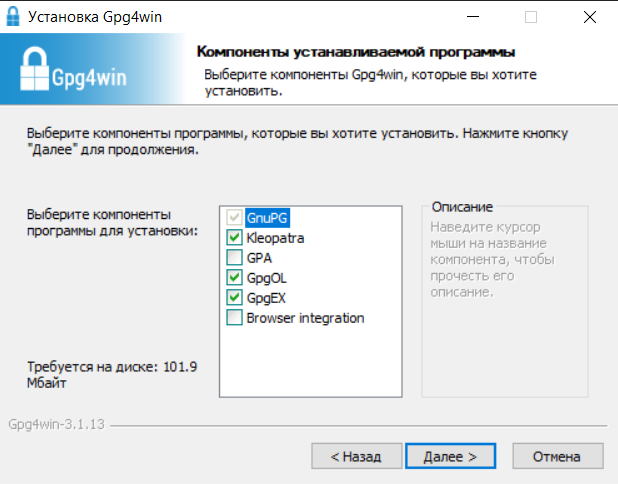
**Бужак Андрій Васильович, 541м**

**Лабораторна робота №1**

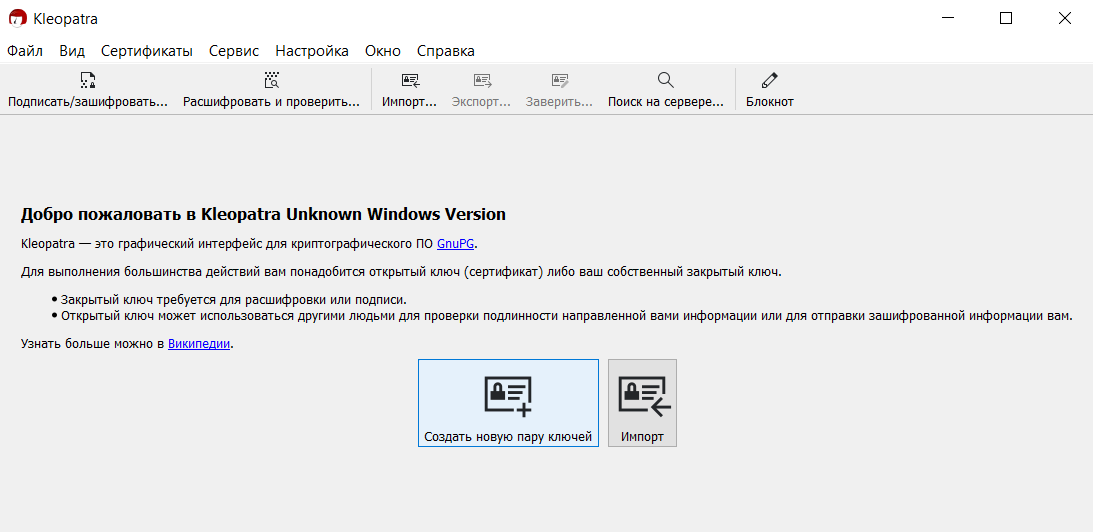
**«Вивчення системи захисту інформації GnuPG та Kleopatra»**

