УДК 519.7

ПРИМЕНЕНИЕ ГЕНЕТИЧЕСКИХ АЛГОРИТМОВ К ЗАДАЧЕ КРИПТОАНАЛИЗА КРИПТОСИСТЕМЫ МЕРКЛИ-ХЕЛЛМАНА

Беселия Л.Р.[1], *Кочладзе З.Ю.*[2]

[1]Сухумский государственный университет, Грузия
[2]Тбилисский государственный университет им. И. Джавахишвили, Грузия

Аннотация

Криптоанализ современных криптосистем является сложной задачей, в которой объем вычислений часто выходит за пределами реальных возможностей криптоаналитика. Эволюционные алгоритмы, а именно генетические алгоритмы, имеют возможность на основе целенаправленного поиска значительно уменьшить количество таких вычислений. В статье обсуждается вопрос использования генетических алгоритмов, для взлома криптосистемы Меркли-Хеллмана.

Cryptanalysis of modern cryptosystems is a complex task in which the amount of computation often goes beyond the real possibilities of the cryptanalyst. Evolutionary algorithms, namely genetic algorithms, have the ability, based on targeted search significantly reduce the number of such calculations. This article discusses the use of genetic algorithms to break the cryptosystem Merkley - Hellman.

Введение

Криптосистема Меркли - Хеллмана является шифром с открытым ключом, основанная на известной задаче ранца [1]. В первые Спильман [2] использоваль генетический алгоритм, чтобы взломать этот шифр. Несколько других исследователей [3,4,5] расширили работы в этом направлении концентрируя основное внимание на начальных параметров генетических алгоритмов. При этом, во всех этих работах рассматривается задача расшифрования шифротекста без нахождения секретного ключа.

Как известно, существует полиномиальный алгоритм А. Шамира [6], который успешно вскрывает систему Меркли -Хеллмана, вычисляя именно секретный ключ из открытого ключа. Целью данной работы является организовать с помощью генетических алгоритмов такое нападение на критосистему, который позволит нам восстановить секретный ключ из открытого ключа и сравнить полученные результаты с результатами работы алгоритма А. Шамира.

Шифр Меркли - Хеллмана, шифрация и дешифрация, генетические алгоритмы

Как известно, задача криптоанализа современных криптографических систем с открытым ключом является сложной задачей, решение которой требует как сложных математических вычислений над большими числами, так и обнаружение изъянов в самой криптосистеме.

Последнее время появились работы, в которых предпринята попытка применить методологию генетических алгоритмов для решения этой задачи.

Данная работа посвящена применению генетических алгоритмов к криптоанализу известной системы Меркли-Хеллмана. Выбор криптосистемы определен тем, что система, как известно, скомпрометирована и существует известный алгоритм Шамира, с помощью которого взломана эта система. Это даёт возможность сравнить насколько лучше может справиться с этой задачей генетический алгоритм.

Известные в литературе подходы вскрытия системы Меркли-Хеллмана с помощью генетических алгоритмов применяют атаку на основе известного открытого текста. При этом алгоритмы были ориентированы найти алгоритм дешифрации без нахождения секретного ключа. В отличие от таких подходов, в нашей работе предпринимается попытка из открытого ключа вычислить секретный ключ, применяя опять же атаку на основе открытого текста. Фитнес функция для нашего случая будет длина Хемминга, между данным открытым текстом и открытым текстом полученным на каждом этапе. Для того, чтобы произвести программное решение данной темы, мы применяем программный язык $C++$. Поставленную задачу, мы реализуем следующими действиями:

1. Анализ алгоритмов криптосистемы Меркли-Хеллмана;
2. Написание программного кода на $C++$ и создание формы;
3. Анализ генетического алгоритма и написание его программного кода;
4. Вынос на данную форму полученного открытого текста, погрешности и ключа.

Список использованных источников:

1. Merkle R.C., Hellman M.E. Hidding information and signatures in trapdoor Knapsak, IEEE Trans. Inform. Theory, IT-24 (1978), pp. 525-530.
2. Spillman R. Cryptanalysis of Knapsack ciphers using genetic algorithms. Cryptologria, October, 1993.
3. Yaseen, Sahasrabuddhe. A Genetic Algorithm for cryptanalysis of Chor Rivest Knapsack Public key cryptosystem, Third international conference on computational intelligence and multimedia applications, 1999.
4. Garg P., Shastri A. An Improved Cryptanalytic Attack on Knapsack Cipher using Genetic Algorithm. International Journal of Information Technology 3:3 2007.
5. Muthuregunathan R., Vekataraman D., Rajasekaran P. Cryptanalysis of Knapsack Ciher Using Parrallel Evolutionary Computing. International Journal of Recent Trends in Engineering, Vol. 1, No 1, May 2009.
6. Shamir A. A Polinomial-Time Algorithm for Breaking the Basic Merkle-Hellman Cryptosystem. IEEE Transactions on Information Theory Vol., IT-30, No5, september 1984, pp. 699-704.