МІНІСТЕРСТВО ОСВІТИ ТА НАУКИ УКРАЇНИ

НАЦІОНАЛЬНИЙ АВІАЦІЙНИЙ УНІВЕРСИТЕТ

Факультет кібербезпеки комп’ютерної та програмної інженерії

Кафедра безпеки інформаційних технологій

**Технології забезпечення конфіденційності і цілісності інформаційних ресурсів**

**Лабораторна робота №6**

Тема: Алгоритм електронного цифрового підпису RSA

Тривалість заняття: 90 хв.

Київ 2023

**Тема:** Алгоритм електронного цифрового підпису RSA

**Мета:** Ознайомитись з принципом роботи алгоритму електронного цифрового підпису RSA. Навчитись застосовувати цей алгоритм.

**Теоретичні відомості**

RSA (абревіатура від прізвищ Rivest, Shamir та Adleman) — криптографічний алгоритм з відкритим ключем, що базується на обчислювальній складності задачі факторизації великих цілих чисел.

RSA став першим алгоритмом такого типу, придатним і для шифрування, і для цифрового підпису. Алгоритм застосовується до великої кількості криптографічних застосунків.

Це асиметричний алгоритм шифрування, який названий на честь Рона Ріввеста, Аді Шаміра та Лена Адлемана, які його винайшли (Rivest, Shamir, Adleman). Перша публікація про алгоритм RSA датується 1977 роком.

Наразі криптосистема RSA є найпоширенішим криптографічним алгоритмом з відкритим ключем у світі, що використовується майже в усіх інтернет-транзакціях для захисту конфіденційних даних. Даний алгоритм можна використовувати як для шифрування, так і для цифрових підписів.

Безпека RSA залежить від обчислювальної складності розкладання великих цілих чисел на прості множники, тому міцність шифрування безпосередньо пов’язана з розміром ключа. Зі збільшенням обчислювальної потужності та відкриттям ефективніших алгоритмів розкладання на множники — зростає й здатність розкладати на множники все більші й більші числа.

Алгоритм RSA складається з чотирьох етапів: 1) генерація ключа; 2) розподіл ключа; 3) шифрування; 4) дешифрування.

1. Генерація ключа. Даний етап, своєю чергою, ділиться ще на декілька підетапів:

Вибір двох простих чисел. На даному етапі необхідно обрати два великі прості числа p та q (просте число — це таке, що може ділитись без залишку лише на 1 та на себе). Числа p і q повинні триматись в таємниці, оскільки саме на них базується процес створення приватного та публічного ключа. Для більшої надійності p та q повинні: бути обрані навмання; бути великими; мати велику різницю.

Визначення модуля. На даному етапі необхідно визначити число n, що використовується як модуль для відкритого і закритого ключа: n = p \* q. Довжина n, що виражена в бітах, і є довжиною ключа.

Застосування функції Ейлера. Далі необхідно визначити значення функції Ейлера від числа n, що має наступний вигляд: φ(n) = (p — 1) \* (q — 1).

Вибір відкритої експоненти. Після визначення значення функції Ейлера необхідно випадково обрати ціле число e таке, що 2 < e < φ(n). Число e (яке також називають відкритою експонентою) повинно бути взаємно простим до значення φ(n). Занадто малі значення відкритої експоненти можуть послабити алгоритм RSA.

Знаходження приватної експоненти (оберненого за модулем числа). В той час, коли відкрита експонента e є частиною публічного ключа, то приватна експонента d (або ж секретна) являється частиною приватного ключа. Приватна експонента d знаходиться як обернене за модулем φ(n) до числа e, тобто: d \* e ≡ 1(mod(φ(n)). Значення оберненого за модулем числа можна визначити з допомогою розширеного алгоритму Евкліда.

2. Розподіл ключа. Тепер, коли визначено всі необхідні числа, можна сформувати приватний та публічний ключ. Приватний ключ складається з пари d та n, а публічний з пари e та n.

Число d повинно триматись у таємниці, оскільки воно використовується для дешифрування повідомлення. Числа p, q та φ(n) також повинні триматись у таємниці, адже з допомогою них можна визначити приватну експоненту d, але після її визначення ці числа можна одразу відкинути.

Публічний ключ пересилається з допомогою надійного, але не обов’язково зашифрованого каналу зв’язку.

3. Шифрування. Для того, щоб зашифрувати текст m, необхідно обчислити таку рівність: c = (mod n), де c — зашифрований текст, m — простий текст.

4. Дешифрування. Для того, щоб розшифрувати текст c, необхідно обчислити таку рівність: m = (mod n).

**Приклад роботи алгоритму**

Алгоритм шифрування:

Обираємо пару простих чисел p та q:

P = 19, q = 23

Рахуємо n = p\*q = 19\*23 = 437

Знаходимо

Обираємо ціле e, таке жо 1 < e < та e – взаємно просте з . e = 13;

Знаходимо d = = 61.

В результаті отримаємо пару ключів для шифрування (e,n) та дешифрування (d,n):

OpenKey = (13,437), SecretKey = (61,437);

Виконуємо шифрування за алгоритмом RSA:

Відкритий текст = 21;

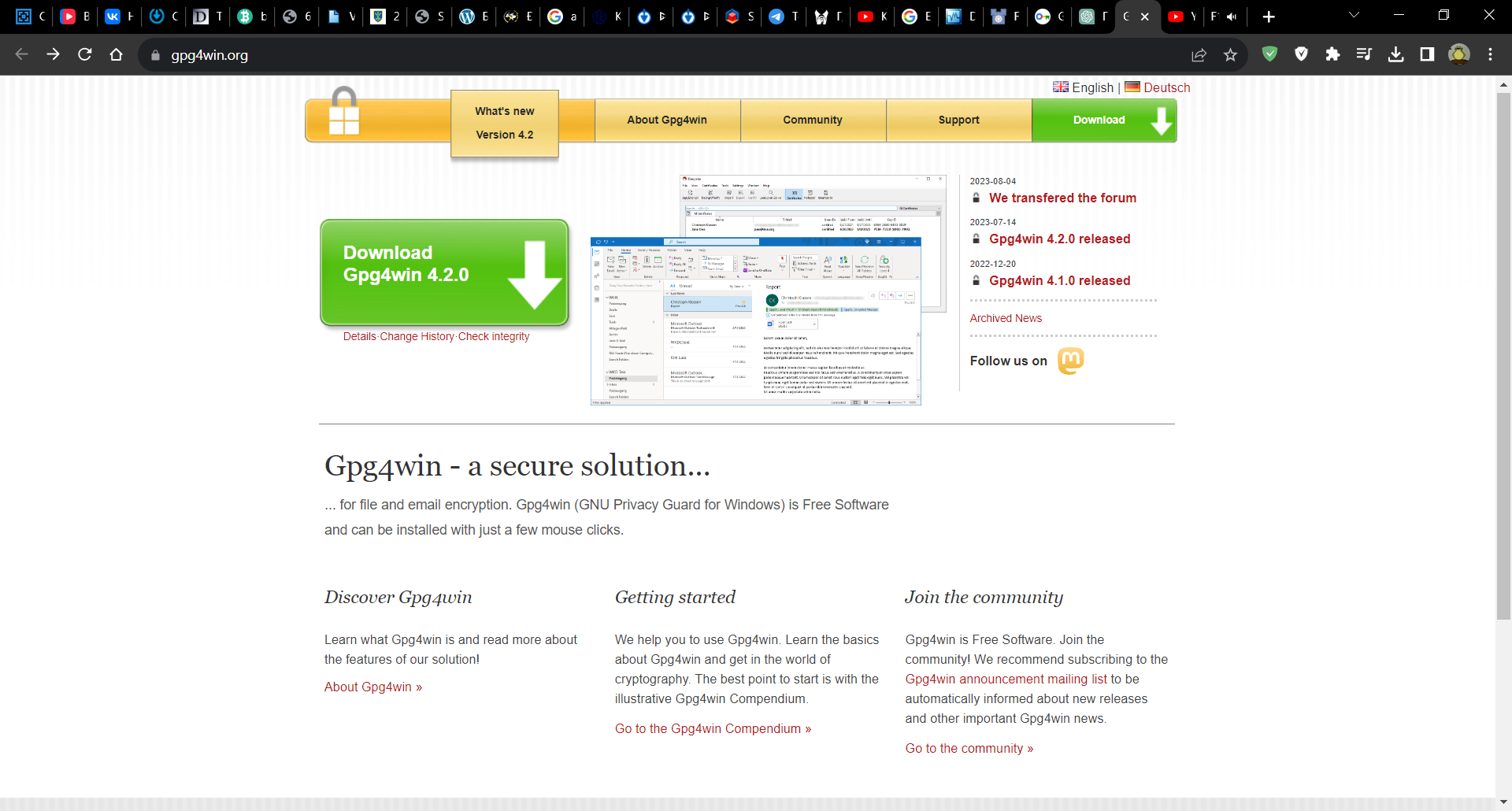
Шифротекст = mod 437 = 364;

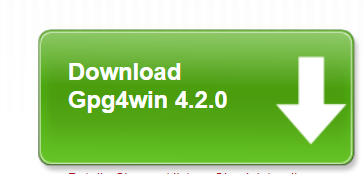
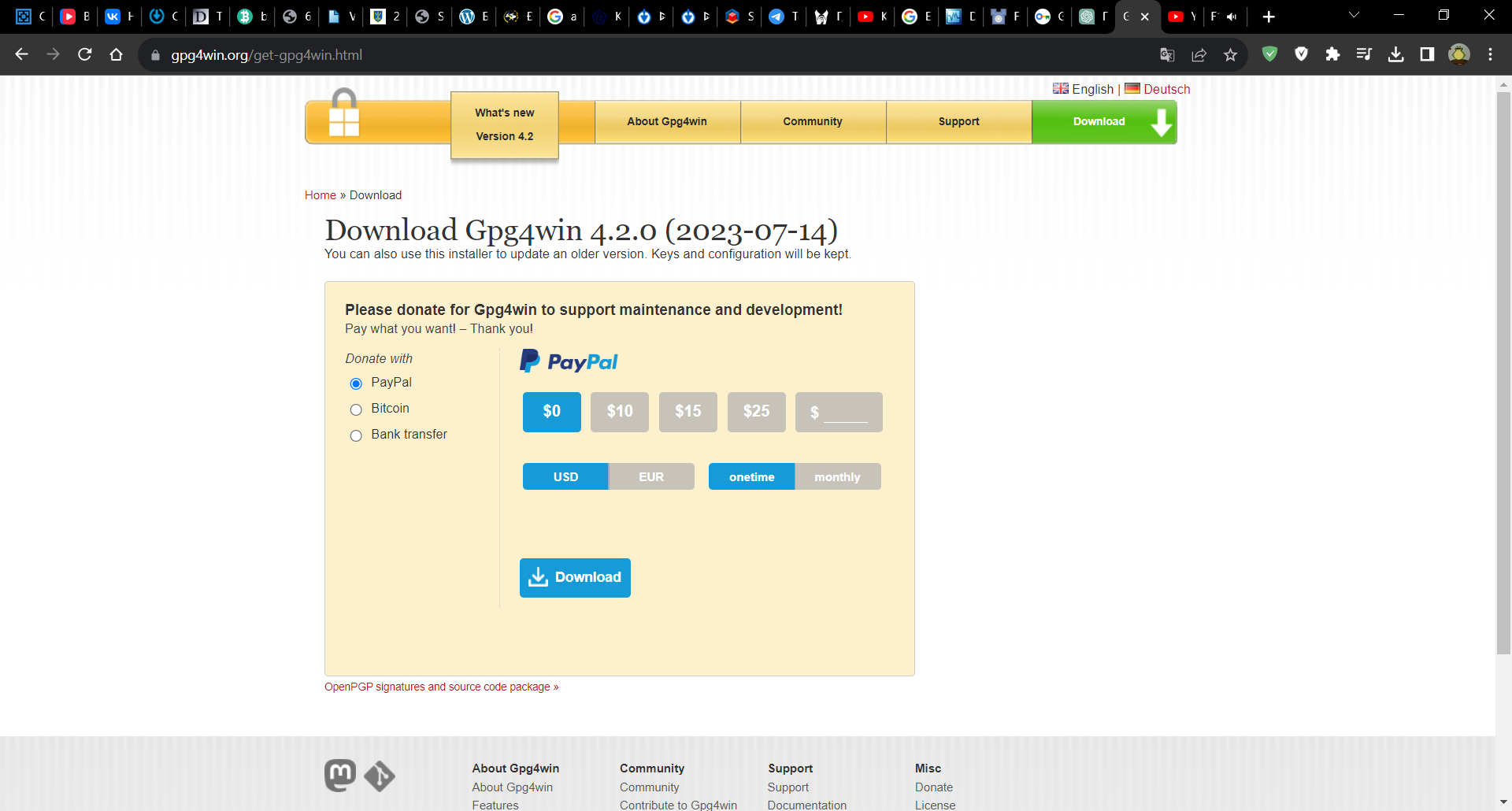
Дешифруємо текст з допомогою закритого ключа:

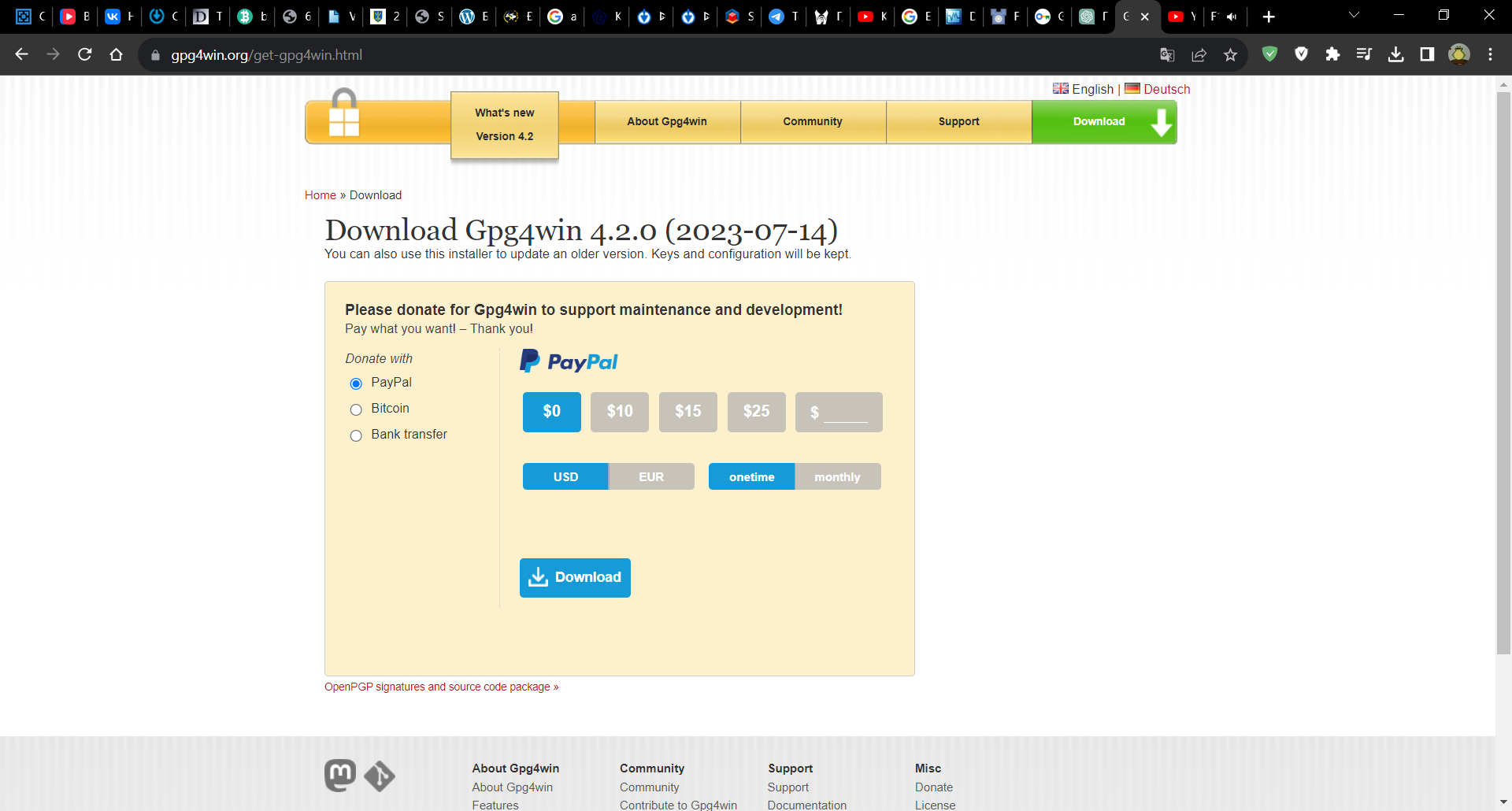
Дешифрований текст = mod437 = 21;

**Завдання**

1. Ознайомтесь з теоретичними відомостями.
2. Перейдіть за посиланням та перегляньте відеоролик <https://www.youtube.com/watch?v=jKRmyafuoAI&list=PLEeeVYx0ZR3zCxFdKTelJuT_fankSUl06&index=13>
3. Обрахуйте самі вручну алгоритм цифрового підпису RSA, з такими вхідними даними p = 3557, q = 2579, e = 3, відкритий текст = 111111
4. Розробити блок-схему для алгоритму RSA.
5. Вам потрібно перейти за посиланням <https://gpg4win.org/>

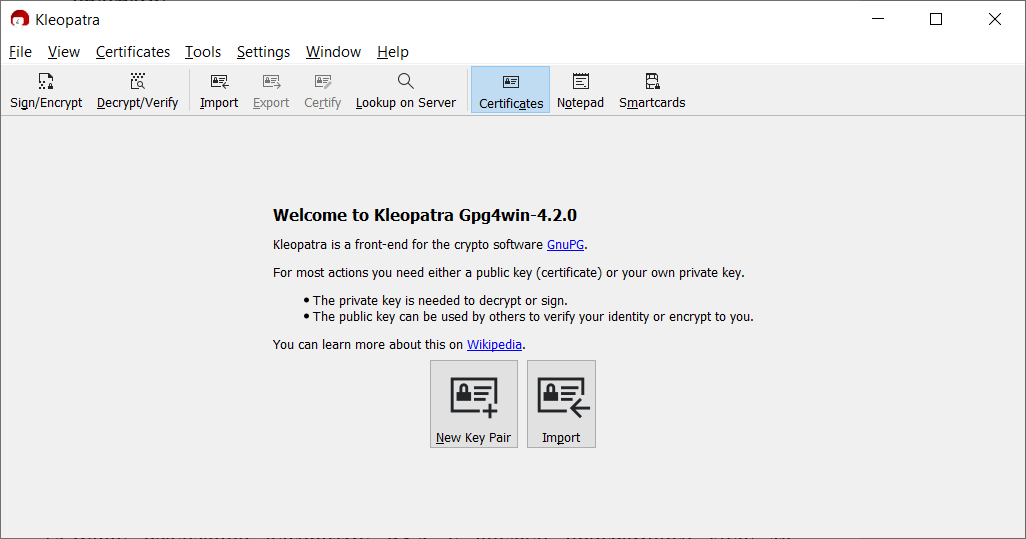


1. Натиснути на велику зелену кнопку Download Gpg4win 4.2.0 
2. На відкритій сторінці виставити такі самі значення як на малюнку 
3. Натиснути синю кнопку Download, далі файл скачається

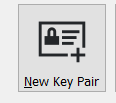


1. На скачаний файл потрібно натиснути два рази для того щоб почати встановлення програми.
2. Для встановлення програми вам потрібно слідувати інструкціям з майстра установки.
3. Після встановлення програми на ваш комп’ютер, натисніть двічі на піктограму встановленої вами піктограми, для того щоб відкрити програму.

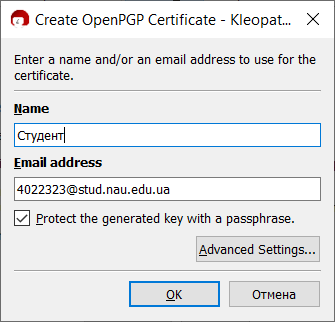




1. Після відкриття програми натисніть кнопку New key pair



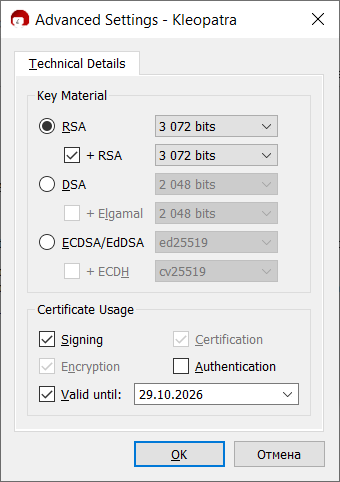
1. У вікні яке було відкрите після натискання кнопки введіть своє ім’я та свою електронну адресу ( якщо у вас немає електронної адреси, то вам потрібно її створити)



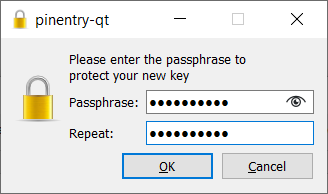
1. Далі натисніть кнопку Advanced Settings



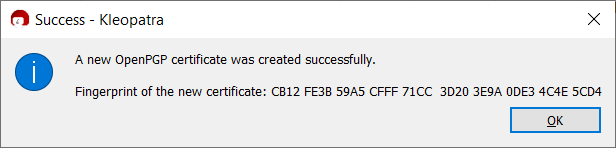
1. Вам потрібно виставити такі параметри як на рисунку, після чого натиснути кнопку ОК.



1. Після чого знову натиснути кнопку ОК
2. У вікні яке відкрилось введіть парольну фразу (має містити 8 символів, та хоча б одну цифру) якою буде захищено ваш новий ключ, та натисніть кнопку ОК

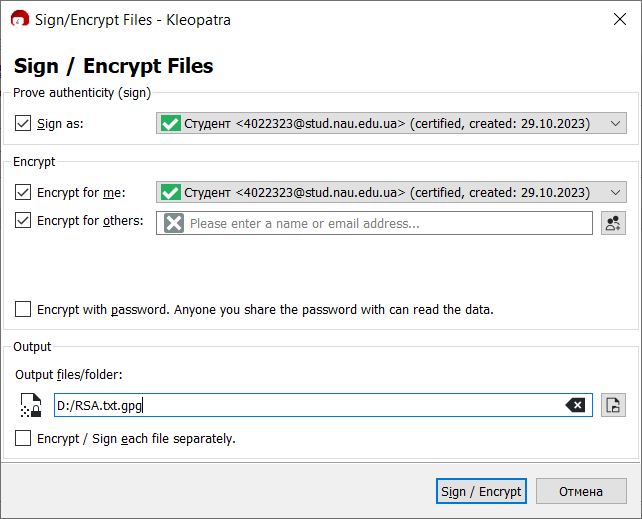


1. Далі у вас має відкритись таке вікно як на малюнку, натисніть кнопку ОК

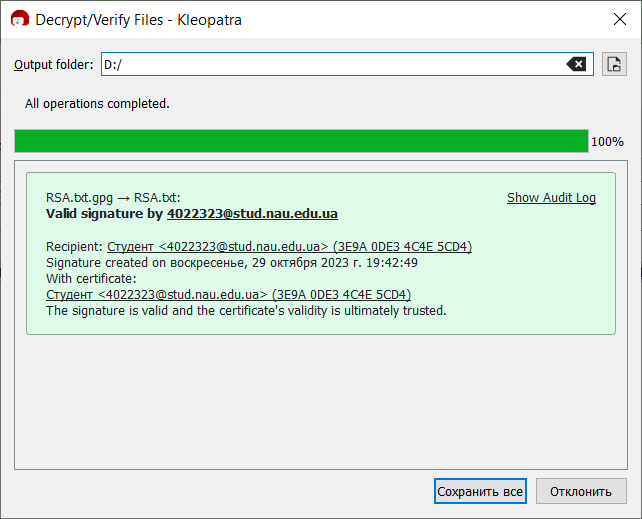


1. Ваш закритий ключ зберігається за таким посиланням "C:\Users\Ваше\_ім’я\_користувача\AppData\Roaming\gnupg\private-keys-v1.d" і має наступний вигляд (це ПРИКЛАД того як можу виглядати ваш закритий ключ ) lQHYBFWsdjYBBADZk0SJ/YrHM9UEVqrwN/awvHvSygtbyVBfXVtfxNp04PkJiWBs.key
2. Створіть новий документ в блокноті з наступним текстом « Я ім’я\_фамілія, студент номер\_групи використовую алгоритм цифрового підпису RSA ». Збережіть цей документ під назвою RSA.txt
3. В програмі Kleopatra, натисніть кнопку Sign/Encrypt, виберіть створений вами файл з назвою RSA, у відкритому вікні вам потрібно виставити галочку навпроти:





1. Натисніть копку  для того щоб підписати та зашифрувати файл.
2. Далі вам потрібно буде ввести свою парольну фразу, яка була створена вами в пункті 17. Після чого в місці куди ви вибрали зберегти зашифрований файл, ви можете знайти файл який було зашифровано за допомогою алгоритму цифрового підпису RSA. Спробуйте відкрити зашифрований вами файл.
3. На наступному етапі, видаліть файл з назвою RSA.txt, який було створено вами в пункті 19.
4. В програмі натисніть кнопку  для того аби розшифрувати зашифрований раніше файл. Виберіть свій зашифрований файл, він називається RSA.txt.gpg. Далі натисніть кнопку зберегти все, розшифрований файл буде збережено в вибрану вами папку.



1. Відкрийте збережений(розшифрований) файл (ви його розшифрували в попередньому пункті), перегляньте текст в цьому файлі.
2. Зроблену вами роботу у вигляді опису з скріншотами занести до звіту.
3. Дати відповіді на контрольні питання.
4. Зробити висновки та занести їх до звіту.

**Контрольні питання**

1. Що представляє собою алгоритм RSA?
2. Зі скількох етапів складається алгоритм?
3. Опишіть етапи роботи цього алгоритму.
4. В якому році було опубліковано опис RSA алгоритму?