УДК 004.056.55

ОБЗОР АЛГОРИТМОВ РЕШЕНИЯ ЗАДАЧ КРИПТОАНАЛИЗА НА ОСНОВЕ БИОИНСПИРИРОВАННЫХ ТЕХНОЛОГИЙ ИСКУССТВЕННОГО ИНТЕЛЛЕКТА

Ю. О. Чернышев, А. С. Сергеев, Е. О. Дубров

ГОУ ВПО «Донской государственный технический университет»

Поступила в редакцию 22.04.2014 г.

Аннотация. Рассматривается задача криптоанализа на основе новых моделей искусственного интеллекта – биоинспирированных методов. Приводится обзор авторских работ, посвященных решению задачи криптоанализа классических криптографических методов. Также исследуются «алгоритм муравья» и алгоритм «колонии пчел» для реализации криптоанализа перестановочных шифров, а также для реализации криптоанализа асимметричных алгоритмов шифрования на основе решения теоретико-числовых задач криптографии наряду с экспериментальными результатами.
Ключевые слова: криптоанализ, биоинспирированные методы, генетический алгоритм, муравьиные алгоритмы, пчелиные алгоритмы, шифры перестановок, шифры замены.
Annotation. The problem of cryptanalysis on the basis of new models of artificial intelligence – the bioinspired methods is considered. The review of the handiworks devoted to the solution of a problem of cryptanalysis of classical cryptographic methods is provided. Also «the algorithm of an ant» and algorithm of «a colony of bees» for realization of cryptanalysis of permutable codes, and also for realization of cryptanalysis of asymmetric algorithms of enciphering on the basis of the solution of number-theoretic problems of cryptography along with experimental results are investigated.
Keywords: the cryptanalysis, the bioinspired methods, genetic algorithm, ant algorithms, bee algorithms, codes of shifts, replacement codes.

1. ВВЕДЕНИЕ

В настоящее время при разработке компьютерных технологий, обеспечивающих информационную безопасность и защиту информации, широкое применение находят криптографические методы защиты. Для решения этой задачи, относящейся к классу NP-полных, в последние годы применяются алгоритмы, основанные на природных системах. К ним относятся методы моделирования отжига, генетические алгоритмы (ГА), эволюционные методы, алгоритмы роевого интеллекта и т. д.[1]

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 т. ч. генетический алгоритм, генетическое программирование, эволюционные стратегии, эволюционное программирование.

Реализация криптоанализа симметричных алгоритмов шифрования. Ранее в [1–3] рассматривалась задача криптоанализа и приведены результаты криптоанализа классических криптографических алгоритмов с использованием методов эволюционной оптимизации и генетического поиска для симметричных шифров перестановок. Различают следующие шифры перестановок: простые шифрующие таблицы; шифрующие таблицы с одиночной перестановкой по ключу; шифрующие таблицы с двойной перестановкой по ключу; магические квадраты. Методы шифрования с помощью простых шифрующих таблиц, с помощью одиночной перестановки

по ключу, двойной перестановки описаны, например, в [1, 4].

При использовании шифрующих таблиц ключом является перестановка $(p_1, p_2, \ldots, p_n)$, поэтому хромосома в ГА должна также задавать перестановку. Основной вопрос при этом – как осуществить представление отдельных генов особи. В простейшем случае шифрование осуществляется путем присвоения отдельным генам соответствующих элементов ключа, т. е. i-м геном хромосомы P считать элемент p_i. Несмотря на недостатки такого подхода, отмеченные в [5], (например, гены получаются зависимыми друг от друга, что приводит к возможности получения нелегальных решений), такое определение генов интуитивно понятно и не требует дополнительных затрат на их формирование (вычисление).

Альтернативным подходом является использование некоторого промежуточного представления, при котором набор генов задает некоторое правило или объект, из которого формируется ключ [1, 5]. При этом основной задачей является нахождение промежуточного решения, задаваемого в виде битовой строки для применения стандартных генетических операторов. При реализации ГА криптоанализа использовался первый подход, т. е. в качестве генов особи рассматриваются элементы ключа. Для предотвращения получения нелегальных решений при десятичном кодировании хромосом используется правило: при появлении в хромосоме одинаковых генов второй повторяющийся ген заменяется на отсутствующий. В качестве функции приспособленности особей использовался факт совпадения открытого текста и шифртекста при реализации криптоанализа 2 типа для определения секретного ключа. В [5, 7] в качестве целевой функции предлагается использовать функцию Якобсена о распределении частот биграмм в открытых текстах. В [1–3] приведены результаты эксперимента при реализации криптоанализа 2 типа при бинарном и десятичном кодировании хромосом методов одиночной и двойной перестановки по ключу, а также простой перестановки, в котором ключом служит размер таблицы. Полученные результаты свидетельствуют о возможности применения эволюционных методов для криптоанализа шифров, использующих шифрующие таблицы для столбцовых и строчных перестановок.