***Хід роботи***

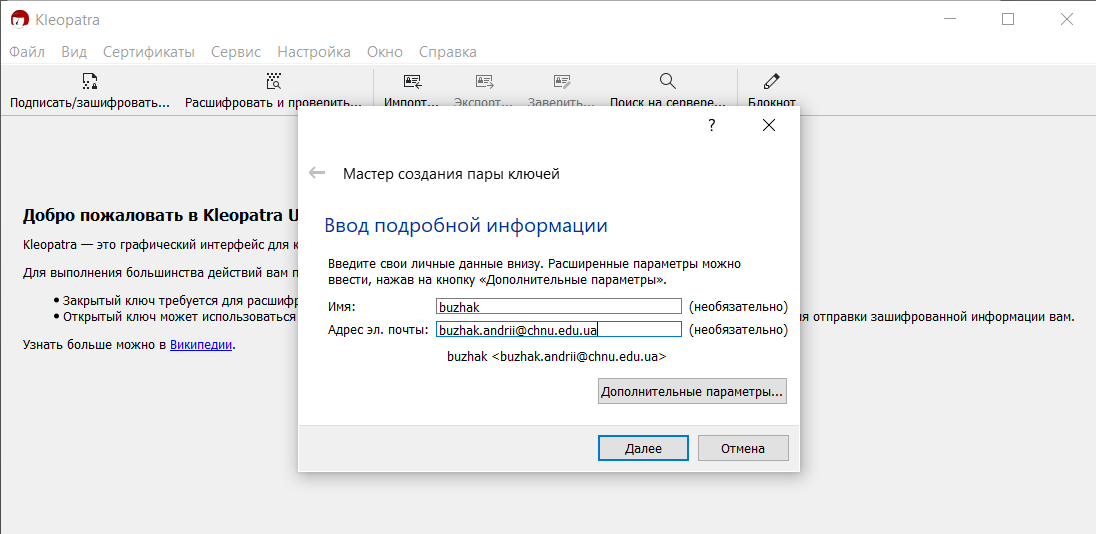
1. Скачаємо потрібні пакети з вказаних на початку методички ресурсів та встановимо Kleopatra разом з GnuPG на своєму комп'ютері.

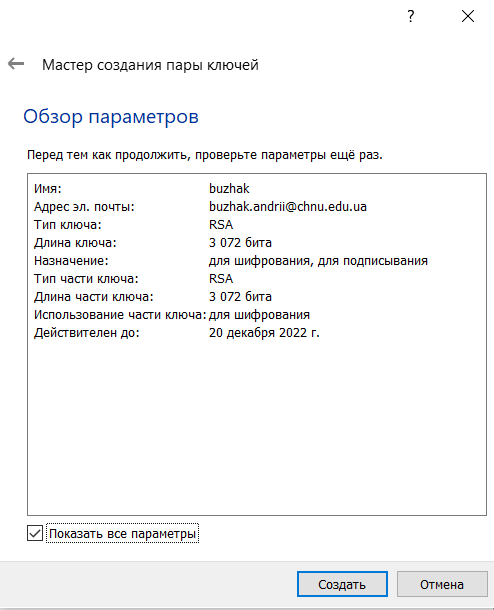
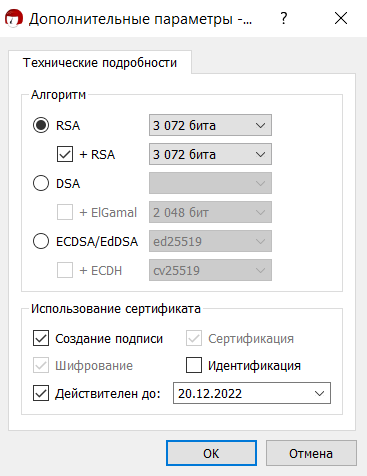


2. Запустимо Kleopatra та згенеруємо пару ключів для шифрування та окрему пару ключів для ЕЦП. Алгоритми та параметри – довільні.

