агентами-разведчиками перспективных позиций для поиска в их окрестности.
4. Выбор пчёл с лучшими значениями ЦФ с каждого участка.
5. Отправка пчёл-фуражиров для случайного поиска и оценка их ЦФ.
6. Формирование новой популяции пчёл.
7. Если условия окончания работы алгоритма выполняются, переход к 8, иначе к 2.
8. Конец.

Первым этапом пчелиного алгоритма является формирование пространства поиска. Позиция a_s пространства поиска представляет собой размещенный в пространстве символ алфавита текста. При этом будем предполагать, что каждая пчела-агент содержит в памяти упорядоченный список $E_s = \{e_{si},\ i = 1, 2, \ldots, n\}$ посещённых символов. Список E_s, поставленный в соответствие каждому символу в пространстве поиска, который посетила пчела, фактически представляет решение — исходный текст, для которого может быть определена ЦФ. В случае текстов достаточно большой размерности для оценки ЦФ может быть применена функция Якобсена, использованная для криптоанализа в [28–30]. В случае строк незначительной длины для оценки качества расшифрования может быть использована формула (1).

Основной операцией пчелиного алгоритма является исследование окрестностей перспективных позиций в пространстве поиска. Пусть пространство поиска, в котором размещены символы алфавита шифртекста, представляет собой прямоугольную матрицу A размером m x m. Назовём окрестностью размера λ позиции a_s множество позиций a_{si}, находящихся на расстоянии (определяемом как количество элементов матрицы), не превышающем λ, от позиции a_s.

Таким образом, для реализации пчелиного алгоритма необходимо задание следующих параметров: количество пчёл-агентов *N*, количество итераций *L*, количество агентов-разведчиков n_r, количество агентов-фуражиров n_f, значение максимального размера окрестности $\lambda_{макс}$.

На $l = 1$ итерации алгоритма n_r агентов-разведчиков случайным образом размещаются в пространстве поиска, то есть выбирается произвольным образом n_r символов в матрице *A*. Поскольку на начальном этапе фрагменты текста не определены (состоят из одного символа), значение ЦФ *R* на начальном этапе полагается равным малому положительному числу.

На следующем шаге алгоритма выбирается n_b базовых (лучших) решений, у которых значения ЦФ *R* не хуже, чем значения ЦФ у любого другого решения. На начальной итерации этот выбор осуществляется, очевидно, случайным образом. Формируется множество базовых позиций $A_b = \{a_{bi}\}$ в пространстве поиска, соответствующих базовым решениям.

На следующем шаге алгоритма в окрестности каждой базовой позиции направляется заданное число пчёл-фуражиров. Отметим, что в [10] предлагается три основных подхода к определению числа агентов-фуражиров, направляемых в окрестности базовых позиций: равномерное распределение фуражиров по базовым позициям, распределение пропорционально значению ЦФ позиции и вероятностный выбор.

После выбора агентом-фуражиром n_{fi} базовой позиции a_i реализуется случайный выбор позиции a_s, расположенной в окрестности базовой позиции a_i. При этом случайным образом определяется значение окрестности λ в границах $1 \le \lambda \le \lambda_{макс}$.

Таким образом, будем предполагать, что каждая пчела-агент содержит в памяти упорядоченный список E_s посещённых символов пространства поиска с определённой для этого списка ЦФ, и данная последовательность ставится в соответствие последнему посещённому пчелой-агентом символу (позиции) пространства поиска. Аналогично [10] введём понятие области D_i, представляющей собой $D_i = a_i \cup O_i$, где O_i — множество позиций, выбранных агентами-фуражирами в окрестности позиции a_i. В каждой области D_i выбирается позиция (символ) *a* с лучшей оценкой ЦФ R_i^*, которую назовём оценкой области D_i. Среди всех оценок областей R_i^* выбирается лучшая оценка R_i^* и соответствующее решение (список E_s). Лучшее решение (вариант исходного текста) запоминается, и осуществляется переход к следующей итерации.

На последующих итерациях алгоритма n_{rl} агентов-разведчиков отправляются на поиск новых позиций ($n_{rl} < n_r$). Множество базовых позиций $A_b(l)$ формируется из двух частей $A_{b1}(l)$ и $A_{b2}(l)$:

$$A_b(l) = A_{b1}(l) \cup A_{b2}(l).$$

Часть $A_{b1}(l)$ содержит n_{b1} лучших решений a^*, найденных в каждой из областей на итерации $l-1$, часть $A_{b2}(l)$ содержит n_{b2} лучших решений из n_{rl} позиций, найденных пчёлами-разведчиками на итерации *l*.

Следовательно, $n_{b1} + n_{b1} = n_b$. Далее, как и на первой итерации, определяется число агентов-фуражиров, отправляемых в окрестности каждой базовой позиции. Каждым агентом-фуражиром n_{fi} выбирается базовая позиция $a_i(l)$, а также позиция $a_s(l)$, расположенная в окрестности этой базовой позиции. Формируются области $D_i(l)$. В каждой области $D_i(l)$ выбирается лучшая позиция a_i^* с лучшей оценкой ЦФ R_i^*, среди оценок R_i^* выбирается лучшая R^*. Если $R^*(l)$ предпочтительней, чем $R^*(l-1)$, то соответствующее решение запоминается, и осуществляется переход к следующей итерации.

