УДК 004.056.55

ИССЛЕДОВАНИЕ ВОЗМОЖНОСТИ ПРИМЕНЕНИЯ АЛГОРИТМА МУРАВЬИНЫХ КОЛОНИЙ ДЛЯ РЕАЛИЗАЦИИ КРИПТОАНАЛИЗА ШИФРОВ ПЕРЕСТАНОВОК

В.А. ФАТХИ
(Донской государственный технический университет),
А.С. СЕРГЕЕВ
(Ростовское областное училище олимпийского резерва)

Исследована возможность применения алгоритмов муравьиных колоний для реализации криптоанализа шифров перестановок, результатом применения которых к открытому тексту является криптограмма, получаемая путем перестановки символов открытого текста в определенном порядке. Показано, как эта проблема может быть сведена к классической задаче о назначениях, решаемой с помощью алгоритма муравьиных колоний. Приведен алгоритм решения, дан пример работы муравьиного алгоритма.
Ключевые слова: *криптоанализ, задача о назначениях, муравьиный алгоритм, феромон, шифр перестановки.*

Введение. В последние годы интенсивно разрабатывается новое научное направление с названием «природные вычисления», которое объединяет математические методы, содержащие принципы природных механизмов принятия решений [1]. Как отмечено в [2], научное направление «природные вычисления» объединяет такие разделы, как эволюционное программирование, нейросетевые вычисления, алгоритмы роевого интеллекта, муравьиные алгоритмы, генетические алгоритмы. В [3-6] рассматривались методы организации криптографических атак на традиционные симметричные криптосистемы, использующие шифры перестановки и замены, а также на блочные криптосистемы с использованием методов эволюционной оптимизации и генетического поиска.

Однако, как отмечено в [7], структуры генетических алгоритмов являются «слепыми» поисковыми структурами с присущим им рядом недостатков. Поэтому представляет интерес применение конструктивных эвристических методов, идеи которых заимствованы у живой природы или физических процессов и в которых решение задачи строится поэтапно путем добавления нового компонента к частично построенному решению. К методам данного вида относят и муравьиные алгоритмы, основу которых составляет имитация самоорганизации муравьиной колонии. Как отмечено в [1], в противоположность примитивному поведению отдельных агентов поведение всей колонии оказывается достаточно разумным.

Отметим, что муравьиные алгоритмы исследуются с середины 90-х годов, и на сегодняшний день известны их применения к задаче о коммивояжере [8], квадратичной задаче о назначениях [9], задаче о раскраске графа [10, 11], задаче маршрутизации в коммутационных сетях [12], задаче маршрутизации транспортных средств [13]. В данной работе мы рассмотрим возможный подход для реализации криптоанализа шифров перестановки и покажем, как эта проблема может быть сведена к классической задаче о назначениях, решаемой с помощью алгоритма муравьиных колоний.

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.* Отметим, что основные виды шифров перестановок описаны, например, в [14, 15]. В общем случае результатом применения данного класса шифров к открытому тексту является строка символов (криптограмма), получаемая путем перестановки символов открытого текста в определенном 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 образом, 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.

В соответствии с [16] задачу о назначениях сформулируем в следующем виде. Определим X_{ij}=1, если объект i назначен в пункт j, и X_{ij}=0 в противном случае, C_{ij} – затраты на передачу объема ресурсов из пункта i в пункт j. В этом случае оптимизационная модель запишется следующим образом:

$$R=\sum_{i=1}^{n}\sum_{j=1}^{n} C_{ij}X_{ij} \rightarrow \text{экстр.}$$

при ограничениях

$$\sum_{j=1}^{n} X_{ij}=1,\ \ i=1,2,\ldots,n,$$

$$\sum_{i=1}^{n} X_{ij}=1,\ \ j=1,2,\ldots,n,$$

где n – число объектов и мест их размещения.

Применительно к задаче криптоанализа будем полагать, что C_{ij} – вероятность того, что за символом в позиции i должен следовать символ в позиции i+1, кроме этого введем параметр Q_i, показывающий, насколько фрагмент текста из i символов носит осмысленный характер, т.е. совпадает с словарным запасом языка. В этом случае оптимизационная модель будет иметь вид

$$R=\sum_{i=1}^{n}\sum_{j=1}^{n} Q_i C_{ij}X_{ij} \rightarrow \max.$$

Отметим, что элементы C_{ij} задаются в виде матрицы размерности nxn (n – число символов текста).

Таким образом, множество вариантов решений определяется числом перестановок $P=n!$ без повторений n символов, входящих в шифртекст в n позициях. Комбинаторный характер этой задачи приводит к необходимости использования метаэвристических алгоритмов.

Алгоритм решения. Таким образом, общее значение целевой функции R, получаемое в каждом конкретном варианте назначения символов в позиции, может быть аналогично [9] определено как длина маршрута, соединяющего выбранные элементы декартова произведения [номер позиции, номер символа], т.е. как

$$R = \sum_{\substack{i=1,\ldots,n-1 \\ j=2,\ldots,n}} C_{ij}.$$

Очевидно, маршруту с большим значением R должна соответствовать более высокая концентрация феромона F, которая используется в качестве вероятности выбора очередного маршрута, представляющего очередной вариант назначения символов в позиции, новыми муравьями-агентами.

Отметим, что в соответствии с [1] любой муравьиный алгоритм независимо от модификаций должен быть представим в следующем виде:

1) создание популяции муравьев;

2) поиск решения;

3) обновление феромона.

Отметим, что на этапе 1 выбор стартовых точек для размещения популяции муравьев зависит от ограничений, накладываемых условиями задачи, так как для каждой задачи способ раз-

мещения является определяющим. Либо муравьи размещаются в одной точке, либо в разных с повторениями, либо в разных без повторений. На этом же этапе задается начальный уровень феромона, который представляет собой небольшое положительное число, чтобы вероятности перехода в следующую вершину не были нулевыми. Определение вероятности перехода между соседними вершинами и нового уровня феромона после обновления может производиться по формулам, приведенным в [1].

Таким образом, в соответствии с [1] и [9] алгоритм включает следующие этапы.

1. Случайным равновероятным образом выбираются m вариантов маршрутов, и вычисляются значения целевых функций $R_1, R_2, \ldots R_m$.

2. Комбинациям ik_l размещения символов k в позиции i присваивается весовой коэффициент

$$f_{ik,l}=R_l,\ \ l=1,2,\ldots,m\ . \tag{1}$$

3. Для каждой комбинации ik вычисляется результирующая концентрация

$$F_{ik}=\sum_{l=1}^{m} f_{ik,l}\ . \tag{2}$$

Для тех комбинаций ik, которые ни разу не встретились в выборке m, задается нижнее значение концентрации феромона

$$F_{\min}=a\cdot\max f_{ik,l} \tag{3}$$

где $0<a<1$.

4. В соответствии с формулой, приведенной в [17] –

$$\tau_{ij}(t)=\tau_{ij}(t)\cdot(1-\rho), \tag{4}$$

производится имитация испарения феромона со всех комбинаций ik, по которым прошли муравьи.

5. После определения нового количества феромона производится возврат муравьев в начальные позиции и определение вероятностей размещения символа k в позиции i в новом маршруте

$$P_{ik}=F_{ik}/(\sum_{i=1}^{n} F_{ik}) \tag{5}$$

Совокупность указанных вероятностей образует матрицу вероятностей размещения nxn.

6. В соответствии с вычисленными вероятностями P_{ik} формируется $d\cdot m$ новых маршрутов ($d<1$), для которых определяются критерии $R_{m+1},\ldots,R_{m+m\cdot d}$, и далее производится выборка из m лучших вариантов. Если оптимальное значение критерия не изменяется в течение достаточно большого количества циклов, то поиск завершается с найденным значением $R_{\text{опт}}$, в противном случае длина пути обнуляется и производится возврат к шагу 2 алгоритма.

Отметим, что, так как шифртекст может содержать повторяющиеся символы, то будем полагать, что циклы в маршруте не запрещены и длина маршрута ограничена числом символов шифртекста.

