УДК 581.341

ЗАСТОСУВАННЯ ПРОГРАМНОЇ РЕАЛІЗАЦІЇ ЕЛЕКТРОННОГО ЦИФРОВОГО ПІДПИСУ RSA ПРИ ВИКЛАДАННІ ДИСЦИПЛІНИ "ЗАХИСТ ІНФОРМАЦІЇ В ТЕЛЕКОМУНІКАЦІЙНИХ СИСТЕМАХ ТА МЕРЕЖАХ"

А.О. Москаленко, Ю.П. Бендес, С.В. Сомов
(Полтавський військовий інститут зв'язку)

Наведено приклад використання віртуальних моделей цифрового підпису на заняттях з дисципліни "Захист інформації в телекомунікаційних системах та мережах".

програмна реалізація, електронний цифровий підпис RSA, захист інформації

Запровадження інформаційних технологій практично в усі сфери суспільного життя неминуче призводить до зростання об'єму інформації, що циркулює в них. В сучасних інформаційних системах оброблюється інформація різних категорій, серед яких й інформація з обмеженим доступом.

Згідно нормативно-правової бази України, інформація, що належить до категорії "З обмеженим доступом" повинна підлягати захисту. Забезпечити надійний захист можуть лише фахівці, що володіють знаннями в області безпеки інформаційних технологій. Тому, в Полтавському військовому інституті зв'язку вивчається дисципліна "Захист інформацій в телекомунікаційних системах та мережах". Як окрема тема даної дисципліни вивчається електронно-цифровий підпис (ЕЦП).

Під ЕЦП розуміється вид електронного підпису, отриманого за результатом криптографічного перетворення набору електронних даних, який додається до цього набору або логічно з ним поєднується і дає змогу підтвердити його цілісність та ідентифікувати підписувача. Електронно-цифровий підпис накладається за допомогою особистого ключа та перевіряється за допомогою відкритого ключа. Одним із видів електронно-цифрового підпису є електронно-цифровий підпис на основі криптографічної системи RSA. Розглянемо принципи його функціонування.

Спочатку необхідно розрахувати пару ключів (закритий та відкритий). Для цього відправник (автор) електронних документів обчислює два великих простих числа P та Q , потім знаходить їх добуток $N = P \cdot Q$ та значення функції $\varphi(N) = (P-1)\cdot(Q-1)$. Потім відправник обчислює число E з умови

$E \le \varphi(N), НОД(E, \varphi(N)) = 1$ та число D з умови $D < N, E \cdot B \equiv 1 (\mathrm{mod}\, \varphi(N))$. Пара чисел (E, N) є відкритим ключем. Цю пару чисел автор передає партнерам з листування для перевірки його цифрових підписів. Число D зберігається автором як секретний ключ для підписання.

Узагальнена схема формування та перевірки цифрового підпису RSA зображена на рис. 1.

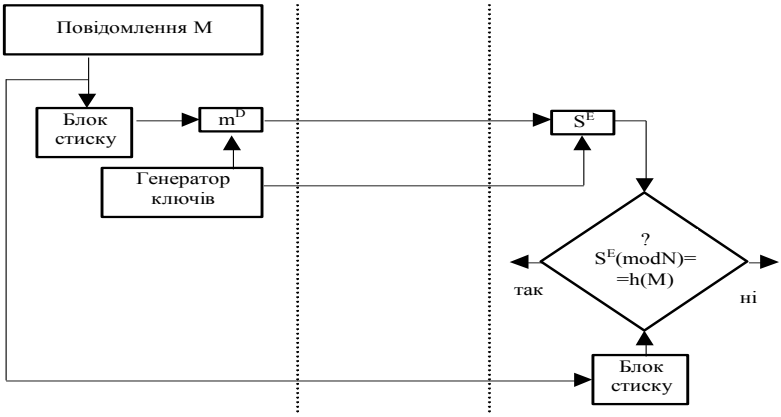

Рис. 1. Узагальнена схема цифрового підпису RSA

Припустимо, що відправник хоче підписати повідомлення M перед його відправкою. Спочатку повідомлення M (блок інформації, файл, таблиця) стискують за допомогою хеш-функції $h(\cdot)$ в ціле число m:

$$m = h(M).$$

Потім розраховують цифровий підпис S під електронним документом M, використовуючи хеш-значення m та закритий ключ D:

$$S = m^D (\mathrm{mod}\, N).$$

Пара (M, S) передається партнеру-одержувачу як електронний документ M, підписаний цифровим підписом S, причому підпис S сформований володарем секретного ключа D. Після прийому пари (M, S) одержувач обчислює хеш-значення повідомлення M двома різними способами. Перед усім він відновлює хеш-значення m', застосовуючи криптографічне перетворення підпису S з використанням відкритого ключа E:

$$m' = S^E (\mathrm{mod}\, N).$$

Крім цього, він знаходить результат хешування прийнятого повідомлення M за допомогою такої ж хеш-функції h (.):

$$m = h(M).$$

Якщо виконується рівність обчислених значень, тобто $S^E(modN) = h(M)$,

то одержувач признає пару (M, S) дійсною. Доведено, що тільки власник секретного ключа D може сформувати цифровий підпис S по документу M, а знайти секретне число D по відкритому числу E не легше, ніж розкласти модуль N на множники.

В сучасному світі ЕЦП застосовується в системах електронних платежів, електронного документообігу та електронної пошти та ін. ЕЦП дозволяє надати юридичний статус електронним документам.

Проте, для дослідження ЕЦП необхідно застосовувати програмні та апаратні засоби, що надзвичайно дорого коштують. А ще, якщо врахувати незначну наочність та неможливість дослідження окремих параметрів ЕЦП, то можливо зробити висновок, що застосовувати розроблені апаратні та програмні засоби ЕЦП для навчання є неефективним. Тому, для дослідження ЕЦП RSA в ПВІЗ розроблено віртуальну лабораторну роботу, що дозволяє значно скоротити витрати, підвищити наочність навчання.

Організаційно віртуальність лабораторної роботи складається з 3 частин: ***описової частини***, що являє собою електронний підручник, в якому викладені положення, необхідні для підготовки та проведення лабораторної роботи (рис. 2); ***тестової частини***, що контролює рівень підготовки для виконання лабораторної роботи (рис. 3); ***практичної частини***, що містить пакет програм, необхідних для проведення лабораторної роботи (рис. 4).

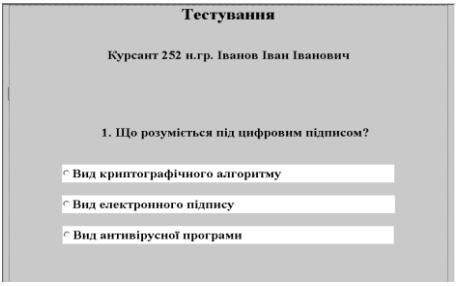

Рис. 2. Описова частина

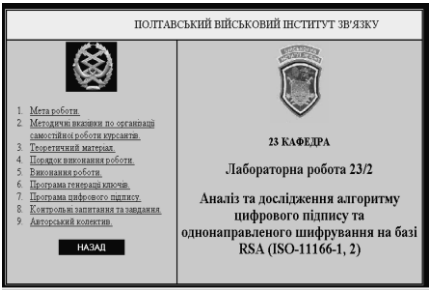

Рис. 3. Тестова частина

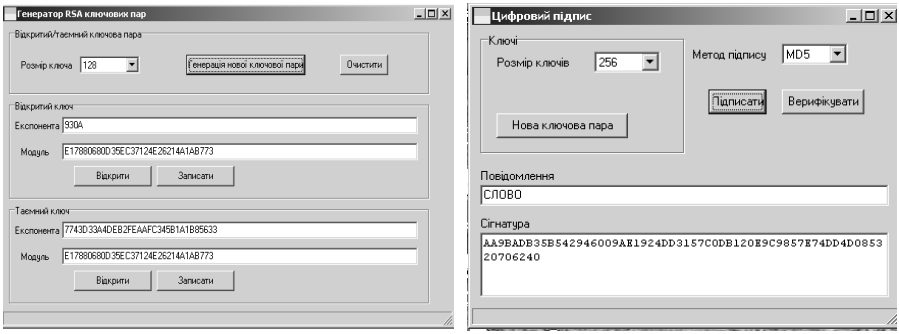

Рис. 4. Практична частина

При виконанні практичної частини роботи необхідно запустити на виконання програму генерації ключів. Змінюючи довжину ключа в межах від 128 до 1024 біт дослідити залежність часу генерації ключа від вибраної довжини ключа. Зберегти ключові послідовності різної довжини у файлах. Потім запустити на виконання програму цифрового підпису.

Для підпису будь-якого повідомлення спочатку необхідно відкрити файли, в яких містяться ключові дані, вибрати метод хешування, а також ввести з клавіатури, або записати з файлу повідомлення, яке необхідно підписати. Далі підписати повідомлення натискаючи кнопку “підписати”. Передати повідомлення з цифровим підписом вказаному абоненту. Для перевірки підпису абонент повинен: відкрити файл ключа, вибрати алгоритм хешування, завантажити повідомлення з цифровим підписом та натиснути кнопку “верифікувати”. При успішній перевірці з’явиться повідомлення “Повідомлення підписано вірно”, в іншому ж випадку – “Повідомлення підписано невірно”. Далі змінюючи розмір ключа, алгоритм хешування та повідомлення, дослідити як ці величини впливають на час генерації та перевірки підпису, форму та розмір підпису. На останньому етапі виконання роботи необхідно виконувати всі вище перераховані дії, але при передачі повідомлення і цифрового підпису абоненту, вносити по черзі зміни в повідомлення та в цифровий підпис.

Висновки. Використання розробленої віртуальної моделі на заняттях з курсантами та студентами показало придатність до застосування при викладанні дисципліни “Захист інформації в телекомунікаційних системах та мережах” як у вигляді лекційних демонстрацій, на практичних заняттях та лабораторних роботах. Проведені заняття з використанням віртуальної моделі показали, що її доцільно використовувати з метою активізації пізнавальної діяльності студентів та курсантів, максимального врахування індивідуальних особливостей та диференціації навчання.

Дана комп’ютерна модель дозволяє перейти від репродуктивного

рівня навчання до творчого, наводити приклади та контрприклади до алгоритму RSA і створювати проблемні ситуації на занятті.

ЛІТЕРАТУРА

1. *Бернет С., Пэйн С. Криптография. Офиц. рук-во RSA Security. – 2002. – 384 с.*
2. *Иванов Б.Н. Дискретная математика. – М.: Наука, 2002. – 288 с.*
3. *Коутинхо С. Введение в теорию чисел. Алгоритм RSA. – М.: Мир, 2001. – 328 с.*

Надійшла 20.10.2005

Рецензент: доктор технічних наук, професор Р.Г. Савенко,
Полтавський військовий інститут зв'язку