Таким образом, алгоритм криптоанализа на основе пчелиной колонии можно сформулировать в следующем виде:

1. Определить начальные параметры алгоритма: количество пчёл-агентов N; количество итераций L; количество агентов-разведчиков n_r; количество агентов-фуражиров n_f; значение максимального размера окрестности $\lambda_{макс}$; количество базовых позиций n_b; n_{b1} — количество базовых позиций, формируемых из лучших позиций a^*, найденных на $l-1$ итерации; n_{rl} — количество агентов-разведчиков, выбирающих случайным образом новые позиции на итерациях 2, 3, …, L; n_{b2} — количество базовых позиций, формируемых из n_{rl} новых лучших позиций, найденных агентами-разведчиками на l итерации.

2. Задать номер итерации $l=1$.

3. Разместить n_r агентов-разведчиков случайным образом в пространстве поиска, то есть выбрать произвольным образом n_r символов в матрице A. Положить значение ЦФ R равным малому положительному числу.

4. Сформировать множество n_b базовых решений и соответствующее множество базовых позиций $A_b=\{a_{bi}\}$ с лучшими значениями ЦФ R.

5. $f=1$ (задание номера агента-фуражира).

6. Выбор базовой позиции $a_i \in A_b$.

7. Выбор позиции $a_s(l)$, расположенной в окрестности базовой позиции a_i, не совпадающей с ранее выбранными на данной итерации позициями, и соответствующего решения (списка E_s).

8. Включить позицию a_s в множество O_i (где O_i — множество позиций, выбранных агентами-фуражирами в окрестности позиции a_i).

9. Для всех вновь включенных позиций рассчитать и поставить им в соответствие решения E_s и соответствующие значения ЦФ R.

10. $f=f+1$, если $f>n_f$, переход к п. 11, иначе к п. 6.

11. Сформировать для каждой базовой позиции a_i области $D_i=a_i \cup O_i$.

12. В каждой области D_i выбрать лучшую позицию a_i^* с лучшим значением ЦФ R_i^*.

13. Среди всех значений R_i^* выбрать лучшее значение R^* и соответствующее решение (список позиций E^*).

14. Если значение $R^*(l)$ предпочтительней значения $R^*(l-1)$, то сохранить значение $R^*(l)$, в противном случае сохранённым остается значение $R^*(l-1)$.

15. Если $l<L$ (не все итерации пройдены), $l=l+1$, переход к п. 16, иначе к п. 20.

16. Начать формирование множества базовых позиций. Во множество A_{b1} включается n_{b1} лучших позиций, найденных агентами среди позиций a_i^* в каждой из областей D_i на итерации $l-1$.

17. Разместить n_{rl} агентов-разведчиков случайным образом в пространстве поиска для выбора n_{rl} позиций в пространстве поиска.

18. Включить в множество A_{b2} n_{b2} лучших позиций из множества n_{rl} новых позиций, найденных агентами-разведчиками на итерации l. Следовательно, $n_{b2}+n_{b1}=n_b$.

19. Определить множество базовых позиций на итерации l как $A_b(l)=A_{b1}(l) \cup A_{b2}(l)$. Перейти к п. 5.

20. Конец работы алгоритма, список E^* — вариант исходного текста с лучшим значением ЦФ R^*.

Демонстрационный пример. Рассмотрим пример реализации представленного выше алгоритма криптоанализа, аналогичный приведённому в [8, 26]. Пусть задана строка символов: *БКСОА.* Тре-

буется определить возможную перестановку символов, входящую в словарный состав языка. Матрица C_{ij}, показывающая частоту биграмм, приведённая в [8, 26], показана на рис. 1.

Определим пространство поиска в виде матрицы *A* размером 11 х 11, заполненной символами из алфавита шифртекста, размещёнными случайным образом в ячейках с соответствующими координатами (рис. 2). При реализации алгоритма будем предполагать, что выбор позиции a_s, расположенной в окрестности базовой позиции a_i, производится пропорционально значению ЦФ *R* полученного решения (списка E_s).

	Б	**К**	**С**	**О**	**А**
Б	**0,01**	**0,01**	**0,1**	**0,5**	**0,6**
К	**0,01**	**0,01**	**0,01**	**0,5**	**0,4**
С	**0,05**	**0,08**	**0,05**	**0,6**	**0,3**
О	**0,6**	**0,3**	**0,5**	**0,02**	**0,1**
А	**0,6**	**0,6**	**0,6**	**0,1**	**0,01**

Рис. 1. Матрица *C*, элемент C_{ij} которой определяет вероятность соседства в тексте символов *i* и *j*

11	О	А	О	А	С	О	О	О	К	А	Б
10	Б	С	К	А	Б	О	Б	Б	Б	О	С
9	А	С	А	К	С	***Б***	К	О	С	О	С
8	К	А	С	К	Б	Б	А	О	К	Б	А
7	С	Б	Б	А	А	К	К	С	К	А	Б
6	***А***	Б	О	К	***К***	А	О	А	К	Б	К
5	Б	А	Б	К	О	А	А	Б	С	С	Б
4	***А***	Б	А	С	А	А	***С***	А	А	***О***	С
3	О	О	С	Б	К	Б	Б	К	Б	О	Б
2	О	К	О	К	А	С	С	О	Б	С	А
1	Б	К	Б	О	Б	К	А	Б	С	А	***К***
	1	2	3	4	5	6	7	8	9	10	11

Рис. 2. Матрица *A*, представляющая пространство поиска для пчелиного алгоритма

Итерация 1.

1. Определим количество агентов-разведчиков $n_r = 7$ и разместим их случайным образом в пространстве поиска, то есть выберем произвольным образом n_r символов в матрице *A*. Пусть это будут символы К(5, 6), С(7, 4), А(1, 4), А(1, 6), Б(6, 9), О(10, 4), К(11, 1), выделенные на рис. 2 курсивом. Положим значение ЦФ *R* для всех позиций равным малому положительному числу *R* = 0,001.

