УДК 681.3.05

В. Г. Красиленко[1], Р.О. Яцковська [2], Ю.М. Тріфонова [1]

krasilenko@mail.ru, rimma_pr@inbox.ru

1 - Вінницький соціально-економічний інститут Університету «Україна»
2 – Вінницький національний аграрний університет

ДЕМОНСТРАЦІЯ ПРОЦЕСІВ СТВОРЕННЯ СЛІПИХ ЕЛЕКТРОННИХ ЦИФРОВИХ ПІДПИСІВ НА ТЕКСТОГРАФІЧНУ ДОКУМЕНТАЦІЮ НА ОСНОВІ МОДЕЛЕЙ МАТРИЧНОГО ТИПУ

Вступ та аналіз публікацій. Однією з актуальних та необхідних задач є задача створення електронних цифрових підписів (ЕЦП) для текстографічних документів (ТГД). Серед них можна відмітити незаперечні підписи, сліпі підписи та інші. Але більшість відомих алгоритмів та протоколів створення ЕЦП, протоколів формування ключів та систем верифікації ЕЦП орієнтовані на послідовну скалярну обробку блоків ТГД. В [1] були запропоновані матричні моделі (ММ), які можуть бути використані і для любих ТГД. Модифікації системи RSA на матричний випадок були запропоновані в роботі [2. Сліпі ЕЦП на основі матричних афінних шифрів та результати їх моделювання розглядалися в роботі [3]. Проблемі створення та моделювання сліпих ЕЦП для ТГД за допомогою (ММ) на основі базової моделі RSA присвячена робота [4]. Але в ній наводилися результати моделювання таких ЕЦП матричного типу (МТ) лише для невеликих масивів чорно-білих на півтонових зображень розмірністю 128×128 елементів. **Постановка задачі**. Тому метою даної роботи є подальше дослідження матричних моделей при створенні сліпих ЕЦП МТ та демонстрація експериментами у середовищі Mathcad їх функціональних можливостей при створенні підписів на великоформатні ТГД.

Виклад основних результатів. Ідея модифікацій класичних ЕЦП СТ до МТ базується на узагальненні базового скалярного алгоритму RSA до відповідної ММ [2]. Для реалізації запропонованого підходу в якості ключів вибираються не скаляри а відповідні матриці KEYP та OKEY. Значення елементів матричних ключів KEYP та OKEY вибираються з множини взаємно простих чисел, що задається відповідною функцією Ейлера від n_{ij}, яка і визначає потужність цієї множини. Ключі формуються як матриці, кожен елемент яких вибирається з множини значень відповідних скалярних ключів e_{ij} та d_{ij}. Для моделювання ми використовували матриці 704 × 572 елементи та ТГД формату А4. Для створення сліпого ЕЦП МТ на документ ТГД (матриця S1) останній коригується до матриці MPR. Така корекція полягає у зменшенні тих градацій інтенсивності пікселів, що перевищують допустимі значення n_{ij}. Ключ KG також коригується абонентом до ключа KGP. Ключ KEYP формується з випадкової матриці G2. Потім формується допоміжна матриця T1: $T1 = KGP^{[\wedge]KEYP} \bmod kl$, де $[\wedge]$ - операція по елементного піднесення в степінь за модулем. Матрицею T1 зображення MPR закривається, а закрите повідомлення T відсилається для підписування нотаріусу: $T = MPR \underset{kl}{\Theta} T1$, де $\left(\underset{kl}{\Theta}\right)$ - операція поелементного множення матриць за модулем kl або модулями n_{ij}, коли використовуються різні модулі для елементів. Отримане повідомлення T підписується ключем OKEY і підписаний документ у вигляді матриці ST відсилається абоненту: $ST = T^{[\wedge]OKEY} \bmod kl$. Нотаріус не бачить текст ТГД, бо бачить лише його закриту копію T, а ключ OKGP він не знає. Отриманий підписаний ТГД (матриця ST), абонент перемножує на матрицю OKGP та отримує підписаний документ PMPR, який є по суті OKEY-степінню документу MPR (MV) за відповідним модулем: $PMPR = ST \underset{kl}{\Theta} OKGP$,

$MV = MPR^{[\wedge]OKEY} \bmod kl$. Результати моделювання ЕЦП МТ будуть продемонстровані.

Висновки. Наведені результати моделювання процесів створення ЕЦП МТ (RSA та Ель-Гамаля) для великоформатних документів у Mathcad, що підтвердили правильність їх функціонування та верифікації.

Список літератури

1. Красиленко В.Г. Моделювання матричних алгоритмів криптографічного захисту / В.Г. Красиленко, Ю.А. Флавицька // Вісник НУ «Львівська політехніка». «Компьютерні системи та мережі». – 2009.– №658. – С.59-63.

2. Красиленко В. Г. Модифікації системи RSA для створення на її основі матричних моделей та алгоритмів для зашифрування та розшифрування зображень [Текст] / В.Г. Красиленко, С. К. Грабовляк // Системи обробки інформації. – 2012 . – №8(106).–С.102-106.

3. Красиленко В.Г., Матричні афінні шифри для створення цифрових сліпих підписів на текстографічні документи / В.Г. Красиленко, С.К. Грабовляк // Системи обробки інформації. – Х.: ХУПС, 2011.–Вип. 7(97).–С.60–63.

4. Красиленко В.Г. Моделювання сліпих електронних цифрових підписів матричного типу на конфіденційну текстографічну документацію / В.Г. Красиленко, Р. О. Яцковська, С. К. Грабовляк, // І Міжнародна науково-методична конференція Вінниця: ВНАУ, 2012. –С. 103-107.