РЕАЛІЗАЦІЯ ЗАСОБУ ПРИСКОРЕННЯ РОБОТИ АСИМЕТРИЧНОГО АЛГОРИТМУ ШИФРУВАННЯ

канд. техн. наук, доц. О.І. Баленко, канд. екон. наук, доц. М.І. Главчев, канд. техн. наук, доц. А.М. Філоненко, магістр Н.О. Брік,
Національний технічний університет "Харківський політехнічний інститут", м. Харків

Криптографічні системи з відкритим ключем (асиметричні криптосистеми) є найбільш криптостійкими та надійними. Вони засновані на розкладенні великих простих чисел, на кінцевих логарифмах та на еліптичних функціях. Але їх активному застосуванню заважають дуже складні математичні розрахунки, а слід з цього, швидкодія цих алгоритмів дуже низька. Тому питання прискорення роботи асиметричних алгоритмів – це дуже актуальна и важлива задача.

Основною метою дослідження в прискоренні обчислення експоненти на кінцевих полях Галуа за рахунок оптимізації організації обчислювального процесу та урахування специфіки виконання цієї операції в реальних системах криптографічного захисту даних. Для виконання мети були вирішені наступні задачі: проведений аналіз використання кінцевих полів Галуа в сучасних протоколах криптографічного захисту інформації для виявлення резервів підвищення їх швидкодії за рахунок прискорення експоненціювання на кінцевих полях Галуа; розроблений метод прискорення експоненціювання на кінцевих полях Галуа за рахунок табличної реалізації частини обчислень проведених попередньо, які залежать лише від утворюючого поліному, що є частиною відритого ключа і, відповідно, практично не змінюється; запропоновано використання технології Монтгомері для прискорення редукції на полях Галуа та розроблений відповідний спосіб виконання множення та експоненціювання на кінцевих полях Галуа з редукціюванням результатів поліноміального множення за технологією Монтгомері.

На підставі дослідження для перевірки ефективності було розроблено програмне забезпечення, яке виконанує порівняння швидкодії експоненціювання на кінцевих полях Галуа класичним та запропонованим методами за експериментальними даними. Результат використання запропонованого методу показав збільшення швидкодії роботи алгоритму та особливо це визначилось при збільшенні розрядності ключа шифрування.

Список літератури: 1. *Menezer A.J.* Handbook of Applied Cryptography / *A.J. Menezer, Van Oorschot P.C., Vanstone S.A* // CRC-Press. – 1997. **2.** *Николайчук Я.М.* Коди полів Галуа: теорія і застосування // Тернопіль: Вид-во ТНУ. – 2012**. 3.** *Montgommery P.L.* Modular multiplication without trial division // Mathematics of Computation. – 1985 – Vol. 44. – P. 519-521.