2. Определим множество базовых решений $n_b = 5$ и соответствующие базовые позиции с лучшими значениями ЦФ (на этом этапе их выберем произвольно). Пусть это будут позиции $A_b = \{\text{К}(5,\ 6),\ \text{Б}(6,\ 9),\ \text{С}(7,\ 4),\ \text{О}(10,\ 4),\ \text{А}(1,\ 4)\}$.

3. Определим число агентов-фуражиров $n_f = 6$ и размер окрестности $\lambda_{макс} = 3$. Пусть базовые позиции выбираются в следующем порядке А, О, Б, К, С, О и им ставятся в соответствие следующие позиции a_s: А→К(2, 2); О→А(9, 4); Б→К(7, 9); К→С(4, 4); С→К(8, 3); О→А(11, 2). Таким образом, на данном шаге мы будем иметь следующий список позиций, решений и соответствующих значений ЦФ: позиции К(5, 6), Б(6, 9), С(7, 4), О(10, 4), А(1, 4), $R = 0,001$, список *E* состоит из одного символа; позиция К(2, 2), $E = \{\text{АК}\}$, $R = 0,6$; позиция А(9, 4), $E = \{\text{ОА}\}$, $R = 0,1$; позиция К(7, 9), $E = \{\text{БК}\}$, $R = 0,01$; позиция С(4, 4), $E = \{\text{КС}\}$, $R = 0,01$; позиция К(8, 3), $R = 0,08$; позиция А(11, 2), $E = \{\text{ОА}\}$, $R = 0,1$. Области D_i будут иметь вид:

$D_1 = \{А(1, 4), К(2, 2)\}$; $D_2 = \{О(10, 4), А(9, 4), А(11, 2)\}$; $D_3 = \{Б(6, 9), К(7, 9)\}$; $D_4 = \{К(5, 6), С(4, 4)\}$; $D_5 = \{С(7, 4), К(8, 3)\}$.

4. В каждой области D_i выберем лучшую позицию a_i^* с лучшим значением ЦФ R_i^*. Получим D_1→К(2, 2), R_1^*=0,6; D_2→А(9, 4), R_2^*=0,1; D_3→К(7, 9), R_3^*=0,01; D_4→С(4, 4), R_4^*=0,01; D_5→К(8, 3), R_5^*=0,08.

5. Выбирая среди всех значений R_i^* лучшее значение, получим, что $R^*(1)$=0,6; $E^*(1) = \{АК\}$.

6. Полагаем $l = 2$.

Итерация 2.

1. Определим число $n_{b1} = 3$. Во множество A_{b1} включается n_{b1} лучших позиций, найденных агентами среди позиций a_i^* в каждой из областей D_i на итерации 1. Получим $A_{b1} = \{К(2, 2), А(9, 4), К(8, 3)\}$. Этим позициям поставлены в соответствие списки, представленные на рис. 3.

2. Определим количество агентов-разведчиков $n_{rl} = 5$ и разместим их произвольным образом в пространстве поиска. Пусть будут выбраны символы О(7, 6), О(10, 3), Б(8, 1), А(8, 6), К(3, 10).

3. Включение в множество A_{b2} $n_{b2} = 2$ лучших позиций из множества n_{rl} новых позиций, найденных агентами-разведчиками на итерации 2. Пусть $A_{b2} = \{О(10, 3), Б(8, 1)\}$. Таким образом, $n_{b1} + n_{b2} = 5$ и $A_b = \{К(2, 2), А(9, 4), К(8, 3), О(10, 3), Б(8, 1)\}$.

4. Как и ранее, полагаем $n_r = 6$ и размер окрестности $\lambda_{макс}$ = 3. Пусть базовым позициям ставятся в соответствие следующие позиции из их окрестностей: К(2, 2)→О(2, 3); А(9, 4)→Б(8, 5); К(8, 3)→О(8, 2); О(10, 3)→А(11, 2); Б(8, 1)→А(10, 1); О(10, 3)→С(11, 4). Таким образом, на данном шаге мы будем иметь следующий список позиций, решений и соответствующих значений ЦФ: позиция К(2, 2), $E = \{АК\}$, $R = 0,6$; позиция А(9, 4), $E = \{ОА\}$, $R = 0,1$; позиция К(8, 3), $E = \{СК\}$, $R = 0,08$; позиции О(10, 3), Б(8, 1), $R = 0,001$, список E состоит из одного символа; позиция О(2, 3), $E = \{АКО\}$, $R = 1,1$; позиция Б(8, 5), $E = \{ОАБ\}$, $R = 0,7$; позиция О(8, 2), $E = \{СКО\}$, $R = 0,58$; позиция А(11, 2), $E = \{ОА\}$, $R = 0,1$; позиция А(10, 1), $E = \{БА\}$, $R = 0,6$; позиция С(11, 4), $E = \{ОС\}$, $R = 0,5$. Отметим, что фрагменты текста, состоящие из трёх и более символов, умножим на значения Q_i в соответствие с частотой встречаемости. Для списков АКО, ОАБ, СКО положим соответственно $Q = 0,6$; $Q = 0,6$; $Q = 1$. В этом случае для позиции О(2, 3), $E = \{АКО\}$, $R = 0,66$; для позиции Б(8, 5), $E = \{ОАБ\}$, $R = 0,42$; для позиции О(8, 2), $E = \{СКО\}$, $R = 0,58$. Области D_i будут иметь вид $D_1 = \{К(2,2), О(2,3)\}$; $D_2 = \{А(9,4), Б(8,5)\}$; $D_3 = \{К(8,3), О(8,2)\}$; $D_4 = \{О(10,3), А(11,2), С(11,4)\}$; $D_5 = \{Б(8,1), А(10,1)\}$.

5. В каждой области D_i выберем лучшую позицию a_i^* с лучшим значением ЦФ R_i^*. Получим D_1→О(2, 3), R_1^*=0,66; D_2→Б(8, 5), R_2^*=0,42; D_3→О(8, 2), R_3^*=0,58; D_4→С(11, 4), R_4^*=0,5; D_5→А(10, 1), R_5^*=0,6.

6. Выбирая среди всех значений R_i^* лучшее значение, получим, что $R^*(2) = 0,66$; $E^*(1) = \{АКО\}$.

7. Полагаем $l = 3$.

11	О	А	О	А	С	О	О	О	К	А	Б
10	Б	С	К	А	Б	О	Б	Б	Б	О	С
9	А	С	А	К	С	Б	К	О	С	О	С
8	К	А	С	К	Б	Б	А	О	К	Б	А
7	С	Б	Б	А	А	К	К	С	К	А	Б
6	А	Б	О	К	К	А	О	А	К	Б	К
5	Б	А	Б	К	О	А	А	Б	С	С	Б
4	А	Б	А	С	А	А	***С***	А	***ОА***	О	С
3	О	О	С	Б	К	Б	Б	***СК***	Б	О	Б
2	О	***АК***	О	К	А	С	С	О	Б	С	А
1	Б	К	Б	О	Б	К	А	Б	С	А	К
	1	2	3	4	5	6	7	8	9	10	11

Рис. 3. Матрица *A*, представляющая пространство поиска для пчелиного алгоритма после 1 итерации

Итерация 3.

1. Определим, как и ранее, число $n_{b1} = 3$. Во множество A_{b1} включается n_{b1} лучших позиций, найденных агентами среди позиций a_i^* в каждой из областей D_i на итерации 2. Получим $A_{b1} = \{\text{О}(2,\ 3),\ \text{А}(10,\ 1),\ \text{О}(8,\ 2)\}$. Этим позициям поставлены в соответствие списки, представленные на рис. 4.

2. Определим количество агентов-разведчиков $n_{rl} = 5$ и разместим их произвольным образом в пространстве поиска. Пусть будут выбраны символы К(2, 2), О(1, 11), К(8, 3), А(10, 11), А(3, 9).

3. Включение в множество A_{b2} $n_{b2} = 2$ лучших позиций из множества n_{rl} новых позиций, найденных агентами-разведчиками на итерации 2. На данной итерации, $A_{b2} = \{\text{К}(2,\ 2),\ \text{К}(8,\ 3)\}$. Таким образом, $n_{b1} + n_{b2} = 5$ и $A_b = \{\text{О}(2,\ 3),\ \text{А}(10,\ 1),\ \text{О}(8,\ 2),\ \text{К}(2,\ 2),\ \text{К}(8,\ 3)\}$.

4. Полагаем $n_f = 6$ и размер окрестности $\lambda_{макс} = 3$. Поставим базовым позициям в соответствие следующие позиции из их окрестностей: О(2, 3)→Б(4, 3); А(10, 1)→К(11, 1); О(8, 2)→А(10, 1); К(2, 2)→О(3, 2); К(8, 3)→А(9, 4); О(8, 2)→Б(8, 1). Таким образом, получаем следующий список позиций, решений и соответствующих значений ЦФ: позиция О(2, 3), $E = \{\text{АКО}\}$, $R = 1{,}1$; позиция А(10, 1), $E = \{\text{БА}\}$, $R = 0{,}6$; позиция О(8, 2), $E = \{\text{СКО}\}$, $R = 0{,}58$; позиция К(2, 2), $E = \{\text{АК}\}$, $R = 0{,}6$; позиция К(8, 3), $E = \{\text{СК}\}$, $R = 0{,}08$; позиция Б(4, 3), $E = \{\text{АКОБ}\}$, $R = 1{,}7$; позиция К(11, 1), $E = \{\text{БАК}\}$, $R = 1{,}2$; позиция А(10, 1), $E = \{\text{СКОБА}\}$, $R = 1{,}78$; позиция О(3, 2), $E = \{\text{АКО}\}$, $R = 1{,}1$; позиция О(9, 4), $E = \{\text{СКООА}\}$, $R = 0{,}7$; позиция Б(8, 1), $E = \{\text{СКОБ}\}$, $R = 1{,}18$. Фрагменты текста, состоящие из трёх и более символов, умножим на значения Q_i в соответствие с частотой встречаемости. Для списков АКО, СКО, АКОБ, БАК, СКОБА, СКООА, СКОБ положим соответственно $Q = 0{,}6$; $Q = 1$; $Q = 0{,}7$; $Q = 1$; $Q = 1$; $Q = 0{,}8$; $Q = 1$. В этом случае для позиции О(2, 3), $E = \{\text{АКО}\}$, $R = 0{,}66$; для позиции О(8, 2), $E = \{\text{СКО}\}$, $R = 0{,}58$; для позиции Б(4, 3), $E = \{\text{АКОБ}\}$, $R = 1{,}19$; для позиции К(11, 1), $E = \{\text{БАК}\}$, $R = 1{,}2$; для позиции А(10, 1), $E = \{\text{СКОБА}\}$, $R = 1{,}78$; для позиции О(3, 2), $E = \{\text{АКО}\}$, $R = 0{,}66$; для позиции О(9, 4), $E = \{\text{СКООА}\}$, $R = 0{,}56$; для позиции Б(8, 1), $E = \{\text{СКОБ}\}$, $R = 1{,}18$.

Таким образом, на данной итерации позиции А(10, 1) соответствует список $E = \{\text{СКОБА}\}$ с максимальным значением ЦФ R = 1,78. Данная позиция, очевидным образом, будет включена в

множество A_b для следующей итерации алгоритма, и списки с лучшим значением ЦФ будут осуществлять постепенное заполнение популяции решений.

11	О	А	О	А	С	О	О	О	К	А	Б
10	Б	С	К	А	Б	О	Б	Б	Б	О	С
9	А	С	А	К	С	Б	К	О	С	О	С
8	К	А	С	К	Б	Б	А	О	К	Б	А
7	С	Б	Б	А	А	К	К	С	К	А	Б
6	А	Б	О	К	К	А	О	А	К	Б	К
5	Б	А	Б	К	О	А	А	Б	С	С	Б
4	А	Б	А	С	А	А	***С***	А	***ОА***	О	С
3	О	***АКО***	С	Б	К	Б	Б	***СК***	Б	О	Б
2	О	***АК***	О	К	А	С	С	***СКО***	Б	С	А
1	Б	К	Б	О	Б	К	А	Б	С	***БА***	К
	1	2	3	4	5	6	7	8	9	10	11

Рис. 4. Матрица *A*, представляющая пространство поиска для пчелиного алгоритма после 2 итерации

Заключение. Рассмотрена возможность применения метода пчелиной колонии для решения задачи криптоанализа перестановочного шифра, приведён пример, иллюстрирующий схему реализации алгоритма. В отличие от классических подходов, описанных, например, в [10, 15], в задаче криптоанализа осуществляется поиск экстремума немонотонной функции, то есть построение списка *E* с наилучшим значением ЦФ не означает его оптимальность на последующих итерациях. В связи с этим при реализации алгоритма может оказаться целесообразным учитывать следующие отличительные особенности:

- пространство поиска должно быть достаточно большим для предотвращения попадания в локальный оптимум;
- на каждой последующей итерации сохраняются списки, поставленные в соответствие каждому символу пространства поиска на предыдущей итерации (как показано на рис. 4);
- при наличии временных и вычислительных ресурсов подсчёт целевой функции для каждого списка может производиться после достижения списком длины шифруемого текста (как при реализации муравьиного алгоритма криптоанализа, описанного в [8]);
- для предотвращения попадания в локальный оптимум могут также использоваться операторы, применяемые в эволюционном моделировании (например, оператор мутации).

Заметим, что при достаточно большом количестве итераций количество списков становится достаточно большим, и работа алгоритма может осуществляться аналогично работе генетического алгоритма. Отметим также, что поскольку задача криптоанализа является оптимизационной задачей и в общем случае может интерпретироваться как задача формирования упорядоченных списков, то, как отмечено в [10], алгоритмы пчелиных колоний могут являться эффективным способом поиска рациональных решений для данного класса задач.

Библиографический список

1. Макконел, Д. Основы современных алгоритмов / Д. Макконел. — Москва : Техносфера, 2004. — 368 с.

2. Родзин, С. И. Интеллектуальные системы. О некоторых алгоритмах, инспирированных природными системами : коллективная монография / С. И. Родзин. — Москва : Физматлит, 2009. — С. 34–45.

3. Курейчик, В. В. Концепция природных вычислений, инспирированных природными системами / В. В. Курейчик, В. М. Курейчик, С. И. Родзин // Известия ЮФУ. — 2009. — № 4. — С. 16–24.

4. Сергеев, А. С. Исследование возможности организации криптографической атаки с использованием эволюционной оптимизации и квантового поиска при разработке систем передачи и защиты информации / А. С. Сергеев // Теоретические и прикладные вопросы современных информационных технологий : мат-лы 6 Всероссийской НТК. — Улан-Удэ, 2005. — С. 61–65.

5. Биоинспирированные алгоритмы криптоанализа асимметричных алгоритмов шифрования на основе факторизации составных чисел / А. С. Сергеев [и др.] // Информационная безопасность — актуальная проблема современности. Совершенствование образовательных технологий подготовки специалистов в области информационной безопасности : сб. трудов. — Краснодар, 2011. — С. 41–47.

6. Сергеев, А. С. Применение методов генетического поиска для организации криптоанализа блочных криптосистем на примере стандарта DES / А. С. Сергеев // Научная мысль Кавказа : Приложение. — 2006. — № 15. — С. 185–193.

7. Сергеев, А. С. Исследование и разработка методов генетического поиска для организации криптоанализа блочных криптосистем в системах управления безопасностью и защиты информации на примере стандарта шифрования DES / А. С. Сергеев // Третья Международная конференция по проблемам управления : Пленарные доклады и избранные труды. — Москва : Ин-т проблем управления, 2006. — С. 328–335.

8. Фатхи, В. А. Исследование возможности применения алгоритма муравьиных колоний для реализации криптоанализа шифров перестановок / В. А. Фатхи, А. С. Сергеев // Вестник Дон. гос. техн. ун-та. — 2011. — Т. 11, № 1 (52). — С. 10–20.

9. Чернышёв, Ю. О. Исследование и разработка методов генетического поиска для реализации криптоанализа алгоритма IDEA и решения основных теоретико-числовых задач криптографии / Ю. О. Чернышёв, А. С. Сергеев, Н. Н. Венцов // Вестник РГУПС. — 2009. — № 3 (35). — С. 70–79.

10. Лебедев, В. Б. Модели адаптивного поведения колонии пчёл для решения задач на графах / В. Б. Лебедев // Известия ЮФУ. — 2012. — № 7. — С. 42–49.

