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-81 | *ст. викладач Бай Ю. П.* |
| *Верзун П.В.* |  |

Київ — 2020

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*)

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. **Хеш-функція** — функція, що перетворює вхідні дані будь-якого (як правило великого) розміру в дані фіксованого розміру.

* *Незворотність* : для заданого значення геш-функції *m* має бути обчислювально неможливо знайти блок даних X, для якого H(X)=m.
* Стійкість *колізіям першого роду* : для заданого повідомлення *M* має бути обчислювально неможливо підібрати інше повідомлення *N* , для якого H(N)=H(M).
* Стійкість до *колізій другого роду* : має бути обчислювально неможливо підібрати пару повідомлень (M, M`), що мають однаковий геш.
* Оборотна функція нестійка до колізій першого і другого роду.
* Функція, нестійка до колізій першого роду, нестійка до колізій другого роду; зворотне невірно.

**Колізією хеш-функції**  називаються два *різних* вхідних блоки даних x і у таких, що H(x)=H(y)

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

*Таблиця 1*

|  |  |  |  |
| --- | --- | --- | --- |
| № | Вхідні дані, *M* | *hash* | Результат,  *h(M)* |
| 1 | *‘Hello, world!’* | sha1 | 943a702d06f34599aee1f8da8ef9f7296031d699 |
| 2 | *‘12345’* | sha1 | 8cb2237d0679ca88db6464eac60da96345513964 |
| 3 | *‘12346’* | sha1 | 94ae0a96d83a445d72a93417b63ac90d79db5eca |
| 4 | *‘’* | sha1 | da39a3ee5e6b4b0d3255bfef95601890afd80709 |
| 5 | *Verzun P.V.* | md5 | 2dce785339b101dd3e549febeaadcccd |
| 6 | *Verzun P.V.* | sha1 | de7f572a0e61eceedb56f24537e8f11e78198969 |
| 7 | *Verzun P.V.* | sha224 | 2463f4ba99b3991fe7e695bcaabbf92f1a783c3c72d4229a1102a875 |
| 8 | *Verzun P.V.* | sha256 | 9fe3a2d3b1a7a51bf2099cb226dbe8d063a1dece776d9311efa2b8e4d926b439 |
| 9 | *Verzun P.V.* | sha512 | 2c9b6c7931cad985a4d437716ad13b620580fb7efb58000e25b0bca0f84f37eb48951e98eaca6b8137c3a27fa63ba9f937a9dd0a93a43dcfe1178c864a610fe8 |
| 10 | *zayava.docx* | sha1 | a78d44b969d6dc529dd6f4c0a9ed007460c78e65 |

3. Див. рядок 10 в *Таблиці 1*.

4. Основні відомості з електронного цифрового підпису.

Електронний цифровий підпис (ЕЦП) - потужний засіб контролю достовірності інформації в електронному вигляді, забезпечення цілісності електронних даних, підтвердження їх авторства і актуальності.  Електронний цифровий підпис - це інформаційний об'єкт, що створюється для підписуваних даних, дозволяє упевнитися в цілісності і автентичності цих даних.

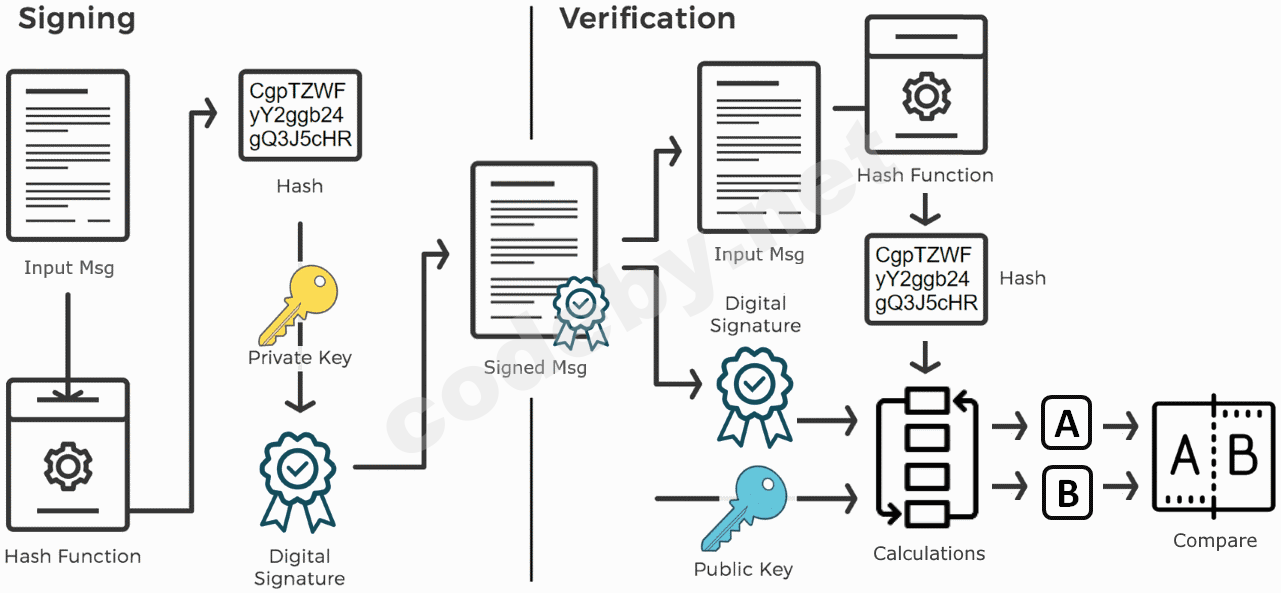
Електронний цифровий підпис за правовим статусом прирівнюється до власноручного підпису (печатки) у разі, якщо:

-  електронний цифровий підпис підтверджено з використанням посиленого сертифіката ключа за допомогою надійних засобів електронного цифрового підпису;

-  під час перевірки використовувався посилений сертифікат ключа, чинний на момент накладення електронного цифрового підпису;

-  особистий ключ підписувача відповідає відкритому ключу, зазначеному у сертифікаті.