Наряду с использованием шифрующих таблиц, широкое распространение для шифрования получили шифры маршрутной перестановки. В [1, 6] рассматриваются методы шифрования перестановками, использующие магические квадраты. Приводится ГА их построения и результаты эксперимента, которые свидетельствуют о возможности применения ГА для решения задач криптоанализа данных шифров перестановки при разработке систем обеспечения информационной безопасности и защиты информации. Отмечается, что существенным отличительным моментом является наличие случайного поиска, позволяющего получать новые результаты при каждой реализации ГА.

В [1, 6, 8] рассматривается применение данных подходов для реализации шифров простой и многоалфавитной замены. Сущность методов простой замены сводится к замене символов шифруемого текста символами того же или другого алфавита с заранее установленным правилом замены. Рассматривается реализация криптоанализа шифров одноалфавитной замены на примере аффинного шифра Цезаря и системы Цезаря с ключевым словом при известной и неизвестной длине ключа, шифров блочной замены на примере шифра Плейфейра и шифра «двойной квадрат» Уитстона при известной и неизвестной длине кодового слова, а также шифра многоалфавитной замены на примере шифра Вижинера. Здесь же приводятся результаты эксперимента, свидетельствующие об области применимости данных методов криптоанализа.

Однако, структуры генетических алгоритмов являются «слепыми» поисковыми структурами с присущим им рядом недостатков [9]. Поэтому представляет интерес применение 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. В [9] приводится описание алгоритма «муравьиных колоний» для реализации криптоанализа шифров перестановки, и показано, как эта проблема может быть сведена к классической задаче о назначениях, решаемой с помощью алгоритма муравьиных колоний. Отличительной особенностью применения алгоритмов «муравьиных колоний» является необходимость представления задачи в виде графовой модели, на которой муравьи могут строить решения.

Одной из последних разработок в области роевого интеллекта является алгоритм пчел, который довольно успешно используется для нахождения экстремумов сложных многомерных функций. Алгоритм криптоанализа шифров перестановок на основе пчелиного алгоритма, рассматривается в [10, 16]. Структура его включает следующие основные этапы:

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

В [16] предлагается реализация основных этапов пчелиного алгоритма, а также приводится демонстрационный пример реализации алгоритма криптоанализа.

Криптоанализ асимметричных алгоритмов шифрования. Наряду с классическими симметричными алгоритмами шифрования сравнительно молодой областью является асимметричная криптография, которая включает криптосистемы с открытым ключом (для шифрования данных используется один ключ (открытый), а для расшифрования другой (секретный)). Представителем ее является алгоритм RSA, криптостойкость которого определяется трудоемкостью факторизации больших чисел. Для проведения криптоанализа и определения секретного ключа необходимо разложение модуля N на простые множители P и Q (определение функции Эйлера $f(N)=(P-1)*(Q-1)$), а также определение секретного ключа $K_{сек}$ из уравнения $K_{откр}*K_{сек}=1 \bmod f(N)$, где $K_{откр}$ – известный открытый ключ (число, взаимно простое с числом $f(N)$), $K_{сек}$ – секретный ключ, подлежащий определению. Отметим, что ГА для решения задачи определения вариантов разложения заданного числа N на множители (нахождения делителей большого целого числа N) описан в [11], где рассматривается процедура инициализации создания элемента популяции, а также применение основных генетических операций. ГА разложения заданного числа на множители рассмотрен в [12], экспериментальные результаты, представлены в таблицах 1, 2.

Алгоритм разложения числа на два взаимно простых сомножителя сформулируем в следующем виде.

