НАЦІОНАЛЬНИЙ ТЕХНІЧНИЙ УНІВЕРСИТЕТ УКРАЇНИ

«КИЇВСЬКИЙ ПОЛІТЕХНІЧНИЙ ІНСТИТУТ

імені Ігоря Сікорського»

Факультет прикладної математики

Кафедра прикладної математики

Звіт

з лабораторної роботи № 6

із дисципліни «Криптографічні методи захисту інформації»

на тему

*Хеш-функції та їх застосування в електронних цифрових підписах*

|  |  |
| --- | --- |
| Виконав: | Керівник: |
| студент групи КМ-ХХ | *ст. викладач Бай Ю. П.* |
| *Іваненко І. І.* |  |

Київ — 20\_\_

ЗМІСТ

[Постановка завдань і хід виконання лабораторної роботи 3](#_Toc58564390)

[Відповіді 4](#_Toc58564391)

[Список літератури 5](#_Toc58564392)

[Додаток 1 6](#_Toc58564393)

***Мета роботи:*** засвоїти *поняття хеш-функції, властивості хеш-функцій, електронний цифровий підпис, алгоритми створення та перевірки ЕЦП*. Отримати практичні навички роботи з найбільш використовуваними на практиці хеш-функціями, отримати практичний досвід створення електронного цифрового підпису з використанням алгоритму RSA, опанувати бібліотеку *rsa* для Python.

# Постановка завдань і хід виконання лабораторної роботи

1. Дати визначення хеш-функцій і навести властивості ідеальної хеш-функції. Дати визначення колізії хеш-функції.

2. Обчислити значення хеш-функцій від заданих вхідних даних, заповнити *Таблицю 1*.

3. Створити файл *zayava.docx* від власного імені, записати Прізвище Ім’я По-батькові. Обчислити *sha1* від вмісту даного файлу, записати в *Таблицю 1.*

4. Навести теоретичні відомості з електронного цифрового підпису. Навести схему створення та верифікації ЕЦП за допомогою асиметричних алгоритмів. Створити електронний цифровий підпис до власного файлу *zayava.docx,* використовуючи алгоритм RSA та бібліотеку *rsa* для Python:

4.1. Встановити бібліотеку *rsa*:

python -m pip install rsa

pip install --upgrade rsa

4.2. Згенерувати секретний (private) і відкритий (public) ключі для алгоритму RSA – для цього необхідно один раз виконати файл ***genkeys.py.***

4.3. Записати секретний і відкритий ключі(згенеровані ключі знаходяться у файлах *private\_key\_1024.pem, public\_key\_1024.pem*) ***display\_key.py***

4.4. Приєднати **метадані** до хеш-коду від вхідного файлу. Зашифрувати одержаний результат, користуючись функцією *rsa.encrypt().* Налаштувати і запустити на виконання файл ***hash\_sign.py****.* Цифровий підпис буде записано в файл ***zayava.docx.sgn****.* Заповнити *Таблицю 2.*

4.5. Передати одержувачу документ *zayava.docx,*  цифровий підпис до нього − *zayava.docx.sgn* тапублічний ключ.

5. Імітувати дії одержувача, верифікувати цифровий підпис (див. файл ***verify\_signature.py***).

6. Створити і верифікувати цифровий підпис до документу *zayava.docx* **без метаданих**, користуючись вбудованими функціями бібліотеки rsa: *rsa.sign(), rsa.verify().* Якщо ЕЦП до файлу вірний, то функція *rsa.verify()* повертає тип хеш-функції, яка використовувалась при хешуванні вхідного файлу.

# Відповіді

1.

…..

2. Визначення дайджестів (хеш-кодів) від рядків та вмісту файлу.

*Таблиця 1*

|  |  |  |  |
| --- | --- | --- | --- |
| № | Вхідні дані, *M* | *hash* | Результат,  *h(M)* |
| 1 | *‘Hello, world!’* | sha1 |  |
| 2 | *‘12345’* | sha1 |  |
| 3 | *‘12346’* | sha1 |  |
| 4 | *‘’* | sha1 |  |
| 5 | *‘Іваненко І. І.’ (власні ПІБ)* | md5 |  |
| 6 | *‘Іваненко І. І.’* | sha1 |  |
| 7 | *‘Іваненко І. І.’* | sha224 |  |
| 8 | *‘Іваненко І. І.’* | sha256 |  |
| 9 | *‘Іваненко І. І.’* | sha512 |  |
| 10 | *zayava.docx* | sha1 |  |

3. Див. рядок 10 в *Таблиці 1*.

4. Основні відомості з електронного цифрового підпису.

……

Схема створення ЕЦП з використанням асиметричних алгоритмів.

……

4.3. Генерація ключів.

а) ключі довжиною 16 біт

*Private Key: n = ; e = ; d = ; p = ; q = .*

*Public Key: n = ; e = .*

б) ключі довжиною 1024 біт

*Private Key: n = ; e = ; d = ; p = ; q = .*

*Public Key: n = ; e = .*

4.4. Метадані до файлу *zayava.docx* та цифровий підпис:

*Таблиця 2*

|  |  |  |
| --- | --- | --- |
| 1 | Ім’я файлу |  |
| 2 | Розмір файлу |  |
| 3 | Дата підписання |  |
| 4 | Хеш-код вмісту файлу |  |
| 5 | Цифровий підпис |  |

5. Скріншот перевірки цифрового підпису (дії одержувача)

# Список літератури

1. Тарнавський Ю.А. Технології захисту інформації [Електронний ресурс] / Ю. А. Тарнавський. – Київ: КПІ ім. Ігоря Сікорського, 2018. – 162 с.
2. Шнайер Б. Прикладная криптография: Протоколы, алгоритмы, исходные тексты на языке Си / Б. Шнайер. – М.: Диалектика, 2003. – 610 с.
3. Алферов А.П., Зубов А.Ю., Кузьмин А.С., Черемушкин А.В. Основы криптографии. – М.: Гелиос АРВ, 2001. – 480 с.
4. Столлингс В. Криптография и защита сетей: принципы и практика, 2-е изд.: Пер. с англ. – М.: «Вильямс», 2001. – 672 с.
5. Menezes A.J., Van Oorschot P.C., Vanstone S.A. Handbook of Applied Cryptography. – CRC Press, Inc., 1997. – 795 p.

# Додаток 1

**Скріншоти виконання файлів**

Результат виконання файлу hash.py:

Результат виконання файлу hash\_sign.py:

Результат перевірки підпису: