УДК 004.942
Яциковська У.- ст. гр. КСМ-31
Тернопільський національний економічний університет

ДОСЛІДЖЕННЯ ЧАСОВОЇ РЕАЛІЗАЦІЇ АЛГОРИТМУ ЕЛЕКТРОННОГО ЦИФРОВОГО ПІДПИСУ RSA

Науковий керівник: викладач Дубчак Л.О.
Консультант: д.т.н., проф. Карпінський М.П.

Сучасні інформаційні системи забезпечують створення, відправлення, передавання, одержання, зберігання, оброблення, використання та знищення електронних документів. Обов'язковим реквізитом електронного документа, без якого він не може мати підстави для обліку і не матиме юридичної сили, є електронний підпис, що використовується для ідентифікації автора або підписувача електронного документа іншими суб'єктами електронного документообігу. Електронний цифровий підпис – це послідовність символів, отримана за результатом криптографічного перетворення набору електронних даних, який додається до цього набору або логічно з ним поєднується. Першою та найвідомішою у світі системою ЕЦП стала система RSA, математична схема якої була розроблена у 1977 році у США. Загальний алгоритм електронного цифрового підпису на основі RSA використовує алгоритм генерування великих простих чисел (в даному випадку використовувалось "сито Ератосфена"), а також алгоритм знаходження НСД двох чисел.

Для проведення аналізу продуктивності та стійкості алгоритму цифрового електронного підпису на основі алгоритму RSA необхідно спочатку визначити загальний час його виконання. Для побудови математичної моделі часової реалізації необхідно здійснити аналіз часу виконання кожної операції даного алгоритму. Крім того, необхідно врахувати ймовірність виконання умов, які використовуються в алгоритмі. Математична модель часової реалізації алгоритму ЕЦП на основі RSA має наступний вигляд:

$$T = 4t_1 + \frac{440}{3}t_2 + 4t_3 + 7t_4 + 4t_5 + 4t_6 + 3t_7 + 14t_8 + 2t_{10} + 3t_{12} + t_{\mathrm{mod\,exp}},$$

де t_1 - час, затрачений на вибір випадкового числа, t_2 - час, затрачений на просте присвоєння, t_3 - затрати часу на додавання (віднімання), t_4 - час, витрачений процесором на перевірку співвідношення двох чисел, t_5 - час, затрачуний на знаходження числа за модулем, t_6 - на множення (ділення) двох чисел, t_7 - на знаходжкння $\lceil a/b \rceil$, t_8 - час, затрачений на $a \oplus b$, t_{10} - на розбиття повідомлення на блоки, t_{12} - час, затрачений на знаходження результату хеш-функції, $t_{\mathrm{mod\,exp}}$ - час піднесення числа до степеня за модулем.

Виходячи з досліджень, проведених на кафедрі БІТ, ТНЕУ, випливає, що алгоритм ЕЦП на основі RSA має найвищу продуктивність та стійкість при використанні β-арного методу зліва направо чи методу ковзаючого вікна зліва направо піднесення до степеня за модулем. Крім того, на загальний час виконання алгоритму ЕЦП впливає і складність одно направленої хеш-функції (що є наступною проблемою для дослідження).

Проведені дослідження дозволяють проводити аналіз і інших алгоритмів електронного цифрового підпису.