Схема створення ЕЦП з використанням асиметричних алгоритмів.



4.3. Генерація ключів.

а) ключі довжиною 16 біт

-----BEGIN RSA PRIVATE KEY-----

MCMCAQACAwCfEwIDAQABAgIWAQICANMCAgDBAgIArQIBQQIBUg==

-----END RSA PRIVATE KEY-----

-----BEGIN RSA PUBLIC KEY-----

MAoCAwCfEwIDAQAB

-----END RSA PUBLIC KEY-----

б) ключі довжиною 1024 біт

-----BEGIN RSA PRIVATE KEY-----

MIICYQIBAAKBgQCHF0EOo9P5zKhzetMoEMbA+qqoCTaWMd6yICEfLqxflvMNl/RX

v6kEaZO9yIyFCPh5SGBQR39g6SAaVrCiMiAxBdjeLGuEYPbtaz5SOAn8eMGKUQF+

L8oJAY8joIOYueAssooc2lR06Ay7XDPhU7TPTUkqrnYPSWHzNQtgVofOrQIDAQAB

AoGAArRUeRaOh9GxDZ7H22V6lSJviC2nChq1eptqDlXA3akH9J22JouPtqbmbkY1

ifREBSmNxA2qXyZLnjteCNbsLQ6t5yYvetvwygLYnhvu+79/njAwZzZ8obb24vDg

/YswCiy3w5z1g7ihfr1tq0v0heRIZe/3qGCph9luJDvC7AECRQD7w+D51OEYsNV2

WtiXfb8Da6AUUMtupIP9jcGlAWUqWB1xOQep7ixq+CvKdkk6Ej2yXpEQoF9a6P1y

zqdYCfTuHO75OQI9AIlc91udBfXBbDNVuHmucXKxPWFTsG/YjFCbwuDUkglWbN2b

Mk6N/J0Q+2sweCyAFxxyRUiOGk8Y4MlFFQJFAOj62Ct5gyBdK/yNjxeJhwT8SLPk

HI1z8qzlzIgMpXis9/n5w4zOWg5XP/boxVTW4n84odeYAQXYzAm9EQEYna7n2YGJ

Ajx+hU6g54Sx07KhpfcAvRhpl679kmQU4NR8+rsI80J/r0ce5u/zQvzGfvnUxRQr

iN/Ap9ABAEJjUHrbZ/ECRQD5Ityjk079YoHCDyYUHssdvT+8F3jEtM9MnNl0SAQQ

SJ7CxqjR9ppwdwSMdWMvOGCrultR5wrKqk7n92C++Wtr5d8ZNw==

-----END RSA PRIVATE KEY-----

-----BEGIN RSA PUBLIC KEY-----

MIGJAoGBAIcXQQ6j0/nMqHN60ygQxsD6qqgJNpYx3rIgIR8urF+W8w2X9Fe/qQRp

k73IjIUI+HlIYFBHf2DpIBpWsKIyIDEF2N4sa4Rg9u1rPlI4Cfx4wYpRAX4vygkB

jyOgg5i54CyyihzaVHToDLtcM+FTtM9NSSqudg9JYfM1C2BWh86tAgMBAAE=

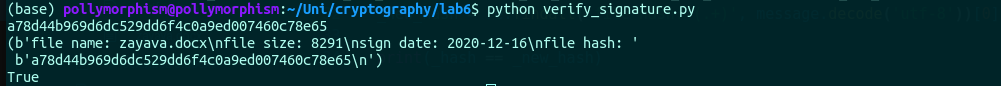
-----END RSA PUBLIC KEY-----

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

*Таблиця 2*

|  |  |  |
| --- | --- | --- |
| 1 | Ім’я файлу | zayava.docx |
| 2 | Розмір файлу | 8291 |
| 3 | Дата підписання | 2020-12-16 |
| 4 | Хеш-код вмісту файлу | a78d44b969d6dc529dd6f4c0a9ed007460c78e65 |
| 5 | Цифровий підпис | b'\x0f\xd6\xc2\xee\x16\xcd+\xac\xa6\x02\xd4\x03\xed\xfe@y<&<\x95\*{\x9aqk\xe7\x94\xfd\xa5\xf5\x04\xbbj\xbfhX7\xc1=\xb3\xa5TV\*\x05\xae\x98\x8a\xc2o\x93\xd7\xc3\xcb\x12!x\x93\xf1\xc5\xbaR\xf1\x0ca\x06S\xad\xc8\xf3?\xaf\xb9\x9a\xc2 \xc6\xfe \x16J\xd8\xcf\xa0\xfe\xe3\xde4\xd0\xeaS\x0c\xc0%\xc9YL\xa3\xd3\xe0\x9e=BR\xec\x05!i\x8a\x16k\xd4\xb2(\x18\xcaFW\xb8\xb26\xda\x1b\xa0\x0e\x18\x1a$' |

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, pезультат виконання файлу hash\_sign.py, Результат перевірки підпису:

