УДК 004.415.5

Г. Поліщук, С. Лупенко
(Тернопільський національний технічний університет імені Івана Пулюя)

МЕТОДИ ФАКТОРИЗАЦІЇ ВЕЛИКИХ ЧИСЕЛ

На сьогоднішній день важко переоцінити важливість безпеки інформації в світлі бурхливого розвитку телекомунікацій. В сучасних умовах розвитку та широкого застосування такого методу захисту інформації як шифрування неабиякої важливості набуває питання безпеки використання алгоритмів шифрування. Базуючись на проблемі факторизації, алгоритм RSA являє собою широке поле для дослідження науковців. Даний алгоритм шифрування з відкритим ключем є найбільш популярним. В силу безперервного розвитку комп'ютерної техніки, а також значних досягнень в області криптоаналізу та теорії чисел регулярна перевірка надійності RSA є актуальною.

Безпека алгоритму RSA побудована на принципі складності факторизації натурального числа [1]. Конкурс, оголошений лабораторією RSA [2], основною метою має визначення безпечної величини числа, що є добутком двох простих чисел (ключів). На даний час число в 1024 біти вважається надійним. Існує припущення, що проблема факторизації не буде вирішена допоки не буде винайдено принципово новий метод розкладу на множники або квантовий комп'ютер, оскільки на якому згідно з [3], використовуючи алгоритм Шора, модуль RSA можна розкласти за поліноміальний час.

На сьогодні відомо декілька ефективних методів факторизації. Основною характеристикою оцінки роботи алгоритмів факторизації є час їх роботи, що може бути оцінений як ймовірнісно так і детермінованій постановці. В залежності від цієї характеристики алгоритми можна розділити на експоненціальні і субекспоненціальні, де перші є досить ефективними для невеликих чисел.

В доповіді розглянуто лише алгоритми, час роботи яких є субекспоненціальним, зокрема, це метод квадратичного решета, метод загального решета числового поля, метод спеціального решета числового поля, метод еліптичних кривих. Проаналізовано їх прикладне застосування до системи RSA, недоліки та переваги, можливі шляхи вдосконалення.

Література

1. Rivest, R.; A. Shamir; L. Adleman (1978). "A Method for Obtaining Digital Signatures and Public-Key Cryptosystems". Communications of the ACM 21 (2): 120–126

2. http://www.rsa.com

3. Lu, Chao-Yang; Browne, Daniel E.; Yang, Tao & Pan, Jian-Wei (2007), "Demonstration of a Compiled Version of Shor's Quantum Factoring Algorithm Using Photonic Qubits", Physical Review Letters 99