Практичне заняття 3
Використання цифрових підписів

Цілі та задачі

Зрозуміти концепції цифрового підпису.

Частина 1: Продемонструвати використання цифрових підписів.

Частина 2: Продемонструвати перевірку цифрового підпису.

Довідкова інформація / Сценарій

Цифровий підпис - це математичний метод, який використовується для перевірки автентичності та цілісності цифрового повідомлення. Цифровий підпис є еквівалентом рукописного підпису. Цифрові підписи можуть бути набагато більш безпечними. Мета цифрового підпису полягає в тому, щоб запобігти підробці та інперсоніфікації цифрових повідомлень. У багатьох країнах, включаючи Сполучені

Штати, цифрові підписи мають таке ж юридичне значення, як і традиційні форми підписаних документів. Уряд Сполучених Штатів тепер публікує електронні версії бюджетів, законів і законопроектів Конгресу з цифровими підписами.

Необхідні ресурси

- ПК або мобільний пристрій з доступом до Інтернету

Part 1: Використання цифрових підписів

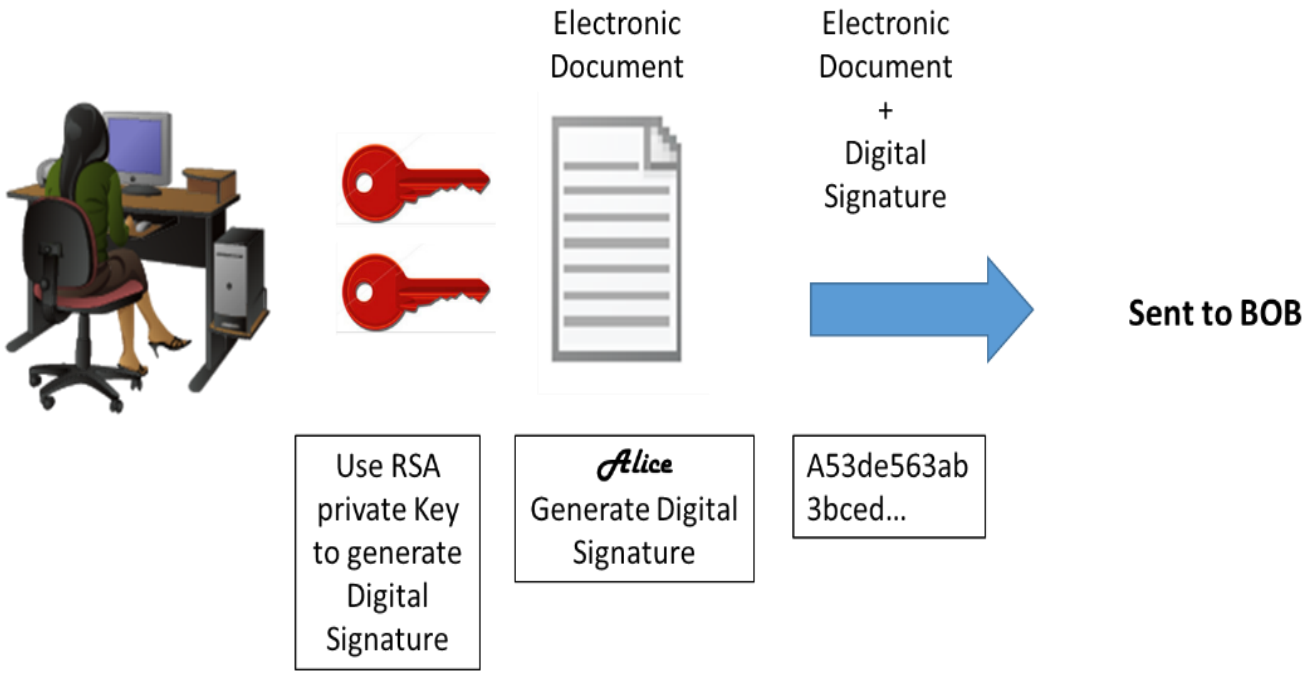
У цій частині ви будете використовувати веб-сайт для перевірки підпису документа між Алісою і Бобом. Аліса і Боб використовують одну пару закритих і відкритих ключів RSA. Кожен з них використовує свій закритий ключ для підписання юридичного документа. Потім вони відправляють документи один одному. І Аліса, і Боб можуть перевірити підпис один одного відкритим ключем. Вони також повинні домовитися про спільну відкриту експоненту для розрахунку.

Таблиця 1 - Відкритий і закритий ключі RSA

Відкритий ключ RSA	d94d889e88853dd89769a18015a0a2e6bf82bf356fe14f251fb4f5e2df0d9f9a94a68a30c428b39e3362fb3779a497eceaea37100f264d7fb9fb1a97fbf621133de55fdcb9b1ad0d7a31b379216d79252f5c527b9bc63d83d4ecf4d1d45cbf843e8474babc655e9bb6799cba77a47eafa838296474afc24beb9c825b73ebf549
Закритий ключ RSA	47b9cfde843176b88741d68cf096952e950813151058ce46f2b048791a26e507a1095793c12bae1e09d82213ad9326928cf7c2350acb19c98f19d32d577d666cd7bb8b2b5ba629d25ccf72a5ceb8a8da038906c84dcdb1fe677dffb2c029fd8926318eede1b58272af22bda5c5232be066839398e42f5352df58848adad11a1
Відкрита експонента	10001

Step 1: Підпишіть документ.

Аліса підписує юридичний документ і відправляє його Бобу з використанням відкритих і закритих ключів RSA, показаних в таблиці вище. Тепер Бобу доведеться перевірити цифровий підпис Аліси, щоб довіряти справжності електронного документа.



Step 2: Перевірте цифровий підпис.

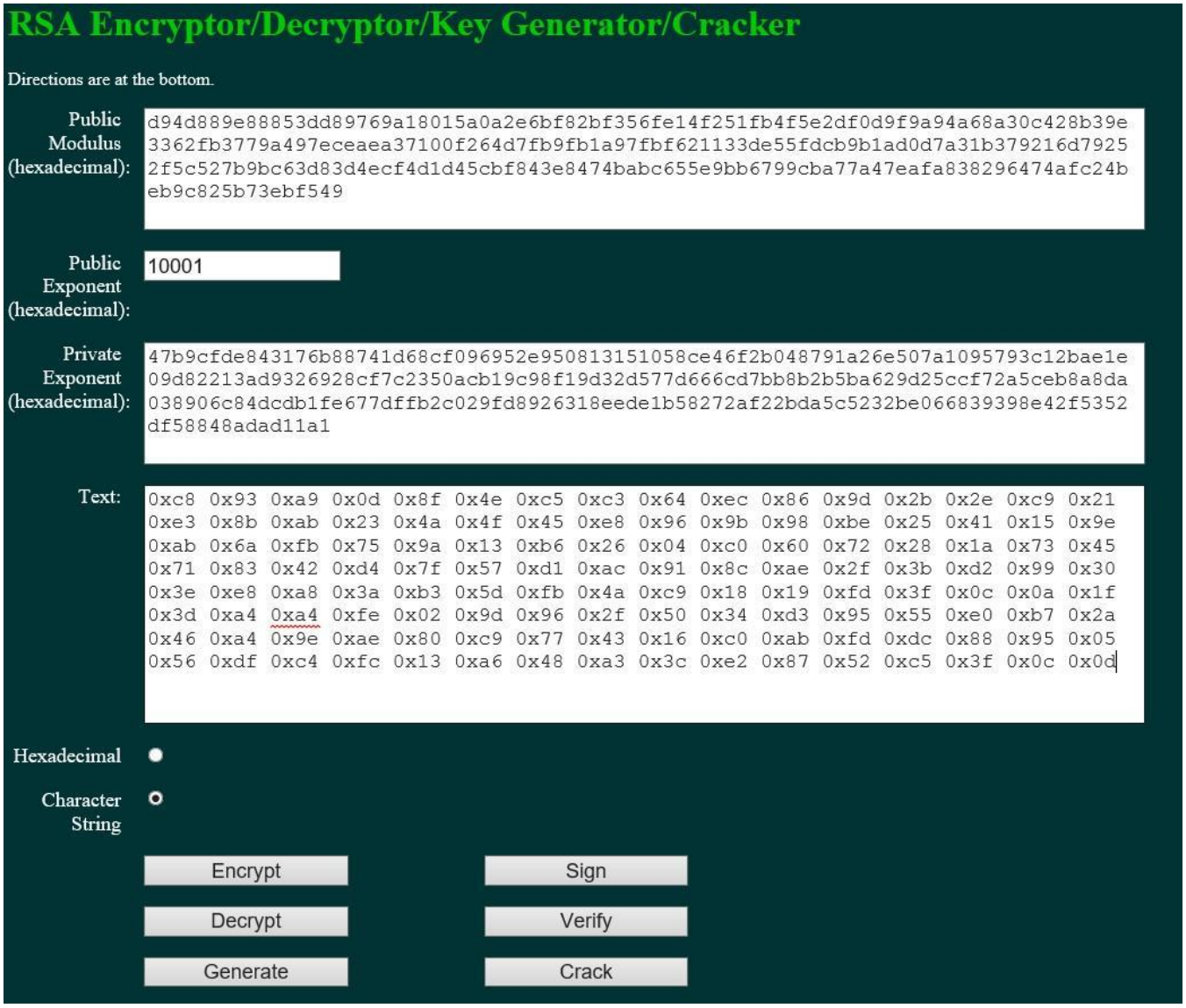
Боб отримує документ з цифровим підписом, показаним в таблиці нижче.

Таблиця 2 - Цифровий підпис Аліси

Цифровий підпис Аліси
0xc8 0x93 0xa9 0x0d 0x8f 0x4e 0xc5 0xc3 0x64 0xec 0x86 0x9d 0x2b 0x2e 0xc9 0x21 0xe3 0x8b 0xab 0x23 0x4a 0x4f 0x45 0xe8 0x96 0x9b 0x98 0xbe 0x25 0x41 0x15 0x9e 0xab 0x6a 0xfb 0x75 0x9a 0x13 0xb6 0x26 0x04 0xc0 0x60 0x72 0x28 0x1a 0x73 0x45 0x71 0x83 0x42 0xd4 0x7f 0x57 0xd1 0xac 0x91 0x8c 0xae 0x2f 0x3b 0xd2 0x99 0x30 0x3e 0xe8 0xa8 0x3a 0xb3 0x5d 0xfb 0x4a 0xc9 0x18 0x19 0xfd 0x3f 0x0c 0x0a 0x1f 0x3d 0xa4 0xa4 0xfe 0x02 0x9d 0x96 0x2f 0x50 0x34 0xd3 0x95 0x55 0xe0 0xb7 0x2a 0x46 0xa4 0x9e 0xae 0x80 0xc9 0x77 0x43 0x16 0xc0 0xab 0xfd 0xdc 0x88 0x95 0x05 0x56 0xdf 0xc4 0xfc 0x13 0xa6 0x48 0xa3 0x3c 0xe2 0x87 0x52 0xc5 0x3f 0x0c 0x0d

Натисніть тут, щоб використати онлайн-інструмент RSA для перевірки справжності цифрового підпису Аліси.

Таблиця 3 Онлайн інструмент цифрового підпису



a. Скопіюйте і вставте **відкриті** і **закриті** ключі з Таблиці 1 вище у поля **Public Modulus** і **Private Exponent** на сайті, як показано на рисунку вище.

b. Переконайтеся, що значення Public Exponent дорівнює 10001.

c. Вставте цифровий підпис Аліси з Таблиці 2 в поле з написом на веб-сайті, як показано вище.

d. Тепер Боб може перевірити цифровий підпис, натиснувши кнопку **Verify** знизу веб-сайту. Чий підпис ідентифіковано?

_____

Step 3: Створіть підпис для відповіді.

Боб отримує і перевіряє електронний документ і цифровий підпис Аліси. Тепер Боб створює електронний документ і генерує свій власний цифровий підпис, використовуючи закритий ключ RSA в Таблиці 1 (Примітка: ім'я Боба великими літерами).