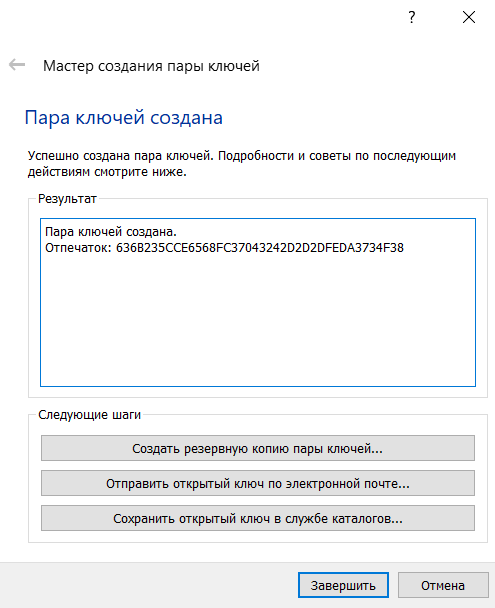


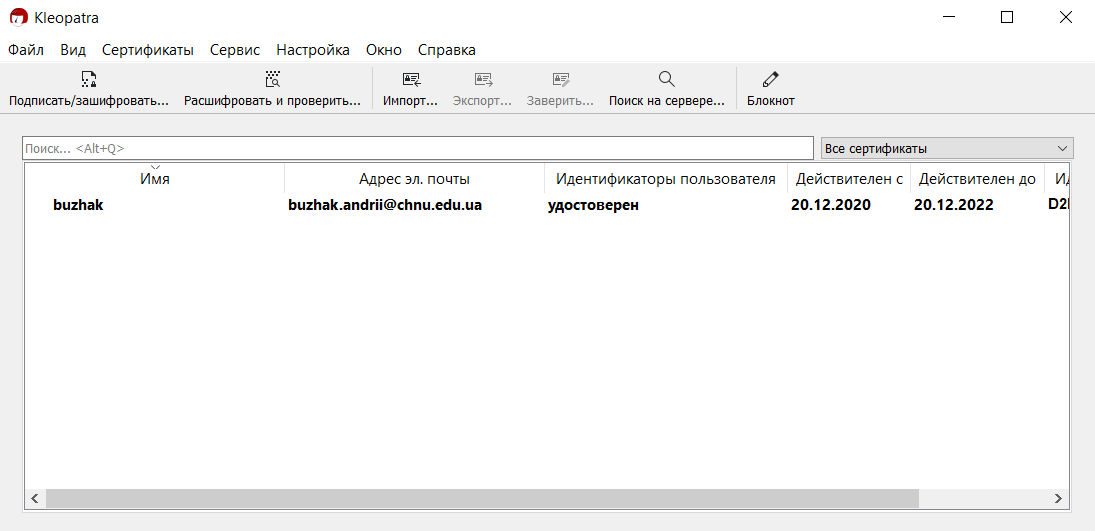
Задамо основні та додаткові параметри





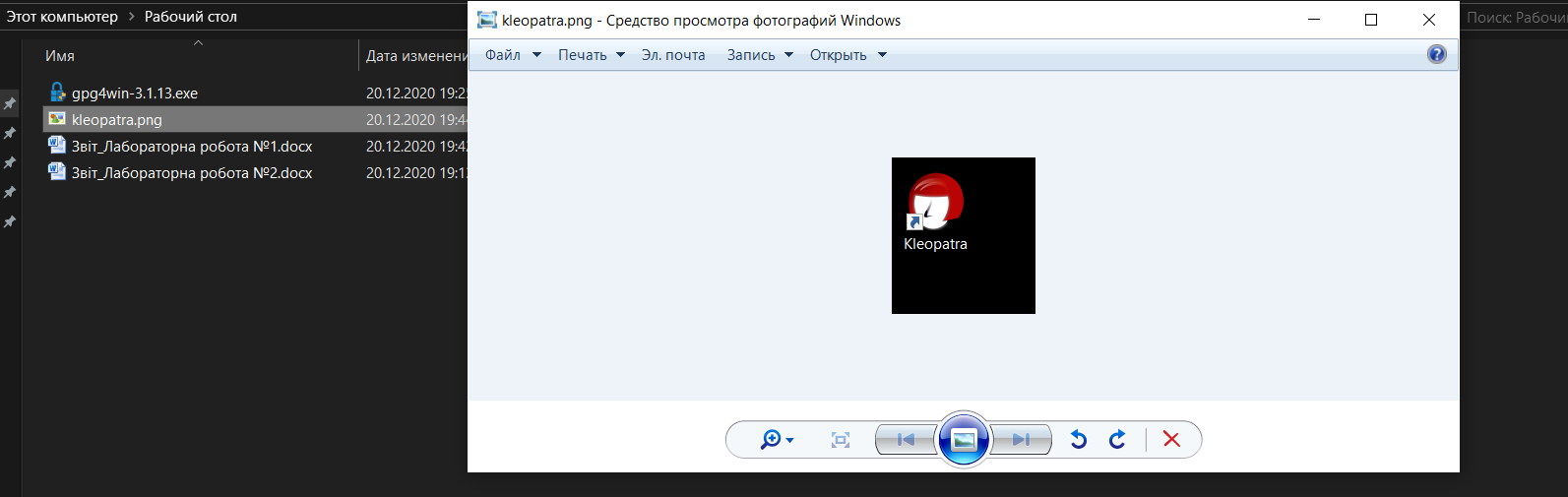
Переглянемо новостворену пару ключів



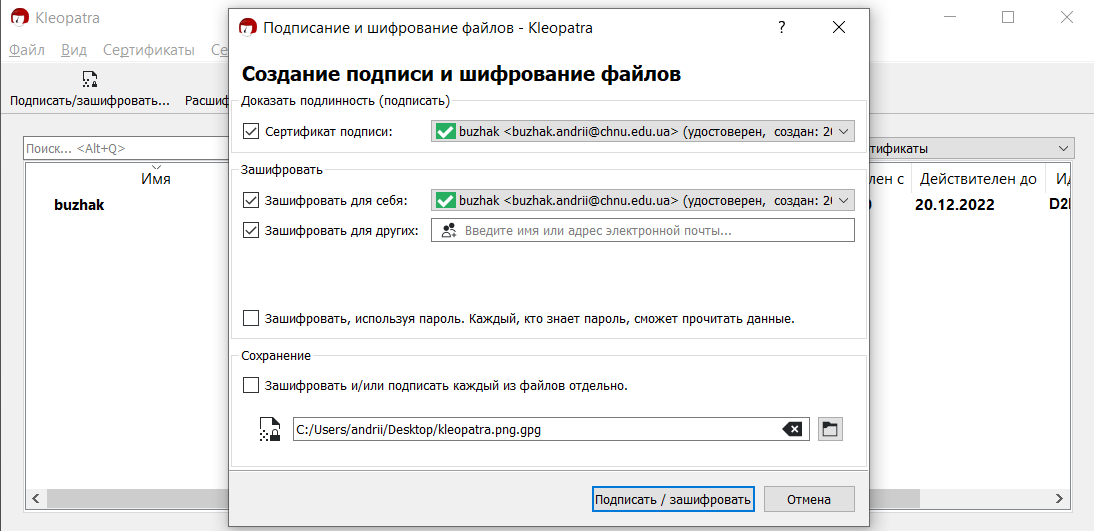


3. Виконайте шифрування/розшифрування файлів та перевірте, що розшифрований файл ідентичний оригінальному. Зробіть висновок про коректність операцій шифруванні/розшифрування