11. Лебедев, О. Б. Трассировка в канале методом муравьиной колонии / О. Б. Лебедев // Известия ЮФУ. — 2009. — № 4. — С. 46–52.

12. The Bees Algorithm. Technical Note, Manufacturing Engineering Centre. Cardiff University, UK, 2005.

13. An IDEA based on honey bee swarm for numerical optimization, technical report. Erciyes University, Engineering Faculty. Computer Engineering Department, 2005.

14. The Bees Algorithm. — A Novel Tool for Complex Optimisation Problems. Manufacturing Engineering Centre. — Cardiff University, Cardiff CF24 3AA, UK.

15. Алгоритм пчёл для оптимизации функции [Электронный ресурс]. — Режим доступа : http://jenyay.net/Programming/Bees (дата обращения : 24.05.2013).

16. Алгоритм пчёл для оптимизации функции [Электронный ресурс]. — Режим доступа : http://lit999.narod.ru/soft/ga/index.html (дата обращения : 24.05.2013).

17. Курейчик, В. В. Роевой алгоритм в задачах оптимизации / В. В. Курейчик, Д. Ю. Запорожец // Известия ЮФУ. — 2010. — № 7 (108). — С. 28–32.

18. Курейчик, В. М. Использование пчелиных алгоритмов для решения комбинаторных задач [Электронный ресурс] / В. М. Курейчик, А. А. Кажаров. — Режим доступа : http://archive.nbuv.gov.ua/portal/natural/ii/2010_3/AI_2010_3/6/00_Kureychik_Kazharov.pdf (дата обращения : 24.05.2013).

19. Курейчик, В. М. Применение пчелиных алгоритмов для раскраски графов / В. М. Курейчик, А. А. Кажаров // Известия ЮФУ. — 2010. — № 12 (113). — С. 7–12.

20. Лебедев, Б. К. Размещение на основе метода пчелиной колонии / Б. К. Лебедев, В. Б. Лебедев // Известия ЮФУ. — 2010. — № 12 (113). — С. 12–19.

21. Курейчик, В. В. Эволюционная оптимизация на основе алгоритма колонии пчёл / В. В. Курейчик, Е. Е. Полупанова // Известия ЮФУ. — 2009. — № 12 (101). — С. 41–46.

22. Биоинспирированные методы криптоанализа асимметричных алгоритмов шифрования на основе факторизации составных чисел / А. С. Сергеев [и др.] // Вестник Дон. гос. техн. ун-та. — 2011. — Т. 11, № 9 (60). — С. 1544–1554.

23. Чернышёв, Ю. О. Применение биоинспирированных методов оптимизации для реализации криптоанализа классических симметричных и асимметричных криптосистем / Ю. О. Чернышёв, А. С. Сергеев, Е. О. Дубров // Системный анализ в проектировании и управлении : сб. науч. трудов 16-й Междунар. науч.-практ. конф. — Санкт-Петербург, 2012. — С. 112–122.

24. Зайцев, А. А. Обзор эволюционных методов оптимизации на основе роевого интеллекта / А. А. Зайцев, В. В. Курейчик, А. А. Полупанов // Известия ЮФУ. — 2010. — № 12 (113). — С. 7–12.

25. Романец, Ю. В. Защита информации в компьютерных системах и сетях / Ю. В. Романец, П. А. Тимофеев, В. Ф. Шаньгин. — Москва : Радио и связь, 2001. — 376 с.

26. Основы криптографии / А. П. Алферов [и др.]. — Москва : Гелиос АРВ, 2002. — 480 с.

27. Чернышев, Ю. О. Применение алгоритма муравьиных колоний для реализации криптоанализа шифров перестановок / Ю. О. Чернышёв, А. С. Сергеев, Е. О. Дубров // Научная сессия, посвящённая Дню радио : сб. докладов 67-й Всероссийской конференции с Международным участием. — Москва, 2012. — С. 71–75.

28. Морозенко, В. В. Генетический алгоритм для криптоанализа шифра Вижинера [Электронный ресурс] / В. В. Морозенко, Г. О. Елисеев. — Режим доступа : http://vestnik.psu.ru/ /files/articles/132_6410.p (дата обращения : 24.05.2013).

29. Городилов, А. Ю. Криптоанализ тригонометрического шифра с помощью генетического алгоритма [Электронный ресурс] / А. Ю. Городилов, А. А. Митраков. — Режим доступа : http://vestnik.psu.ru/files/articles/260_27019.p (дата обращения : 24.05.2013).

30. Городилов, А. Ю. Криптоанализ перестановочного шифра с помощью генетического алгоритма [Электронный ресурс] / А. Ю. Городилов. — Режим доступа : http://vestnik.psu.ru/ /files/articles/8_83883 (дата обращения : 24.05.2013).

Материал поступил в редакцию 17.05.2013.

References

1. McConnell, J. Osnovy sovremennykh algoritmov. [Analysis of algorithms.] Moscow : Tehnosfera, 2004, 368 p. (in Russian).

2. Rodzin, S. I. Intellektualnyye sistemy. O nekotorykh algoritmakh, inspirirovannykh prirodnymi sistemami : kollektivnaya monografiya. [Intelligent systems. On some algorithms inspired by natural systems : multi-author book.] Moscow : Fizmatlit, 2009, pp. 34–45 (in Russian).

3. Kureychik, V. V., Kureychik, V. M., Rodzin, S. I. Kontseptsiya prirodnykh vychisleniy, inspirirovannykh prirodnymi sistemami. [Concept of natural calculations inspired by natural systems.] Izvestiya YuFU, 2009, no. 4, pp. 16–24 (in Russian).

4. Sergeyev, A. S. Issledovaniye vozmozhnosti organizatsii kriptograficheskoy ataki s ispolzovaniyem evolyutsionnoy optimizatsii i kvantovogo poiska pri razrabotke sistem peredachi i zashchity informatsii. [Study into feasibility of cryptographic attack using evolutional optimization and quantum search under developing data transfer and protection systems.] Teoreticheskiye i prikladnyye voprosy sovremennykh informatsionnykh tekhnologiy : materialy 6 Vserossiyskoy NTK. [Theory and application of modern information technologies: Proc. VI All-Russ. Sci. Tech. Conf.] Ulan-Ude, 2005, pp. 61–65 (in Russian).

5. Sergeyev, A. S., et al. Bioinspirirovannyye algoritmy kriptoanaliza asimmetrichnykh algoritmov shifrovaniya na osnove faktorizatsii sostavnykh chisel. [Bioinspired algorithms of asymmetric encryption algorithm cryptanalysis based on composite factorization.] Informatsionnaya bezopasnost — aktualnaya problema sovremennosti. Sovershenstvovaniye obrazovatelnykh tekhnologiy podgotovki spetsialistov v oblasti informatsionnoy bezopasnosti : sbornik trudov. [Cybersecurity — contemporary pressing challenge. Educational technology development for specialist training in information security : coll. of research papers.] Krasnodar, 2011, pp. 41–47 (in Russian).

6. Sergeyev, A. S. Primeneniye metodov geneticheskogo poiska dlya organizatsii kriptoanaliza blochnykh kriptosistem na primere standarta DES. [Application of genetic search techniques for block cryptosystem cryptanalysis with the reference to DES standard.] Nauchnaya mysl Kavkaza : Prilozheniye, 2006, no. 15, pp. 185–193 (in Russian).

7. Sergeyev, A. S. Issledovaniye i razrabotka metodov geneticheskogo poiska dlya organizatsii kriptoanaliza blochnykh kriptosistem v sistemakh upravleniya bezopasnostyu i zashchity informatsii na primere standarta shifrovaniya DES. [R&D of genetic search techniques for block cryptosystem cryptanalysis in control data transfer and protection systems with the reference to DES standard.] Tretya Mezhdunarodnaya konferentsiya po problemam upravleniya : Plenarnyye doklady i izbrannyye trudy. [III Int. Sci. Conf. on control problems : Plenary reports and selecta.] Moscow : Institut problem upravleniya, 2006, pp. 328–335 (in Russian).

8. Fatkhi, V. A., Sergeyev, A. S. Issledovaniye vozmozhnosti primeneniya algoritma muravinykh koloniy dlya realizatsii kriptoanaliza shifrov perestanovok. [Application of ant colony algorithm for realization of transposition ciphers crypt analysis.] Vestnik of DSTU, 2011, vol. 11, no. 1 (52), pp. 10–20 (in Russian).

9. Chernyshev, Y. O., Sergeyev, A. S., Ventsov, N. N. Issledovaniye i razrabotka metodov geneticheskogo poiska dlya realizatsii kriptoanaliza algoritma IDEA i resheniya osnovnykh teoretiko-chislovykh zadach kriptografii. [R&D of genetic search techniques for IDEA algorithm cryptanalysis and solution to basic number-theoretic cryptographical problems.] Vestnik RGUPS, 2009, no. 3 (35), pp. 70–79 (in Russian).

10. Lebedev, V. B. Modeli adaptivnogo povedeniya kolonii pchel dlya resheniya zadach na grafakh. [Bee colony adaptive behaviour models for solving graph problems.] Izvestiya YuFU, 2012, no. 7, pp. 42–49 (in Russian).

11. Lebedev, O. B. Trassirovka v kanale metodom muravinoy kolonii. [Channel routing through ant colony method.] Izvestiya YuFU, 2009, no. 4, pp. 46–52 (in Russian).

12. The Bees Algorithm. Technical Note, Manufacturing Engineering Centre. Cardiff University, UK, 2005.

13. An IDEA based on honey bee swarm for numerical optimization, technical report. Erciyes University, Engineering Faculty. Computer Engineering Department, 2005.

14. The Bees Algorithm. — A Novel Tool for Complex Optimisation Problems. Manufacturing Engineering Centre. — Cardiff University, Cardiff CF24 3AA, UK.

15. Algoritm pchel dlya optimizatsii funktsii. [Bee algorithm for function optimization.] Available at : http://jenyay.net/Programming/Bees (accessed : 24.05.2013) (in Russian).

16. Algoritm pchel dlya optimizatsii funktsii. [Bee algorithm for function optimization.]. Available at : http://lit999.narod.ru/soft/ga/index.html (accessed : 24.05.2013) (in Russian).

17. Kureychik, V. V., Zaporozhets, D. Y. Royevoy algoritm v zadachakh optimizatsii. [Swarm algorithm in optimization problems.] Izvestiya YuFU, 2010, no. 7 (108), pp. 28–32 (in Russian).

18. Kureychik, V. M., Kazharov, A. A. Ispolzovaniye pchelinykh algoritmov dlya resheniya kombinatornykh zadach. [Bee algorithm application for combinatorial problem solution.] Available at :

http://archive.nbuv.gov.ua/portal/natural/ii/2010_3/AI_2010_3/6/00_Kureychik_Kazharov.pdf (accessed : 24.05.2013) (in Russian).

19. Kureychik, V. M., Kazharov, A. A. Primeneniye pchelinykh algoritmov dlya raskraski grafov. [Bee algorithm application for graph coloring.] Izvestiya YuFU, 2010, no. 12 (113), pp. 7–12 (in Russian).

20. Lebedev, B. K., Lebedev, V. B. Razmeshcheniye na osnove metoda pchelinoy kolonii. [Allocation based on bee colony technique.] Izvestiya YuFU, 2010, no. 12 (113), pp. 12–19 (in Russian).

21. Kureychik, V. V., Polupanova, E. E. Evolyutsionnaya optimizatsiya na osnove algoritma kolonii pchel. [Evolutionary optimization based on bee colony technique.] Izvestiya YuFU, 2009, no. 12 (101), pp. 41–46 (in Russian).

22. Sergeyev, A. S., et al. Bioinspirirovannyye metody kriptoanaliza asimmetrichnykh algoritmov shifrovaniya na osnove faktorizatsii sostavnykh chisel. [Cryptanalysis bioinspired methods of asymmetric key on the basis of composite number factorization.] Vestnik of DSTU, 2011, vol. 11, no. 9 (60), pp. 1544–1554 (in Russian).

23. Chernyshev, Y. O., Sergeyev, A. S., Dubrov, E. O. Primeneniye bioinspirirovannykh metodov optimizatsii dlya realizatsii kriptoanaliza klassicheskikh simmetrichnykh i asimmetrichnykh kriptosistem. [Bioinspired optimization methods application for implementing cryptanalysis of classical symmetric and asymmetric cryptosystems.] Sistemnyy analiz v proyektirovanii i upravlenii : sb. nauch. tr. 16 Mezhdunarodnoy nauch.-prakt. konf. [System analysis in design and management : collection of research papers of XVI Int. Sci.-Pract. Conf.] Saint Petersburg, 2012, pp. 112–122 (in Russian).

24. Zaytsev, A. A., Kureychik, V. V., Polupanov, A. A. Obzor evolyutsionnykh metodov optimizatsii na osnove royevogo intellekta. [Overview of evolutionary optimization methods on the basis of Swarm Intelligence.] Izvestiya YuFU, 2010, no. 12 (113), pp. 7–12 (in Russian).

25. Romanets, Y. V., Timofeyev, P. A., Shangin, V. F. Zashchita informatsii v kompyuternykh sistemakh i setyakh. [Information security in computer systems and networks.] Moscow : Radio i svyaz, 2001, 376 p. (in Russian).

26. Alferov, A. P., et al. Osnovy kriptografii. [Cryptography basics.] Moscow : Gelios ARV, 2002, 480 p. (in Russian).

27. Chernyshev, Y. O., Sergeyev, A. S., Dubrov, E. O. Primeneniye algoritma muravinykh koloniy dlya realizatsii kriptoanaliza shifrov perestanovok. [Ant colony algorithm application for implementing cryptanalysis of transposition ciphers.] Nauchnaya sessiya, posvyashchennaya Dnyu radio : sb. dokladov 67 Vserossiyskoy konf. s Mezhdunarodnym uchastiyem. [Scientific session dedicated to Radio Day : Proc. 67 All-Russ.-Int. Conf.] Moscow, 2012, pp. 71–75 (in Russian).

28. Morozenko, V. V., Yeliseyev, G. O. Geneticheskiy algoritm dlya kriptoanaliza shifra Vizhenera. [Genetic algorithm for Vigenere cipher cryptanalysis.] Available at : http://vestnik.psu.ru/files/articles/ /132_6410.p (accessed : 24.05.2013) (in Russian).

29. Gorodilov, A. Y., Mitrakov, A. A. Kriptoanaliz trigonometricheskogo shifra s pomoshchyu geneticheskogo algoritma. [Trigonometric cipher cryptanalysis through genetic algorithm.] Available at : http://vestnik.psu.ru/files/articles/260_27019.p (accessed : 24.05.2013) (in Russian).

30. Gorodilov, A. Y. Kriptoanaliz perestanovochnogo shifra s pomoshchyu geneticheskogo algoritma. [Transposition cipher cryptanalysis through genetic algorithm.] Available at : http://vestnik.psu.ru/files/articles/8_83883 (accessed : 24.05.2013) (in Russian).

RESEARCH ON APPLICABILITY OF BIONIC TECHNIQUES OF ARTIFICIAL BEE COLONIES FOR IMPLEMENTATION OF CLASSICAL TRANSPOSITION CIPHER CRYPTANALYSIS*

Y. O. Chernyshev, A. S. Sergeyev, E. O. Dubrov, A. N. Ryazanov

The applicability of the bionic techniques of artificial bee colonies for the implementation of the classical transposition cipher cryptanalysis is considered. The problem is a classical optimization problem to the solution of which the known techniques of artificial bee colonies fallen within a relatively new class of bioinspired optimization methods are applied. It is shown that this is a subproblem of allocation, and it can be solved with an artificial bee colony algorithm, as the bee behavior principle is a self-organization delivering a collective swarm goal. At the first stage, a set of promising areas-sources is formed with the aid of scout-bees, at the second stage, the neighborhood of these areas is explored with the aid of foraging bees. At this, the main goal of the bee colony is to find a source with a maximum amount of nectar. Solution representation methods (positions in search space) are considered, a formula for determining an object function value (amount of nectar) is given. It is shown that the target search is the determination of an optimal symbol combination with the highest value of the objective function. Principle stages of the artificial bee colony algorithm, as well as an example of its application, are given.

Keywords: *cryptanalysis, problem of allocation, bioinspired methods, artificial bee colony algorithm, worker-bees (foragers), scout-bee, transposition cipher.*

* The research is done with the financial support from the Russian Foundation for Basic Research (project 12-01-00474).