-

Таблиця 4 Цифровий підпис Боба

Цифровий підпис Боба
0x6c 0x99 0xd6 0xa8 0x42 0x53 0xee 0xb5 0x2d 0x7f 0x0b 0x27 0x17 0xf1 0x1b 0x62 0x92 0x7f 0x92 0x6d 0x42 0xbd 0xc6 0xd5 0x3e 0x5c 0xe9 0xb5 0xd2 0x96 0xad 0x22 0x5d 0x18 0x64 0xf3 0x89 0x52 0x08 0x62 0xe2 0xa2 0x91 0x47 0x94 0xe8 0x75 0xce 0x02 0xf8 0xe9 0xf8 0x49 0x72 0x20 0x12 0xe2 0xac 0x99 0x25 0x9a 0x27 0xe0 0x99 0x38 0x54 0x54 0x93 0x06 0x97 0x71 0x69 0xb1 0xb6 0x24 0xed 0x1c 0x89 0x62 0x3d 0xd2 0xdf 0xda 0x7a 0x0b 0xd3 0x36 0x37 0xa3 0xcb 0x32 0xbb 0x1d 0x5e 0x13 0xbc 0xca 0x78 0x3e 0xe6 0xfc 0x5a 0x81 0x66 0x4e 0xa0 0x66 0xce 0xb3 0x1b 0x93 0x32 0x2c 0x91 0x4c 0x58 0xbf 0xff 0xd8 0x97 0x2f 0xa8 0x57 0xd7 0x49 0x93 0xb1 0x62

Боб посилає Алісі електронний документ і цифровий підпис.

Step 4: Перевірте цифровий підпис.

a. Скопіюйте і вставте **відкриті** і **закриті** ключі з Таблиці 1 вище у поля **Public Modulus** і **Private Exponent** на сайті, як показано на рисунку вище.

b. Переконайтеся, що значення Public Exponent дорівнює 10001.

c. Вставте цифровий підпис Боба з Таблиці 4 в поле з написом на веб-сайті, як показано вище.

d. Тепер Аліса може перевірити цифровий підпис, натиснувши кнопку **Verify** знизу веб-сайту. Чий підпис ідентифіковано?

_____

Part 2: Створіть свій власний цифровий підпис

Тепер, коли ви бачите, як працюють цифрові підписи, ви можете створити свій власний цифровий підпис.

Step 1: Створіть нову пару RSA-ключів.

Перейдіть на інструмент веб-сайту і створіть новий набір відкритих і закритих ключів RSA.

a. Видаліть вміст полів з написами **Public Modulus**, **Private Modulus** і **Text**. Просто використовуйте мишу, щоб виділити текст і натисніть клавішу delete на клавіатурі.

b. Переконайтеся, що поле «Public Exponent» має значення **10001**.

c. Створіть новий набір ключів RSA, натиснувши кнопку **Generate** в правому нижньому кутку вебсайту.

d. Скопіюйте нові ключі в Таблицю 5.

Таблиця 5 - Нові ключі RSA

Відкритий ключ	
Закритий ключ	

e. Тепер введіть своє повне ім'я в поле з написом **Text** і натисніть **Sign**.

Таблиця 6 Персональний цифровий підпис

Персональний цифровий підпис	

Part 3: Обміняйтеся і перевірте цифрові підписи

Тепер ви можете використовувати цей цифровий підпис.

Step 1: Обміняйтеся вашими новими відкритими і закритими ключами в Таблиці 5 з вашим партнером по лабораторній роботі.

a. Запишіть відкриті і закриті ключі RSA свого партнера з його Таблиці 5.

b. Запишіть обидва ключа в таблиці нижче.

Таблиця 7 - Ключі RSA партнера по лабораторній роботі

Відкритий ключ	
Закритий ключ	

c. Тепер обміняйтеся цифровими підписами з Таблиці 6. Запишіть цифровий підпис в таблиці нижче.

Цифровий підпис партнера по лабораторній роботі	

Step 2: Перевірте цифровий підпис партнера по лабораторній роботі

a. Щоб підтвердити цифровий підпис свого партнера, вставте його або її відкриті і закриті ключі до відповідних полів, помічених **Public and Private modulus** на веб-сайті.

b. Тепер вставте цифровий підпис в поле з написом **Text**.

c. Тепер перевірте його або її цифровий підпис, натиснувши кнопку verify.

d. Що відображається в текстовому полі?

_____