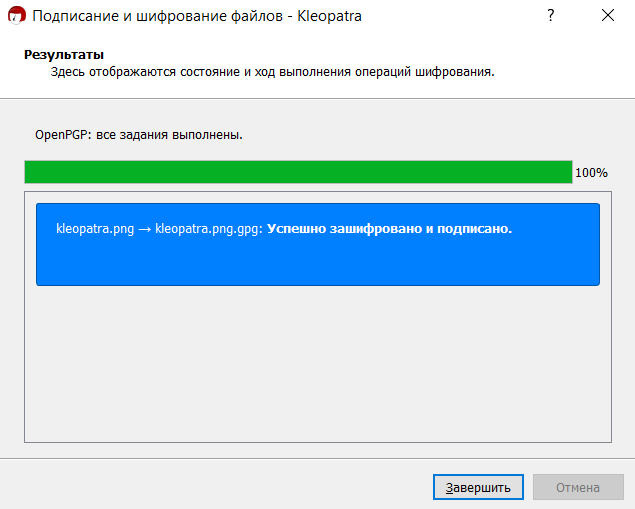
Маємо файл-картинку для шифрування

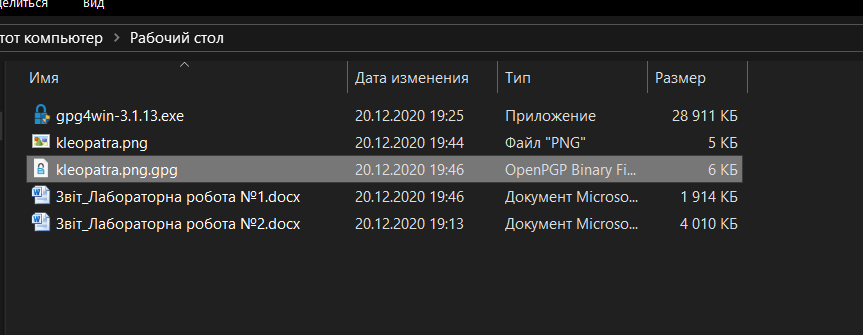


Проводимо шифрування



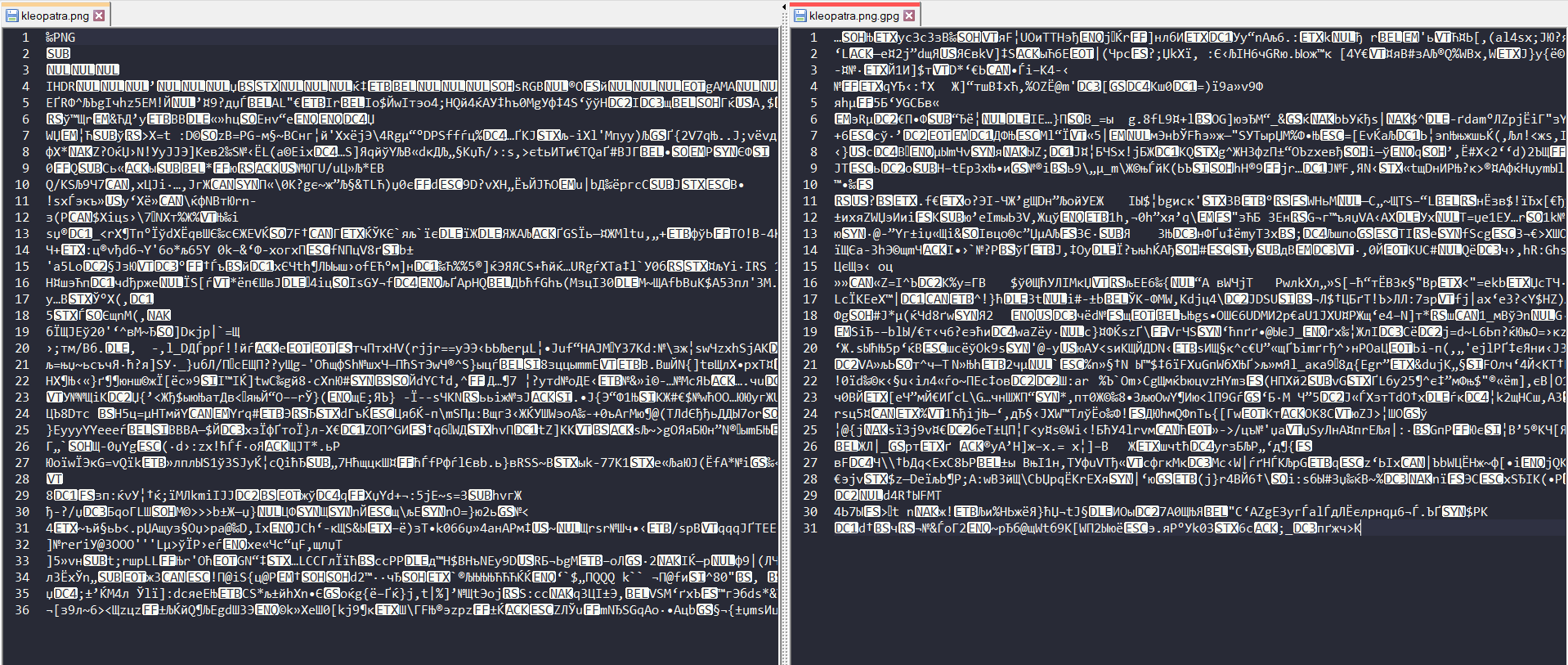
Отримали зашифрований файл



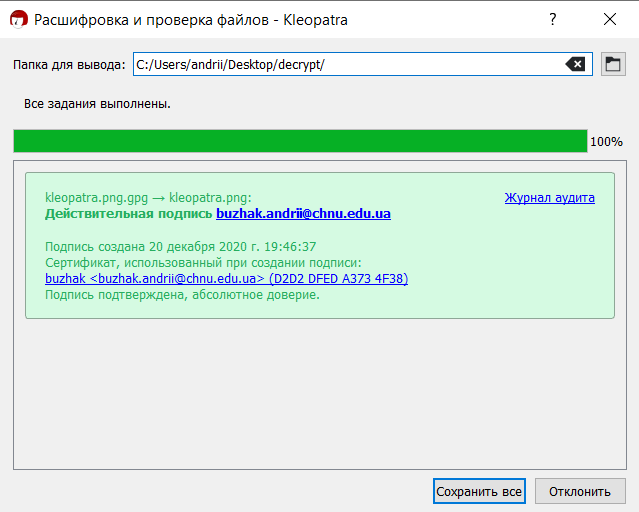


Переглянемо вміст через текстовий редактор

