УДК 004.056.55

Побудова інтелектуальної моделі криптоаналізу шифру Рабіна на базі генетичного алгоритму

Гриник Р.О., викладач, r.grynyk@yandex.ru,
Полотай О.І., ст. викладач, к.т.н., orest.polotaj@gmail.com
Львівський державний університет безпеки життєдіяльності, м. Львів

Алгоритм Рабіна - це асиметрична криптосистема яка використовує відкритий ключ (n) для шифрування повідомлення і закритий ключ (q, n) для розшифрування криптограми. Безпека даної криптосистеми визначається складністю пошуку квадратних коренів по модулю складного числа [6]. Генерування ключів відбувається наступним чином:

- Вибираються пара великих простих чисел (p, q) таких, щоб при діленні на 4 вони давали остачу 3.
- Обчислюється модуль $\mathrm{n} = \mathrm{p} * \mathrm{q}$, який і є відкритим ключем

Крипостійкість алгоритму Рабіна визначається трудомісткістю факторизації великих чисел, тобто для розкриття криптограми необхідно відкритого ключа (n) отримати два простих числа $(p * q)$, тобто задача криптоаналізу зводить до розкладання на множники великого числах.

Перед побудовою інтелектуальної системи для вирішення задачі факторизації необхідно вирішити декілька задач, таких як:

- спосіб представлення хромосоми;
- побудова цільової функції;
- формування початкової популяції;
- вибір (комбінування) генетичних операторів, таких як: вибір батьківських хромосом, схрещення, мутації та селекція.

Структура хромосом. Структура хромосоми являє собою бітову стрічку, котра зберігає інформацію про простий множник, а другий множник знаходиться з $\mathrm{n} = \mathrm{p} * \mathrm{q}$.

Формування початкової популяції. Для формування початкової популяції генерується просте число *G* випадковим вибором значення бітів, причому останній біт завжди повинен бути рівним одиниці. Коли число згенероване, необхідно визначити середню відстань між простими числа заданого порядку – *r*.

$$r = \ln(G) = \frac{log_2 G}{log_2 e} = \frac{log_2 G}{1.44265}$$

Знаючи число біт *n* рівняння приймає наступний вигляд:

$$r = \frac{n}{1.442695} \quad (3)$$

Після обчислення r формується масив чисел в діапазоні $[G - r; G + r]$. Для заданого діапазону будуємо решето Ератосфена. Кожне число $x \in [G - r; G + r]$ послідовно перевіряємо на подільність з простими числами в діапазоні $[2; 2r]$. В даному випадку прості числа в цьому діапазоні необхідно вирахувати заздалегідь, причому будь-яким методом.

Після звуження простору пошуку рішень, до множини можливих рішень, що залишилися застосовуємо тест Міллера-Рабіна [1].

Побудова цільової функції. Декодування хромосоми дає значення першого потенційно простого множника p, для якого є лише один однозначний співмножник. Далі, до отриманого результату застосовуємо імовірнісний тест Міллера-Рабіна з метою отримання інформації про ймовірність простоти числа q. Оскільки кожна хромосома знаходиться в результаті локального пошуку із застосуванням вищевказаного імовірнісного тесту, то можна припустити, що кожний співмножники з певною ймовірністю являється простим. Таким чином, значення цільової функції визначається добутком ймовірностей двох співмножників.

Оператор вибору пари хромосом для створення нової хромосоми. Найбільш ефективним для даної задачі є випадковий вибір батьківських хромосом, оскільки ймовірність того, що $p(q) = 0$ досить висока відповідно і ймовірність того, що цільова функція в цілому для багатьох хромосом в популяції буде дорівнювати нулю, висока, то елітний вибір і «колесо рулетки» будуть призводити до локалізації простору пошуку [2].

Вибір оператора схрещення. У даній роботі застосовувався двоточковий кросинговер. У двоточковому кросинговері хромосоми розглядаються як цикли, які формуються з'єднанням кінців лінійної хромосоми. На даний момент багато дослідників погоджуються, що двоточковий кросинговер кращий, ніж одноточковий [5].

Оператор мутації. Після процесу схрещення відбувається процес мутації. Даний оператор необхідний для «вибивання» популяції з локального екстремуму і перешкоджає передчасній збіжності алгоритму. Це досягається за рахунок того, що змінюється випадково обраний ген в хромосомі.

Селекція. Для створення нової популяції можна використовувати різні методи відбору особин, такі як: елітарний відбір, витіснення, відбір усіканням та інші. Витіснення в даному випадку формує нову популяцію скоріше з віддалених особин, ніж з особин, що групуються близько поточного знайденого рішення. Даний метод найбільш придатний для багато екстремального завдання, при цьому крім визначення глобальних екстремумів з'являється можливість виділити і ті локальні максимуми, значення яких близькі до глобальних [5].

Параметри інтелектуальної системи. Представлена інтелектуальна система характеризується наступними параметрами:

а) кількість популяцій;

б) розмір популяцій;

в) кількість індивідів для вибірки при міграції.

Висновок. Отже, використавши генетичний алгоритм, можна побудувати інтелектуальну модель розкладання великого числа на два простих співмножника, що дає змогу здійснити успішну атаку на криптографічну систему Рабіна знаючи відкритий ключ. Для здійснення успішної атаки необхідно правильно підібрати такі параметри, як кількість популяції та її розмір.

Список літератури

1. Arnault, F. "Rabin-Miller Primality Test: Composite Numbers Which Pass It." Math. Comput.64, 355-361, 1995.

2. David Michael Chan, Automatic Generation of Prime Factorization Algorithms Using Genetic Programming, Stanford Bookstore, 2002.

3. Yitang Zhang, Bounded gaps between primes, Annals of Mathematics 2013

4. Кажаров Х.А. Разработка генетической модели поиска простых чисел для криптоанализа rsa на основе клиент-серверной структуры / Х.А. Кажаров // Известия Южного федерального университета. Технические науки. Т 86, №9, 2008. С. 40-46.

5. Панченко Т.В., Генетические алгоритмы: учебно-методическое пособие/ под ред. Ю.Ю. Тарасевича. — Астрахань : Издательский дом «Астраханский университет», 2007. — 87 с

6. Шнайер Б., Прикладная криптография. 2-е издание. Протоколы, алгоритмы и исходные тексты на языке С. – Пер. с англ.: М.: Издательство ТРИУМФ, 2002. 816 с.