**Міністерство освіти та науки України**

**Державний торговельно-економічний університет**

***Кафедра інженерії програмного забезпечення та кібербезпеки***

**ЗВІТ**

***З ЛАБОРАТОРНОЇ РОБОТИ № 10***

*з дисципліни*

**«ОСНОВИ КІБЕРБЕЗПЕКИ»**

**НА ТЕМУ:**

ВИКОРИСТАННЯ ЦИФРОВИХ ПІДПИСІВ

(назва теми)

**Виконала:** студентка факультету інформаційних технологій

Групи 4 курсу 3

Авєріна Наталія Ігорівна

**Викладач:** Ковальова Людмила Ігорівна

Київ 2024

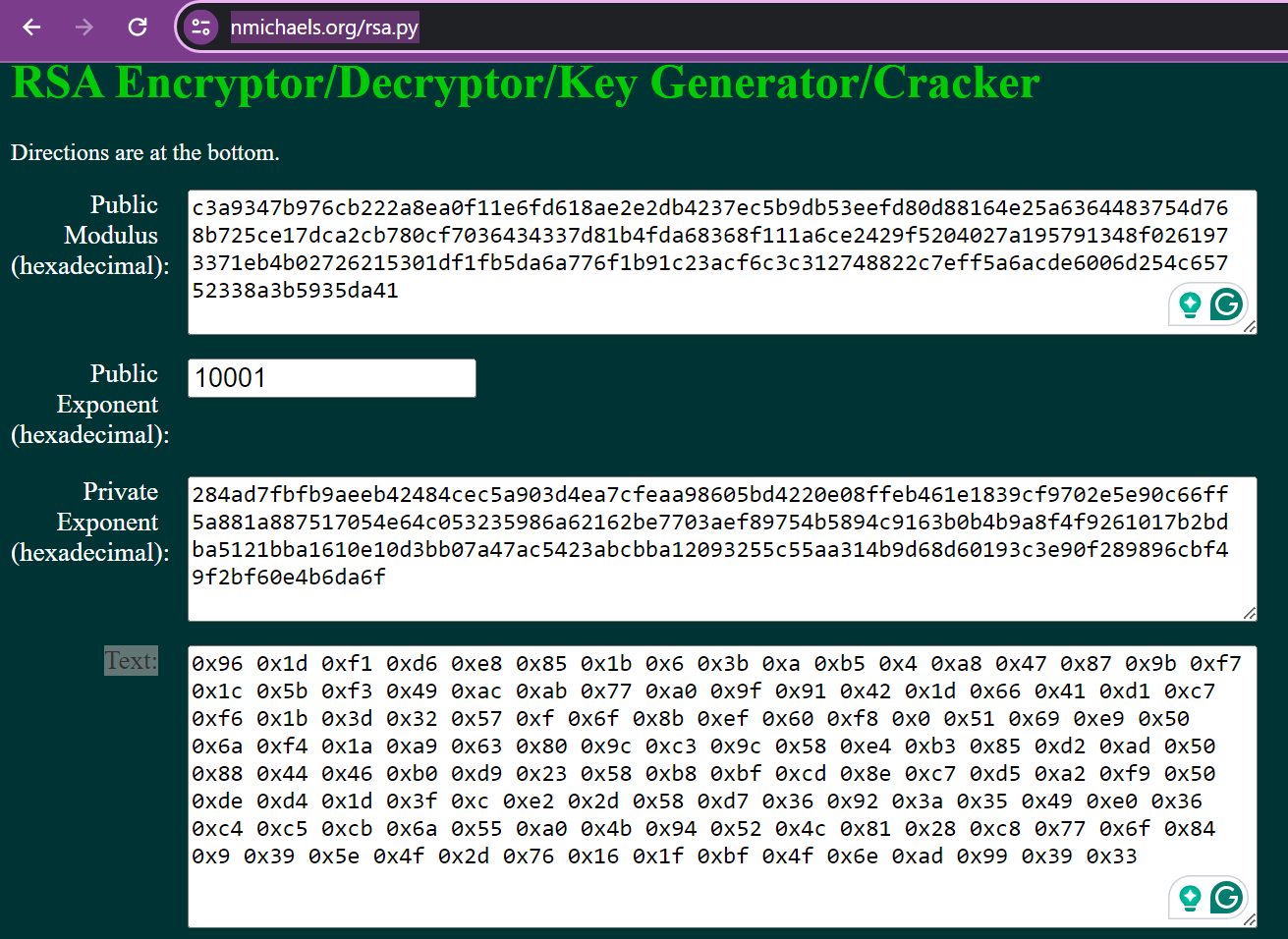
**Лабораторна робота №10**

**Тема:** Використання цифрових підписів

**Цілі та задачі:** Зрозуміти концепції цифрового підпису.

**Хід роботи:**

1. Створення нової пари RSA-ключів.
   1. За допомогою інструменту <https://www.nmichaels.org/rsa.py> створюємо новий набір ключів RSA, натиснувши кнопку Generate.
   2. Вводимо в поле Text повне ім’я (Авєріна Наталія Ігорівна) та натискаємо на Sign.

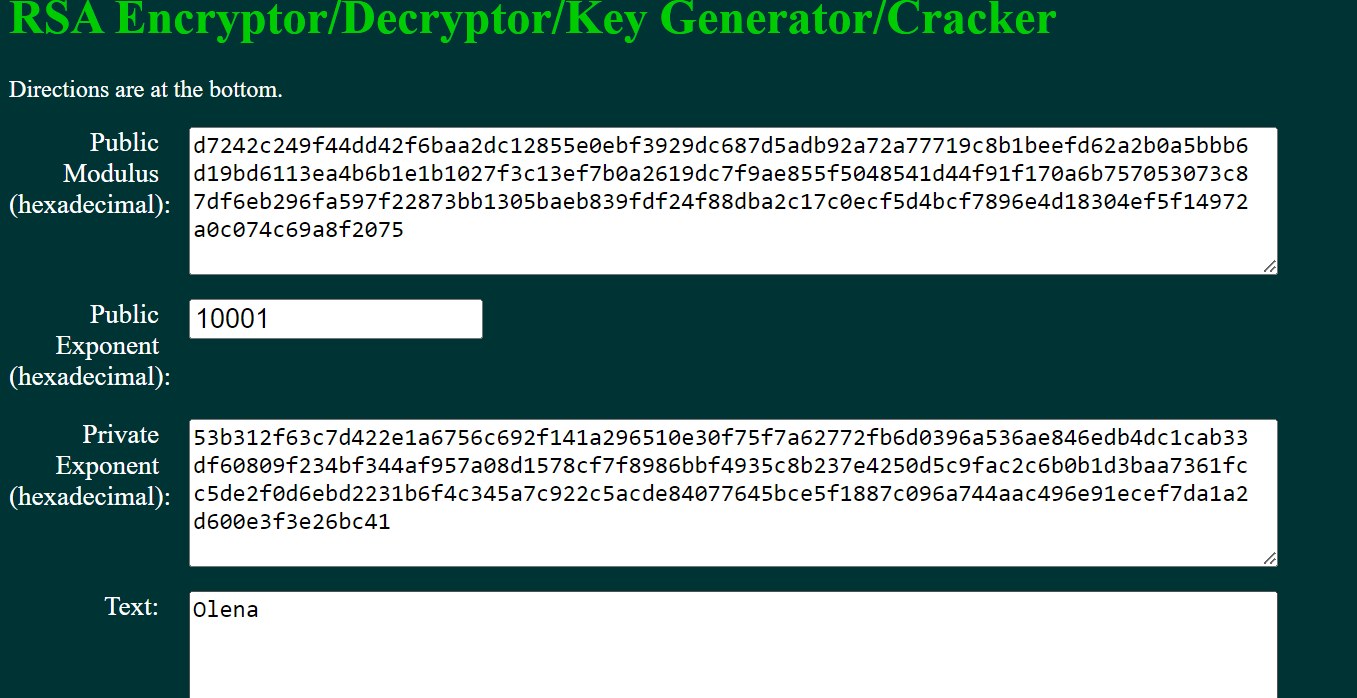


|  |  |
| --- | --- |
| Відкритий ключ | c3a9347b976cb222a8ea0f11e6fd618ae2e2db4237ec5b9db53eefd80d88164e25a6364483754d768b725ce17dca2cb780cf7036434337d81b4fda68368f111a6ce2429f5204027a195791348f0261973371eb4b02726215301df1fb5da6a776f1b91c23acf6c3c312748822c7eff5a6acde6006d254c65752338a3b5935da41 |
| Закритий ключ | 284ad7fbfb9aeeb42484cec5a903d4ea7cfeaa98605bd4220e08ffeb461e1839cf9702e5e90c66ff5a881a887517054e64c053235986a62162be7703aef89754b5894c9163b0b4b9a8f4f9261017b2bdba5121bba1610e10d3bb07a47ac5423abcbba12093255c55aa314b9d68d60193c3e90f289896cbf49f2bf60e4b6da6f |
| Персональний цифровий підпис | 0x96 0x1d 0xf1 0xd6 0xe8 0x85 0x1b 0x6 0x3b 0xa 0xb5 0x4 0xa8 0x47 0x87 0x9b 0xf7 0x1c 0x5b 0xf3 0x49 0xac 0xab 0x77 0xa0 0x9f 0x91 0x42 0x1d 0x66 0x41 0xd1 0xc7 0xf6 0x1b 0x3d 0x32 0x57 0xf 0x6f 0x8b 0xef 0x60 0xf8 0x0 0x51 0x69 0xe9 0x50 0x6a 0xf4 0x1a 0xa9 0x63 0x80 0x9c 0xc3 0x9c 0x58 0xe4 0xb3 0x85 0xd2 0xad 0x50 0x88 0x44 0x46 0xb0 0xd9 0x23 0x58 0xb8 0xbf 0xcd 0x8e 0xc7 0xd5 0xa2 0xf9 0x50 0xde 0xd4 0x1d 0x3f 0xc 0xe2 0x2d 0x58 0xd7 0x36 0x92 0x3a 0x35 0x49 0xe0 0x36 0xc4 0xc5 0xcb 0x6a 0x55 0xa0 0x4b 0x94 0x52 0x4c 0x81 0x28 0xc8 0x77 0x6f 0x84 0x9 0x39 0x5e 0x4f 0x2d 0x76 0x16 0x1f 0xbf 0x4f 0x6e 0xad 0x99 0x39 0x33 |

1. Обмін цифровими підписами з партнером по лабораторній роботі.
   1. Моїм партнером по лабораторній роботі є Лимар Олена. Вона згенерувала свої відкриті і закриті ключі та створила цифровий підпис.

|  |  |
| --- | --- |
| Відкритий ключ | d7242c249f44dd42f6baa2dc12855e0ebf3929dc687d5adb92a72a77719c8b1beefd62a2b0a5bbb6d19bd6113ea4b6b1e1b1027f3c13ef7b0a2619dc7f9ae855f5048541d44f91f170a6b757053073c87df6eb296fa597f22873bb1305baeb839fdf24f88dba2c17c0ecf5d4bcf7896e4d18304ef5f14972a0c074c69a8f2075 |
| Закритий ключ | 53b312f63c7d422e1a6756c692f141a296510e30f75f7a62772fb6d0396a536ae846edb4dc1cab33df60809f234bf344af957a08d1578cf7f8986bbf4935c8b237e4250d5c9fac2c6b0b1d3baa7361fcc5de2f0d6ebd2231b6f4c345a7c922c5acde84077645bce5f1887c096a744aac496e91ecef7da1a2d600e3f3e26bc41 |
| Персональний цифровий підпис | 0x6d 0xb3 0x81 0x60 0x37 0x8e 0x66 0x3a 0x8f 0x61 0xe4 0xac 0xd6 0x62 0x26 0x98 0xd5 0x64 0x39 0x2 0x5 0x1e 0xff 0xb3 0xfe 0xf8 0x32 0x47 0x10 0x34 0x2d 0x42 0x93 0x90 0x52 0x92 0x16 0xbb 0xcc 0xcf 0x98 0xf 0x49 0xff 0xfd 0xef 0x18 0x13 0x2d 0xe 0xaf 0xd6 0x89 0xc7 0xe1 0xd4 0x9 0xe1 0x7a 0x90 0xc 0xb 0x61 0x9b 0xe0 0x3c 0x32 0x33 0xe3 0x55 0x4a 0xae 0xb7 0x6b 0x61 0x86 0xcc 0xd1 0x13 0x65 0xae 0xfe 0xa2 0xbc 0xb 0xe6 0x24 0x15 0x33 0x13 0xb1 0x60 0x5c 0x3c 0x48 0xee 0x49 0xa7 0x18 0xdf 0xf6 0x11 0x81 0x11 0x5f 0x53 0x13 0xb 0x1a 0x8d 0x62 0xef 0x8a 0xf2 0xe7 0xfa 0x5c 0xd0 0x39 0x3e 0xc9 0xbe 0x71 0x5 0xf6 0xf0 0xf5 0x56 |

* 1. Перевіримо цифровий підпис. Для цього вставляємо в інструмент, який ми використали вище, ключі та цифровий підпис. Натискаємо кнопку Verify.



* 1. В текстовому полі відображається ім’я Olena, отже електронний підпис був створений успішно.

**Висновок**: в ході виконання лабораторної роботи було вивчено концепцію цифрового підпису, створено його та перевірено з партнером по лабораторній роботі.