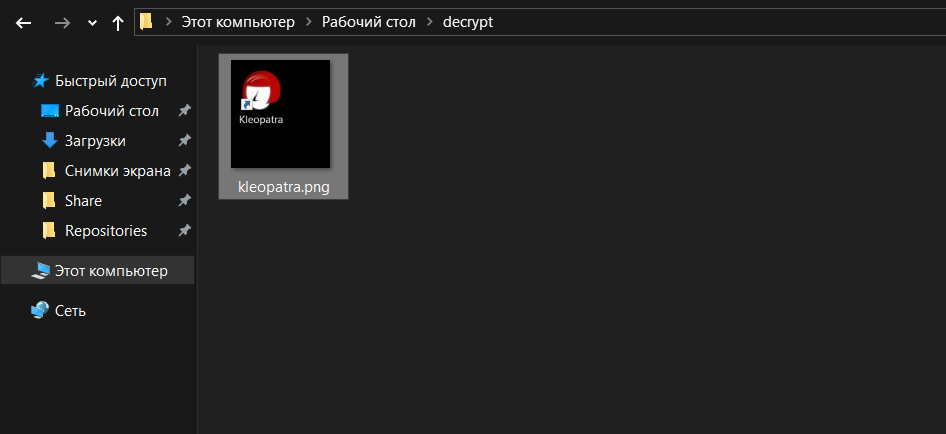
Як бачимо на рисунку, файл зберігся в спеціальному форматі і дійсно є зашифрованим.



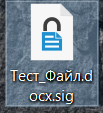
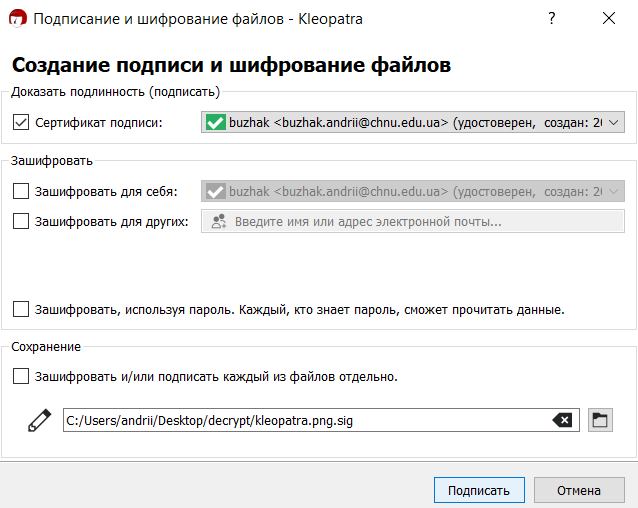
Проведемо розшифрування файлу в окрему папку та переглянемо його вміст після вказаної процедури