1. Задается число в десятичной форме.
2. Задается популяция хромосом 10000x2, где первая часть соответствует первому сомножителю, вторая часть – второму (в двоичной форме).
3. Выполняются генетические операции (кроссинговер, мутация, инверсия, элитная селекция). Применялся 4-х точечный кроссинговер между хромосомами, принадлежащими одной части (норма мутации 5 %, норма инверсии 10 %, количество потомков варьировалось в пределах 40–60 %).
4. Подсчитывается целевая функция путем умножения соответствующих хромосом в двоичной форме с идентичными номерами из каждой части.
5. Конец.

При криптоанализе асимметричных алгоритмов шифрования актуальной также является задача нахождения простого делителя заданного числа. Для проверки, является ли число простым, использовался тест Миллера-Рабина. Алгоритм нахождения простого делителя числа сформулируем следующим образом.

1. Задается число в десятичной форме (32, 48 или 64 бита), переводится в двоичную форму.

2. Случайным образом генерируется начальная популяция двоичных хромосом.

3. Вычисляется целевая функция путем деления заданного числа на хромосому (деление производится в десятичной форме). В качестве целевой функции принимается остаток от деления.

4. В случае если после деления получено целое число, переход к 6, иначе к 5.

5. Выполняются генетические операторы: 4-х точечный кроссинговер случайно сформированных пар родителей, инверсия (норма 10 %), мутация (норма 5 %). Для перехода к следующей генерации выполняется селекция.

6. По алгоритму Миллера-Рабина проверяется, является ли число с высокой степенью вероятностью простым; если нет, то осуществляется переход к пункту 5.

7. Конец.

Таким образом, представленные результаты свидетельствуют о возможности применения генетических алгоритмов для решения основных теоретико-числовых задач криптографии: факторизации числа и нахождения простого делителя числа.

Таблица 1

Экспериментальные результаты применения генетического алгоритма для факторизации числа

Длина ключа	Размер начальной популяции (в парах)	Количество итераций
32	2 000	134 664
	3 000	122 537
	8 000	99 571
48	8 000	3 400 274
	10 000	3 259 667
	20 000	2 564 448
64	20 000	84 092 423
	24 000	79 549 001
	48 000	81 663 284

Для ликвидации отмеченных выше недостатков ГА актуальной является разработка биоинспирированных алгоритмов криптоанализа данных методов шифрования. В то же время основной проблемой при реализации ГА, описанного в [11], является нахождение экстремума немонотонной функции, то есть функции, значение $f(x)$ которой в каждой точке x является, по сути, случайной величиной и не дает информации о приближении к глобальному экстремуму. В этом плане отметим работы [3, 13], в которых приводится описание применения биоинспирированных методов для решения задачи криптоанализа асимметричных алгоритмов шифрования на основе факторизации составных чисел. Здесь представлены алгоритмы муравьиных и пчелиных колоний для разложения составных чисел на множители путем определения делителя числа с заданной точностью в заданном интервале. Приводится алгоритм решения, а также пример работы муравьиного и пчелиного алгоритма.

Таблица 2

Экспериментальные результаты применения генетического алгоритма для нахождения простого делителя числа

Длина ключа	Размер начальной популяции (в парах)	Количество итераций
32	2 000	84 315
	3 000	80 448
	8 000	77 304
48	8 000	247 558
	10 000	210 589
	20 000	209 557
64	20 000	1 014 899
	24 000	1 144 346
	48 000	987 467

Экспериментальные результаты факторизации чисел с использованием алгоритма муравьиных колоний приведены в таблице 3, где показаны начальные параметры, собственно само число, количество итераций, необходимых для получения сомножителей, и эти сомножители. Здесь $[x, y]$ – координаты отрезка; M – количество муравьев; m – число вершин в маршруте; Q – параметр порядка длины оптимального пути.

Таблица 3

Экспериментальные результаты применения муравьиного алгоритма для факторизации числа

Число для разложения (N)	Полученные сомножители	Начальные параметры	Количество итераций
15238657	7 * 7 * 353 * 881	[5,2000], $M = 4, m = 4, Q = 4$	568
		[5,1000], $M = 5, m = 5, Q = 4$	550
		[5,1000], $M = 6, m = 6, Q = 4$	543
16123897	23 * 37 * 18947	[5,30000], $M = 4, m = 4, Q = 4$	611
		[5,20000], $M = 5, m = 5, Q = 4$	638
		[5,20000], $M = 6, m = 6, Q = 4$	599

Таблица 4

Экспериментальные результаты применения пчелиного алгоритма для факторизации числа

Число для разложения (N)	Интервалы для проведения поиска	Полученные сомножители
4154963851	[1, 250000], [250001, 500000], [500001, 750000], [750001, 1000000], [1000001,1250000], [1250001, 1500000], [1500001, 1750000], [1750001,2000000].	3943, 1053757

Оба числа являются 24 битными. Простота числа проверялась с помощью алгоритма Миллера-Рабина.

При реализации пчелиного алгоритма проводилось разложение 32-битного числа. Результаты эксперимента представлены в таблице 4. Простота чисел также была проверена с помощью теста Миллера-Рабина.

В [1] описаны отличительные особенности методов шифрования, для которых доказана абсолютная криптографическая стойкость (например, метод Вернама и шифр гаммирования). Отмечается возможность атак на данные шифры, основанных в большинстве своем либо на факте значительного отклонения статистических характеристик гаммы от действительно случайного потока или на повторном использовании некоторых частей гаммы в процессе шифрования.

В заключение отметим некоторые новые оригинальные методы, используемые для криптоанализа. Работы [5, 7, 14], посвящены применению ГА для криптоанализа шифров перестановок, шифров многоалфавитной замены, а также оригинального метода, отличающегося, по мнению авторов, «бесконечным» периодом гаммирования [15]. В данных публикациях наряду с описанием алгоритмов криптоанализа (способов кодирования решения, описания используемых генетических операций и демонстрационных примеров) приведены экспериментальные результаты криптоанализа, подтверждающие достоверность представленных подходов решения задачи криптоанализа.

В ряде работ (в том числе в [5, 7, 14]) приводится описание нового подхода к решению задачи определения целевой функции приспособленности особей при решении задачи криптоанализа. В качестве фитнесс-функции предлагается использовать функцию Якобсена $F(k)$ о распределении частот биграмм в открытых текстах. Эта функция в общем случае вычисляется как:

$$F(k) = \sum_{ij} \left| D_{ij}^k - E_{ij} \right|,$$

где D_{ij}^k – частота встречаемости биграммы $a_i a_j$ в тексте, полученном при расшифровании с помощью ключа k, E_{ij} – среднестатистическая частота встречаемости этой би-

граммы. Среднестатистические частоты встречаемости биграмм являются заранее известными, и, как показывают приведенные в [5, 7, 14] примеры, применение целевой функции данного типа при криптоанализе дает результаты, достаточно близкие к оптимальным.

ЗАКЛЮЧЕНИЕ

Таким образом, в данной статье, в основном, представлен обзор авторских работ, посвященных решению задачи криптоанализа классических и асимметричных алгоритмов шифрования на основе новых технологий искусственного интеллекта – биоинспирированных методов, имитирующих процессы эволюции живой природы. Описаны основные отличительные особенности применения данных методов, приведены экспериментальные результаты, свидетельствующие о возможности применения данных методов для решения задач криптоанализа.

СПИСОК ЛИТЕРАТУРЫ

1. *Чернышев Ю.О, Сергеев А.С., Дубров Е.О., Крупенин А.В., Третьяков О.П.* Криптографические методы и генетические алгоритмы решения задач криптоанализа: монография. – Краснодар : ФВАС, 2013. – 138 с.

2. *Чернышев Ю.О., Сергеев А.С., Дубров Е.О.* Применение биоинспирированных методов оптимизации для реализации криптоанализа классических и блочных криптосистем // Теоретические и прикладные вопросы современных информационных технологий: Материалы 11 Всероссийской научно-технической конференции. – Улан-Удэ : Изд-во ВСГТУ, 2012. – С. 121–131.

3. *Чернышев Ю.О., Сергеев А.С., Дубров Е.О.* Применение биоинспирированных методов оптимизации для реализации криптоанализа классических симметричных и асимметричных криптосистем // Системный анализ в проектировании и управлении: Сборник научных трудов 16 Международной научно-практической конференции. С-Пб. : Изд-во Политехн. Ун-та, 2012. – С. 112–122.

4. *Романец Ю.В., Тимофеев П.А., Шаньгин В.Ф.* Защита информации в компьютерных системах и сетях. – М. : Радио и связь, 1999. – 328 с.

5. *Городилов А.Ю.* Криптоанализ перестановочного шифра с помощью генетического алгоритма//Вестник пермского университета. Серия: математика, механика, информатика, 2007, № 7. – С. 44–49.

6. *Дубров Е.О., Рязанов А.Н., Сергеев А.С., Чернышев Ю.О.* Разработка методов криптоанализа шифров перестановок и замены в системах защиты информации на основе эволюционно-оптимизационных методов // Радиоэлектронные устройства и системы для инфокоммуникационных технологий: научная конференция, посвященная дню радио. – Москва, 2013. – С. 220–224.

7. *Морозенко В.В., Елисеев Г.О.* Генетический алгоритм для криптоанализа шифра Вижинера//Вестник пермского университета. Серия: математика, механика, информатика, 20010, № 1. – С. 75–80.

8. *Чернышев Ю.О., Сергеев А.С., Дубров Е.О., Рязанов А.Н.* Применение эволюционных методов оптимизации для реализации криптоанализа классических шифров замены // Информатика: проблемы, методология, технологии: материалы XIII междунар. науч.-метод. конф. / ВГУ. – Воронеж, 2013, С. 415–418.

9. *Фатхи В.А., Сергеев А.С.* Исследование возможности применения алгоритма муравьиных колоний для реализации криптоанализа шифров перестановок. – Вестник ДГТУ, том 11, № 1(52), 2011. – С. 10–20.

10. *Чернышев Ю.О, Сергеев А.С., Дубров Е.О.* Исследование и разработка методов криптоанализа шифров перестановок на основе биоинспирированных методов пчелиных колоний // Системный анализ в проектировании и управлении. Часть 1: Сборник научных трудов 17 Международной научно-практической конференции. – С-Пб. : Изд-во Политехн. Ун-та, 2013. – С. 143–150.

11. *Сергеев А.С.* О возможности применения методов генетического поиска для реализации криптоанализа асимметричного алгоритма шифрования данных RSA. – Известия

ВУЗов. Сев.-Кавк. Регион. Техн. Науки, 2008. – № 3. – С. 48–52.

12. *Чернышев Ю.О, Сергеев А.С., Дубров Е.О.* Применение биоинспирированных алгоритмов оптимизации для реализации криптоанализа классических и асимметричных криптосистем // Информатика: проблемы, методология, технологии: материалы XIV Международной научно-методической конференции / ВГУ. – Воронеж : Издательский дом ВГУ, 2014. –. 206–210.

13. *Сергеев А.С., Третьяков О.П., Васильев А.Е., Чернышев Ю.О.* Биоинспирированные методы криптоанализа асимметричных алгоритмов шифрования на основе факторизации составных чисел. – Вестник ДГТУ, том 11, № 9(60), 2011. – С. 1544–1554.

14. *Городилов А.Ю., Митраков А.А.* Криптоанализ тригонометрического шифра с помощью генетического алгоритма. //Вестник пермского университета. Серия: математика, механика, информатика, 20011, № 4, с. 75-82.

15. Материалы сайта http://mp.fizteh.urfu.ru/КМЗИ/Литература/В.П Сизов. Пример попытки разработки криптоалгоритма.doc – Сизов В.П. Новый алгоритм шифрования.

16. *Чернышев Ю.О, Сергеев А.С., Дубров Е.О., Рязанов А.Н.* Исследование возможности применения бионических методов пчелиных колоний для реализации криптоанализа классических шифров перестановок // Вестник ДГТУ, том 14, № 1(76), 2014. – С. 62–75.

Чернышев Юрий Олегович – почетный профессор ДГТУ, заслуженный деятель науки, доктор технических наук, профессор, кафедра «Автоматизация производственных процессов», Донской государственный технический университет. Тел.: (918) 599-16-45.

Chernyshev Yury Olegovich - honorary Professor DSTU, honored scientist , doctor of technical Sciences, Professor, the dept. «Automation of Production Processes», Don State Technical University. Phone: (918) 599-16-45.

Сергеев Александр Сергеевич – кандидат технических наук, доцент, докторант, кафедра «Автоматизация производственных процессов», Донской государственный технический университет. Тел.: (928) 758-57-19.

Sergeev Aleksandr Sergeevich - candidate of technical Sciences, associate Professor, doctoral candidate, Department of «Automation of Production Processes», Don State Technical University. Phone: (928) 758-57-19.

Дубров Евгений Олегович – аспирант, кафедра «Автоматизация производственных процессов», Донской государственный технический университет. Тел.: (918) 506-31-03.

Dubrov Evgeny Olegovich – postgraduate student, the dept. of «Automation of production processes», Don State Technical University. Phone: (918) 506-31-03.