УДК 004.056

ЗАСТОСУВАННЯ АЛГОРИТМУ КОЛОНІЇ БДЖІЛ ДЛЯ КРИПТОАНАЛІЗУ АСИМЕТРИЧНИХ КРИПТОГРАФІЧНИХ АЛГОРИТМІВ

Шадий В.І.

Гриник Р.О., ЛДУ БЖД, викладач КУІБ

ЛДУ БЖД

Усі асиметричні алгоритми шифрування використовують два ключі: відкритий K_{pub} та закритий K_{priv}.Кожен ключ складається з пари чисел, власне самого ключа та модуля *N*, $N = p \times q$, де *p* і *q* випадкові великі прості числа. Існує декілька варіантів атак на такі шифри, але найбільш оптимальним варіантом атак є розклад числа *N* на співмножники *p* і *q*.

Так як в даному випадку необхідно знайти екстремум не монотонної функції $F(x)$, то дослідження можливості застосування для вирішення даної задачі евристичних методів, що не використовують безпосередньо апарат математичного аналізу, є актуальним завданням. Таким чином, на основі математичної моделі алгоритму, заснованого на поведінці колонії бджіл, і його опису алгоритм факторизації числа сформулюємо в наступній формі:

1. Визначаються параметри алгоритму: кількість бджіл-розвідників *D*, кількість бджіл-робочих *B*, кількість ділянок для дослідження околиць *Z*, точність знаходження дільника *E*.
2. Вибираються на відрізку $[n_i, n_j]$ *D* значень аргументу $x_1, ..., x_D$.
3. У вибрані точки x_i відправляються бджоли-робочі для пошуку в їхніх околицях простих чисел, у відповідності з алгоритмом [1]:
   3.1. Визначити для кожного значення x_i значення околиці $r = n/1,442695$, де *n* – число біт в двійковому записі числа.
   3.2. Кожне число $y \in [x_i - r, x_i + r]$ послідовно перевіряється на ділення з простими числами з інтервалу $[2, 2 \times r]$.
   3.3. До чисел які пройшли тест на ділення застосовується тест Міллера-Рабіна [2].
4. Після визначення множини простих чисел *Y* для кожного $y_i \in Y$ обчислити значення функції $F(y_i)$, знайти $\min F(y_i)$. Визначити y_i для яких $F(y_i) < E$.
5. З множини *Y* вибираються випадковим чином *Z* елементів, дані значення позначаються як $x_1, ..., x_Z$. Далі відправляються бджоли-розвідники для пошуку на відрізку $[n_i, n_j]$ *D* значень аргументу $x_{Z+1}, ..., x_{Z+D}$. Якщо умова виходу з алгоритму не виконана необхідно перейти до пункту 3, якщо виконана до пункту 6.
6. Завершити роботу алгоритму.

Умовою зупинки алгоритму може бути закінчення часового ресурсу, визначення величини x_i для яких $F(x_i) = 0$ або $F(x_i) < E$, визначення значення функції $F(x_i)$ для всіх $x_i \in [n_i, n_j]$.

Таким чином, в даному алгоритмі вибір значень аргументу $x_i \in [n_i, n_j]$ імітує поведінку бджіл-розвідників, а пошук в околиці найбільш ймовірних простих чисел імітує поведінку робочих бджіл (бджіл-фуражирів). Оскільки в даному випадку визначається екстремум не монотонної функції, то вибір точок x_i на відрізку $[n_i, n_j]$ для пошуку простих

чисел в їх околиці проводиться на кожній ітерації випадковим чином, що призводить в загальному випадку до рівно ймовірної можливості отримання глобального оптимуму на кожній ітерації (на відміну від спрямованого сходження до екстремуму в класичному бджолиному алгоритмі, описаному в [3]).

ЛІТЕРАТУРА

1. Кажаров А.А. Разработка модели криптоанализа RSA при помощи генетических алгоритмов / А. А. Кажаров, Х. А. Кажаров.

2. 20. Аврутин, В. А. Алгоритм поиска простых чисел в заданном интервале / В. А. Аврутин. Электрон, ресурс. Режим доступа: http://library.mephi.ru/data/scientific-eessions/2003/12/024.html

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