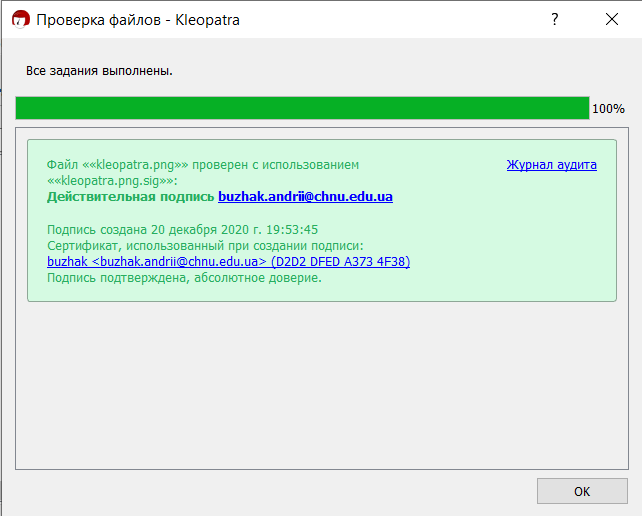
Як бачимо, вміст документу є ідентичний оригінальному. Отже, операції шифруванні/розшифрування за допомогою Kleopatra є коректними.



4. Підпишемо документи за допомогою ключів підпису та перевіримо коректність процедури підпису.



