МОДЕЛЬ РОЗКРИТТЯ КРИПТОСИСТЕМИ РАБІНА НА БАЗІ ГЕНЕТИЧНОГО АЛГОРИТМУ

Богдан Куровець, Наталія Кухарська, Ростислав Гриник
Львівський державний університет безпеки життєдіяльності, м. Львів

У роботі розглянуті принципи асиметричної криптосистеми Рабіна, аналізуються методи розкриття шифрів, побудованих на основі розкладання на множники великих чисел.

Ключові слова: криптосистема Рабіна, криптографія, генетичний алгоритм, система інформаційної безпеки, система безпеки, інформаційні ресурси.

The paper considers the principles of the asymmetric cryptosystem of Rabin, analyzes the methods of disclosure of ciphers constructed on the basis of the complexity of the decomposition of a large number on simple factors.

Key words: Rabin cryptosystem, cryptography, Genetic Algorithm, information security system, security system, information resources.

Шифрування інформації в даний час стало чи не основним методом її захисту. Доступність обчислювальної техніки та стрімкий прогрес у її розвитку привели до вдосконалення давно відомих криптографічних систем захисту інформації і застосуванню їх в масовому масштабі. Однак у цього прогресу є й інша сторона: великі можливості обчислювальних пристроїв сьогодні успішно застосовуються не тільки для шифрування, але і для розкриття тих криптосистем, які ще вчора, здавалося б, гарантували надійний захист інформації.

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 [1]. Генерування ключів відбувається наступним чином:

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

Крипостійкість алгоритму Рабіна визначається трудомісткістю факторизації великих чисел, тобто для розкриття криптограми необхідно для відкритого ключа *(n)* отримати два простих числа *(p,q)*, тобто задача криптоаналізу зводиться до розкладання на множники великих чисел [2].

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 є бітоою стрічкою, котра зберігає інформацію про простий множник, а другий множник шукається з $n = p \times q$.

Побудова цільової функції. Декодування хромосоми дає значення першого потенційно простого множника *p*, для якого є лише один однозначний співмножник:

$$q = \frac{n}{p}$$

Далі, до отриманого результату застосовуємо імовірнісний тест Міллера-Рабіна з метою отримання інформації про ймовірність простоти числа *q*. Таким чином, значення цільової функції (ЦФ) визначається добутком ймовірностей двох співмножників:

$$P = P(q) \times P(p)$$

Формування початкової популяції. Просте число генерується випадковим вибором значення бітів. Останній біт завжди встановлюється рівним одиниці. Потім обчислюється середня відстань між простими числами – *r*, після чого в діапазоні $[G-r;G+r]$ здійснюється пошук найімовірнішого простого числа.

Вибір батьківських хромосом. Експериментальні дослідження показали, що найбільш ефективним є випадковий вибір [1]. Це обумовлено специфікою завдання. 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, а генетичний алгоритм увійде в стан стагнації.

Оператором схрещення був обраний кросинговер — це комбінування хромосом шляхом замін значень генів і утворення нових хромосом на їх місцях.

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

Селекція полягає в тому, що батьками можуть стати тільки ті особини, значення пристосованості яких не менше порогової величини, наприклад, середнього значення пристосованості по популяції.

Криптосистема Рабіна є однією з стійких алгоритмів шифрування інформації з відкритим ключем. Безпека алгоритму Рабіна обумовлюється складністю факторизації цілих чисел. Для розкриття цієї криптосистеми необхідно вирішити задачу розкладання модуля *n* на два простих числа *p* і *q*. Цю задачу можна вирішити з допомогою генетичного алгоритму, для цього необхідно підібрати спосіб представлення ключа та оптимальну фітнес-функцію.

Література

1. Шнайер Б., Прикладная криптография. 2-е издание. Протоколы, алгоритмы и исходные тексты на языке С. – Пер. с англ.: М.: Издательство ТРИУМФ, 2002. 816 с.
2. David Michael Chan, Automatic Generation of Prime Factorization Algorithms Using Genetic Programming, Stanford Bookstore, 2002.