Демонстрационный пример. Рассмотрим функционирование представленного выше алгоритма на демонстрационном примере. Пусть задана строка символов Б К С О А. Требуется определить возможную перестановку символов, входящую в словарный состав языка. Вначале на основе словаря русского языка составим матрицу C_{ij}, показывающую вероятность того, что за символом i может следовать символ j (рис.1).

	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

Определим количество муравьев m=5 и поставим их в соответствие каждому символу.

Итерация 1.

1. На 1-ом этапе выберем случайным образом m маршрутов, представляющих варианты размещения символов в позиции, и определим значения их критериев R_1, …, R_m. Пусть выбраны следующие маршруты:

1. К С Б А О R_1=0,01+0,05+0,6+0,1=0,76
2. Б К О С А R_2=0,01+0,5+0,5+0,3=1,31
3. С К А Б О R_3=0,08+0,4+0,6+0,5=1,58
4. О А К Б С R_4=0,1+0,6+0,01+0,1=0,81
5. А К Б О С R_5=0,6+0,01+0,5+0,5=1,61

Поскольку 1, 2, 4, 5 варианты далеки от словарного состава языка, то умножим их на весовой коэффициент Q=0,5, а 3 вариант, наиболее близкий к словарному составу, умножим на коэффициент Q=0,9. Получим следующие значения критериев: R_1=0,35; R_2=0,655; R_3=1,422; R_4=0,405; R_5=0,805.

2. На 2-м этапе всем комбинациям размещения символов в позиции присваивается весовой коэффициент в соответствии с формулами (1) и (2). Для тех комбинаций, которые не встретились в выборке из m маршрутов, зададим нижнее граничное значение концентрации $F_{\min}=a\cdot\max f_{ik,l}$. Значение a определим как a=0,1, тогда $F_{\min}$=0,14. Матрица результирующих концентраций феромона будет иметь вид, показанный на рис.2.

		Позиции				
		1	2	3	4	5
Символы	Б	0,655	0,14	1,155	1,825	0,14
	К	0,35	2,88	0,405	0,14	0,14
	С	1,42	0,35	0,14	0,655	1,21
	О	0,405	0,14	0,655	0,805	1,772
	А	0,805	0,405	1,42	0,35	0,655

Рис.2. Матрица результирующих концентраций феромона после 1-й итерации

3. Далее в соответствии с формулой (4) проведем испарение феромона, определив в соответствии с [17] ρ=0,6 (рис.3).

		Позиции				
		1	2	3	4	5
Символы	Б	0,262	0,14	0,462	0,73	0,14
	К	0,14	1,152	0,162	0,14	0,14
	С	0,568	0,14	0,14	0,262	0,484
	О	0,162	0,14	0,262	0,322	0,7
	А	0,322	0,162	0,568	0,14	0,262

Рис.3. Матрица концентраций феромона после его испарения после 1-й итерации

4. Вычислим вероятности размещения символов в соответствующие позиции по формуле (5) (рис.4).

		Позиции				
		1	2	3	4	5
Символы	Б	0,18	0,08	0,29	0,46	0,08
	К	0,09	0,66	0,1	0,09	0,08
	С	0,39	0,08	0,09	0,16	0,28
	О	0,11	0,08	0,16	0,2	0,4
	А	0,22	0,1	0,36	0,09	0,15

Рис.4. Матрица вероятностей размещения символов в позиции после 1-й итерации

5. В соответствии с вычисленными вероятностями сформируем новые маршруты, выбрав d=0,8. Разместим муравьев в следующие позиции символов в соответствии с вероятностями размещения: С, А, Б, О. Случайным образом сформируем 4 маршрута:

1. А О К Б С R_6=0,1+0,3+0,01+0,1=0,51
2. С К Б О А R_7=0,08+0,01+0,5+0,1=0,69
3. Б К А О С R_8=0,01+0,4+0,1+0,5=1,01
4. О К А Б С R_9=0,3+0,4+0,6+0,1=1,4

Для вариантов 6, 7, 8, 9 определим значения Q соответственно: 0,5; 0,9; 0,6; 0,5. Получим:

R_6=0,255; R_7=0,621; R_8=0,606; R_9=0,7.

Из полученной популяции выберем 5 вариантов с лучшими значениями целевой функции. Это будут варианты: R_2, R_3, R_5, R_7, R_9. Обозначим: R_1=R_2=0,655; R_2=R_3=1,422; R_3=R_5=0,805; R_4=R_7=0,621; R_5=R_9=0,7.

Итерация 2.

1. Матрица результирующих концентраций феромона будет иметь вид, показанный на рис.5.
2. После испарения феромона получим матрицу концентраций, показанную на рис.6.
3. Матрица вероятностей размещения символов в позиции показана на рис.7.

Символы	Позиции 1	2	3	4	5
Б	0,655	0,14	1,426	2,122	0,14
К	0,14	4,203	0,14	0,14	0,14
С	2,043	0,14	0,14	0,655	1,505
О	0,7	0,14	0,655	1,426	1,422
А	0,805	0,14	2,122	0,14	1,276

Рис.5. Матрица результирующих концентраций феромона после 2-й итерации

Символы	Позиции 1	2	3	4	5
Б	0,262	0,14	0,57	0,848	0,14
К	0,14	1,68	0,14	0,14	0,14
С	0,82	0,14	0,14	0,262	0,602
О	0,28	0,14	0,262	0,57	0,56
А	0,322	0,14	0,848	0,14	0,51

Рис.6. Матрица концентраций феромона после его испарения после 2-й итерации

Символы	Позиции 1	2	3	4	5
Б	0,15	0,06	0,29	0,45	0,07
К	0,07	0,76	0,07	0,06	0,07
С	0,4	0,06	0,07	0,13	0,3
О	0,15	0,06	0,13	0,3	0,29
А	0,18	0,06	0,44	0,06	0,26

Рис.7. Матрица вероятностей размещения символов в позиции после 2-й итерации

4. Случайным образом сформируем 4 маршрута, разместив муравьев в следующие позиции: С,С,А,Б.

1. С К Б О А R_6=0,08+0,01+0,5+0,1=0,69
2. С К О Б А R_7=0,08+0,5+0,6+0,6=1,78
3. Б К А О А R_8=0,01+0,4+0,1+0,1=0,61
4. А К Б Б А R_9=0,6+0,01+0,01+0,6=1,22

Для вариантов 6, 7, 8, 9 определим значения Q соответственно: 0,9; 1; 0,5; 0,5. Получим: R_6=0,621; R_7=1,78; R_8=0,305; R_9=0,61.

Далее вновь из полученной популяции выберем 5 лучших маршрутов с лучшими значениями целевой функции. Это будут варианты: R_7, R_2, R_3, R_5, R_6. Обозначим: R_1= R_7=1,78; R_2=R_2=1,422; R_3=R_3=0,805; R_4=R_5=0,7; R_5=R_6=0,621.

Итерация 3.

1. Матрица результирующих концентраций феромона будет иметь вид, показанный на рис.8.

		Позиции				
		1	2	3	4	5
Символы	Б	0,14	0,14	1,426	3,902	0,14
	К	0,14	5,328	0,14	0,14	0,14
	С	3,823	0,14	0,14	0,14	1,505
	О	0,7	0,14	1,78	1,426	1,422
	А	0,805	0,14	2,122	0,14	2,401

Рис.8. Матрица результирующих концентраций феромона после 3-й итерации

2. После испарения феромона получим матрицу концентраций, показанную на рис.9.

		Позиции				
		1	2	3	4	5
Символы	Б	0,14	0,14	0,57	1,56	0,14
	К	0,14	2,13	0,14	0,14	0,14
	С	1,52	0,14	0,14	0,14	0,602
	О	0,28	0,14	0,712	0,57	0,56
	А	0,322	0,14	0,84	0,14	0,96

Рис. 9. Матрица концентраций феромона после его испарения после 3-й итерации

3. Матрица вероятностей размещения символов в позиции показана на рис.10.

		Позиции				
		1	2	3	4	5
Символы	Б	0,05	0,05	0,23	0,63	0,06
	К	0,05	0,80	0,06	0,05	0,06
	С	0,66	0,05	0,06	0,05	0,25
	О	0,11	0,05	0,30	0,22	0,23
	А	0,13	0,05	0,35	0,05	0,40

Рис. 10. Матрица вероятностей размещения символов в позиции после 3-й итерации

4. Продолжая процесс далее, определим 4 случайных маршрута, размещая муравьев в позиции С, С, С, А.

1. С К А Б О R_6=0,08+0,4+0,6+0,5=1,58
2. С К О Б А R_7=0,08+0,5+0,6+0,6=1,78
3. С К А Б А R_8=0,08+0,4+0,6+0,6=1,68
4. А К О Б А R_9=0,6+0,5+0,6+0,6=2,3

Для вариантов 6, 7, 8, 9 определим значения Q соответственно: 0,9; 1; 0,9;0,9. Получим: R_6=1,422; R_7=1,78; R_8=1,512; R_9=2,07.

Выберем 5 маршрутов с лучшими значениями целевой функции. Это будут варианты: R_9, R_7, R_1, R_8, R_6. Обозначим: R_1=R_9=2,07; R_2=R_7=1,78; R_3=R_1=1,78; R_4=R_8=1,512; R_5=R_6=1,422.

Итерация 4.

1. Матрица результирующих концентраций феромона показана на рис.11.

		Позиции				
		1	2	3	4	5
Символы	Б	0,14	0,14	0,14	8,564	0,14
	К	0,14	8,564	0,14	0,14	0,14
	С	6,494	0,14	0,14	0,14	0,14
	О	0,14	0,14	5,63	0,14	1,422
	А	2,07	0,14	2,934	0,14	7,142

Рис.11. Матрица результирующих концентраций феромона после 4-й итерации

2. Матрица вероятностей размещения символов в позиции после испарения показана на рис.12.

	Позиции				
	1	2	3	4	5
Б	0,03	0,03	0,03	0,88	0,03
К	0,03	0,88	0,03	0,03	0,03
С	0,69	0,03	0,03	0,03	0,03
О	0,03	0,03	0,60	0,03	0,15
А	0,22	0,03	0,31	0,03	0,76

Рис.12. Матрица вероятностей размещения символов в позиции после 4-й итерации

3. Разместим 4-х муравьев в позициях С, С, С, А и определим 4 случайных маршрута:

1. С К О Б А R_6=0,08+0,5+0,6+0,6=1,78
2. С К О Б А R_7=0,08+0,5+0,6+0,6=1,78
3. С К О Б О R_8=0,08+0,5+0,6+0,5=1,68
4. А К О Б О R_9=0,6+0,5+0,6+0,5=2,2

Для вариантов 6, 7, 8, 9 определим значение Q как 1; 1; 0,9; 0,8. Получим:

R_6=1,78; R_7=1,78; R_8=1,512; R_9=1,76.

Выберем 5 маршрутов с лучшими значениями целевой функции. Это будут варианты: R_1, R_2, R_3, R_6, R_7.

Выводы. Была рассмотрена возможность применения алгоритма муравьиной колонии для решения задачи криптоанализа шифров перестановок. Комбинирование алгоритма муравьиных колоний с элементами генетических алгоритмов, а также распараллеливание алгоритма муравьиных колоний может существенно повысить эффективность использования данных методов и вероятность нахождения оптимального решения.

Библиографический список

1. Муравьиные алгоритмы [Электрон. ресурс]. Режим доступа: http://rain.ifmo.ru/cat/data/theory/unsorted/ant-algo-2006/article.pdf

2. Макконел Д. Основы современных алгоритмов / Д. Макконел. – М.: Техносфера, 2004.

3. 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: материалы 6-й всерос. науч.-техн. конф. – Улан-Удэ: Изд-во ВСГТУ, 2005. – С.61-65.

4. Сергеев А.С. Применение методов генетического поиска для организации криптоанализа блочных криптосистем на примере стандарта шифрования DES / Сергеев А.С. // Научная мысль Кавказа. Прил. – Ростов н/Д: Изд-во СКНЦ ВШ. – 2006. – №15. – С.185-193.

5. Сергеев А.С. О возможности применения методов генетического поиска для реализации криптоанализа асимметричного алгоритма шифрования данных RSA / А.С. Сергеев // Изв. вузов. Сев.-Кавк. регион. Сер. Технические науки. – 2008. – №3. – С.48-52.

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

7. Лебедев О.Б. Трассировка в канале методом муравьиной колонии / О.Б. Лебедев // Изв. ЮФУ. Сер. Технические науки. Тем. вып. «Интеллектуальные САПР». – Таганрог: Изд-во ТТИ ЮФУ. – 2009. – №4(93). – С.46-52.

8. Курейчик В.М. О некоторых модификациях муравьиного алгоритма / В.М. Курейчик, А.А. Кажаров // Изв. ЮФУ. Сер. Технические науки. Тем. вып. «Интеллектуальные САПР». – Таганрог: Изд-во ТТИ ЮФУ. – 2008. – №4(81). – С.7-12.

9. Васильев Е.М., Свистунов А.А. Решение комбинаторных задач моделированием поведения муравьиных колоний [Электрон. ресурс]. Режим доступа: http://www.v-itc.ru/electrotech/2008/01/pdf/2008-01-15.pdf

10. Dorigo M. Ant Algorithms for Discrete Optimization //Artificial Life. – 1999. – Vol.5. – No.3. – P.137-172.

11. Costa D., Herts A. Ants can colour graphs. // Journal of the Operation Research Society (JORS), 48:295-305, 1997.

12. Di Caro G. Extending AntNet for best-effort Quality-of-Service routing// Unpublished presentation at ANTS'98 – From Ant Colonies to Artifical Ants: First International Workshop on Ant Colony Optimization, October 15-16, 1998.

13. Игнатьев. А.Л. Использование алгоритма муравьиных колоний для решения задачи маршрутизации транспортных средств [Электрон. ресурс]. Режим доступа: http://2009.it-edu.ru/docs/Sekziya_8/3_Ignat'ev_Ignatyev.doc

14. Романец Ю.В. Зашита информации в компьютерных системах и сетях / Ю.В. Романец, П.А. Тимофеев, В.Ф. Шаньгин. – М.: Радио и связь, 2001.

15. Основы криптографии / А.П. Алферов, А.Ю. Зубов, А.С. Кузьмин, А.В. Черемушкин. – М.: Гелиос АРВ, 2002.

16. Вагнер Г. Основы исследования операций / Г. Вагнер. – М.: Мир, 1972.

17. Алгоритмы муравьиной колонии [Электрон. ресурс]. Режим доступа: http://www.wikiznanie.ru/ruwz/index.php.

Материал поступил в редакцию 05.11.10

References

1. Murav'inye algoritmy [Elektron. resurs]. Pejim dostupa: http://rain.ifmo.ru/cat/data/theory/unsorted/ant-algo-2006/article.pdf. – In Russian.

2. Makkonel D. Osnovy sovremennyh algoritmov / D. Makkonel. – M.: Tehnosfera, 2004. – In Russian.

3. Sergeev A.S. Issledovanie vozmojnosti organizacii kriptograficheskoi ataki s ispol'zovaniem evolyucionnoi optimizacii i kvantovogo poiska pri razrabotke sistem peredachi i zaschity informacii / A.S. Sergeev // Teoreticheskie i prikladnye voprosy sovremennyh informacionnyh tehnologii: materialy 6-i vseros. nauch.-tehn. konf. – Ulan-Ude: Izd-vo VSGTU, 2005. – S.61-65. – In Russian.

4. Sergeev A.S. Primenenie metodov geneticheskogo poiska dlya organizacii kriptoanaliza blochnyh kriptosistem na primere standarta shifrovaniya DES / Sergeev A.S. // Nauchnaya mysl' Kavkaza. Pril. – Rostov n/D: Izd-vo SKNC VSh. – 2006. – №15. – S.185-193. – In Russian.

5. Sergeev A.S. O vozmojnosti primeneniya metodov geneticheskogo poiska dlya realizacii kriptoanaliza asimmetrichnogo algoritma shifrovaniya dannyh RSA / A.S. Sergeev // Izv. vuzov. Sev.-Kavk. region. Ser. Tehnicheskie nauki. – 2008. – №3. – S.48-52. – In Russian.

6. Chernyshev Yu.O. Issledovanie i razrabotka metodov geneticheskogo poiska dlya realizacii kriptoanaliza algoritma IDEA i resheniya osnovnyh teoretiko-chislovyh zadach kriptografii / Yu.O. Chernyshev, A.S. Sergeev, N.N. Vencov // Vestn. RGUPS. – 2009. – №3(35). – S.70-79. – In Russian.

7. Lebedev O.B. Trassirovka v kanale metodom murav'inoi kolonii / O.B. Lebedev // Izv. YuFU. Ser. Tehnicheskie nauki. Tem. vyp. «Intellektual'nye SAPR». – Taganrog: Izd-vo TTI YuFU. – 2009. – №4(93). – S.46-52. – In Russian.

8. Kureichik V.M. O nekotoryh modifikaciyah murav'inogo algoritma / V.M. Kureichik, A.A. Kajarov // Izv. YuFU. Ser. Tehnicheskie nauki. Tem. vyp. «Intellektual'nye SAPR». – Taganrog: Izd-vo TTI YuFU. – 2008. – №4(81). – S.7-12. – In Russian.

9. Vasil'ev E.M., Svistunov A.A. Reshenie kombinatornyh zadach modelirovaniem povedeniya murav'inyh kolonii [Elektron. resurs]. Rejim dostupa: http://www.v-itc.ru/electrotech/2008/01/pdf/2008-01-15.pdf. – In Russian.

10. Dorigo M. Ant Algorithms for Discrete Optimization //Artificial Life. – 1999. – Vol.5. – No.3. – R.137-172.

11. Costa D., Herts A. Ants can colour graphs. // Journal of the Operation Research Society (JORS), 48:295-305, 1997.

12. Di Caro G. Extending AntNet for best-effort Quality-of-Service routing// Unpublished presentation at ANTS'98 – From Ant Colonies to Artifical Ants: First International Workshop on Ant Colony Optimization, October 15-16, 1998.

13. Ignat'ev. A.L. Ispol'zovanie algoritma murav'inyh kolonii dlya resheniya zadachi marshrutizacii transportnyh sredstv [Elektron. resurs]. Rejim dostupa:

http://2009.it-edu.ru/docs/Sekziya_8/3_Ignat'ev_Ignatyev.doc. – In Russian.

14. Romanec Yu.V. Zashita informacii v komp'yuternyh sistemah i setyah / Yu.V. Romanec, P.A. Timofeev, V.F. Shan'gin. – M.: Radio i svyaz', 2001. – In Russian.

15. Osnovy kriptografii / A.P. Alferov, A.Yu. Zubov, A.S. Kuz'min, A.V. Cheremushkin. – M.: Gelios ARV, 2002. – In Russian.

16. Vagner G. Osnovy issledovaniya operacii / G. Vagner. – M.: Mir, 1972. – In Russian.

17. Algoritmy murav'inoi kolonii [Elektron. resurs]. Rejim dostupa:
http://www.wikiznanie.ru/ruwz/index.php. – In Russian.

V.A. FATKHI, A.S. SERGEYEV

APPLICATION OF ANT COLONY ALGORITHM FOR REALIZATION OF TRANSPOSITION CIPHERS CRYPT ANALYSIS

Possibility of application of ant colony algorithms for realization of the transposition ciphers cryptanalysis is studied. Its application to the plain text results in the cryptogram received by shifting symbols of the plain text in a certain order. It is shown how this problem can be restricted to a classical problem of allocation solved by ant colony algorithm. The solution algorithm is given. An example of ant algorithm performance is described.
Key words: *cryptanalysis, problem of allocation, ant algorithm, pheromone, transposition cipher.*