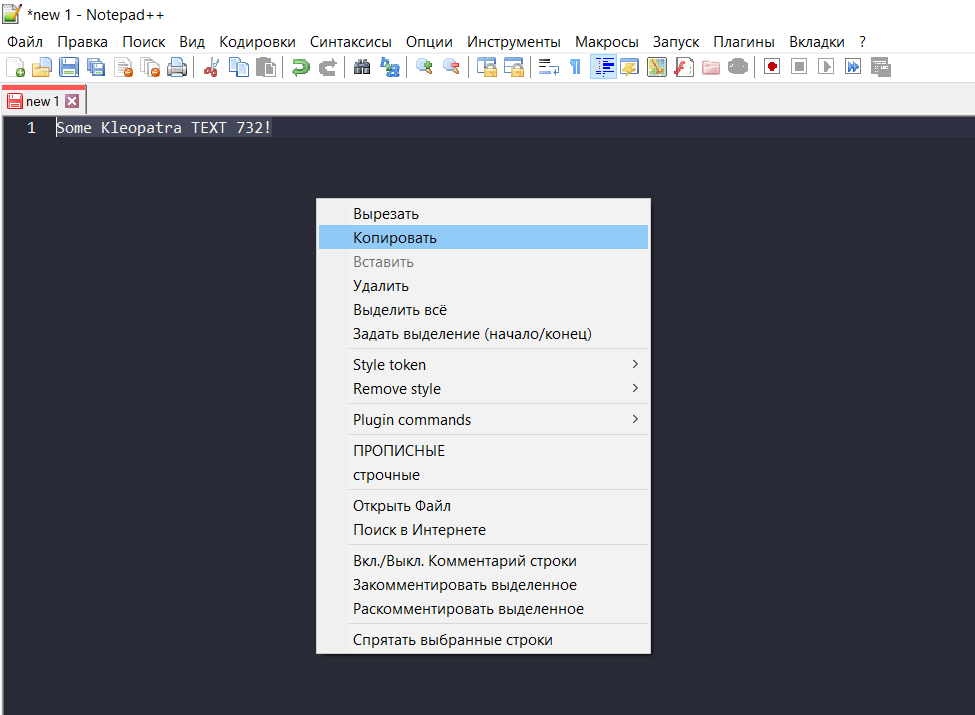
Перевіримо коректність підпису



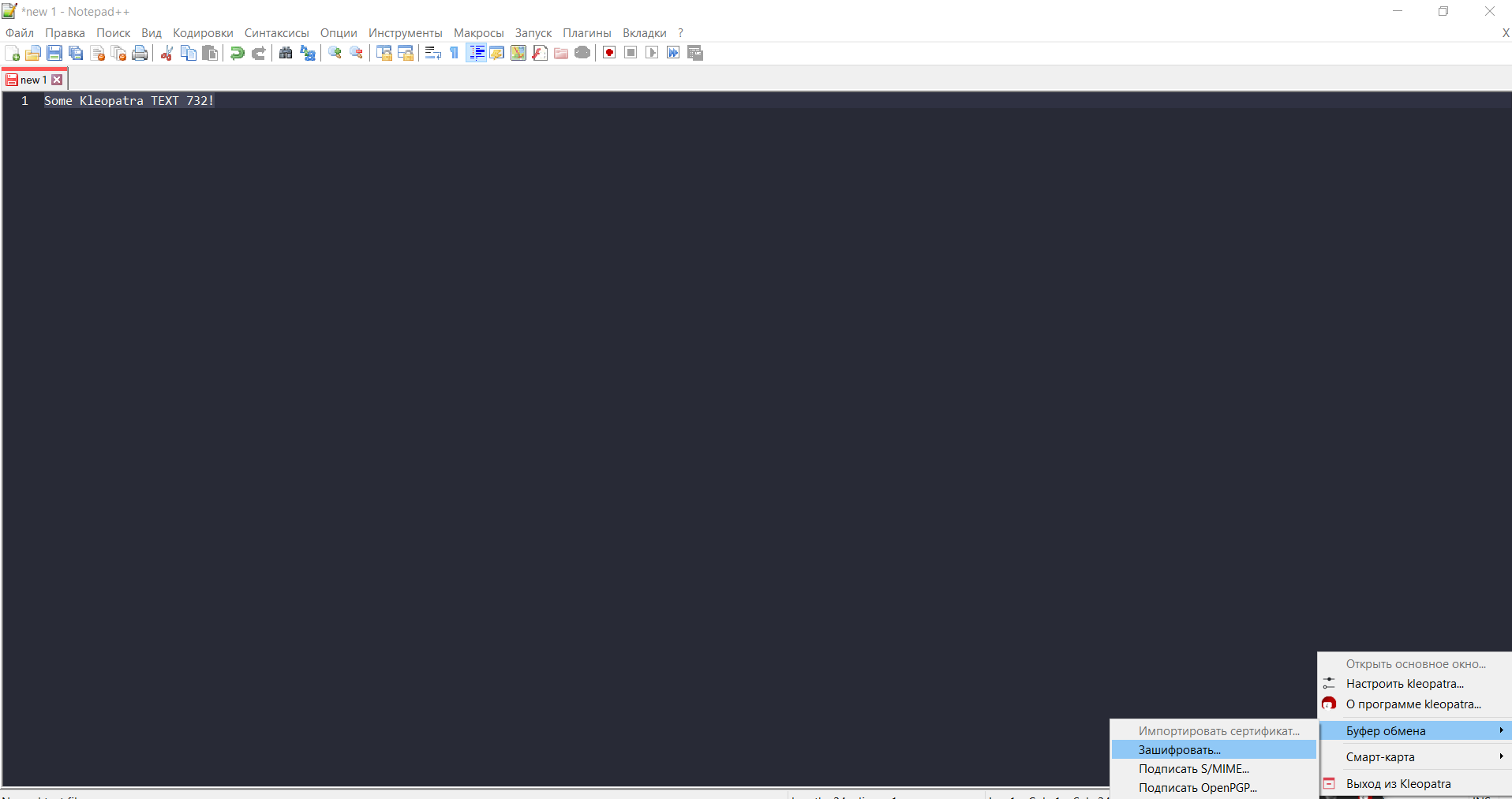
Виконаємо шифрування/розшифрування та підписування/перевірку підпису буферу обміну та поясніть отримані результати.

Скористуємось шифрування через буфер обміну

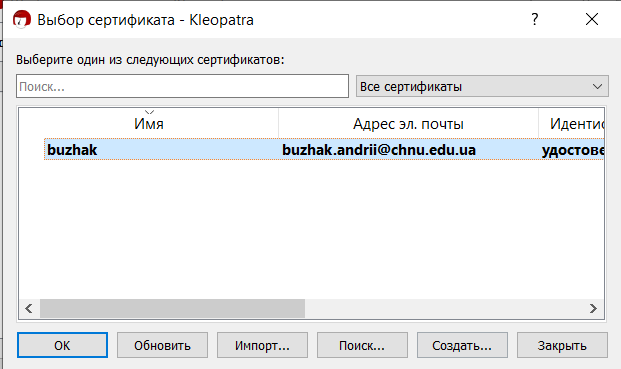
* Копіюємо потрібний текст

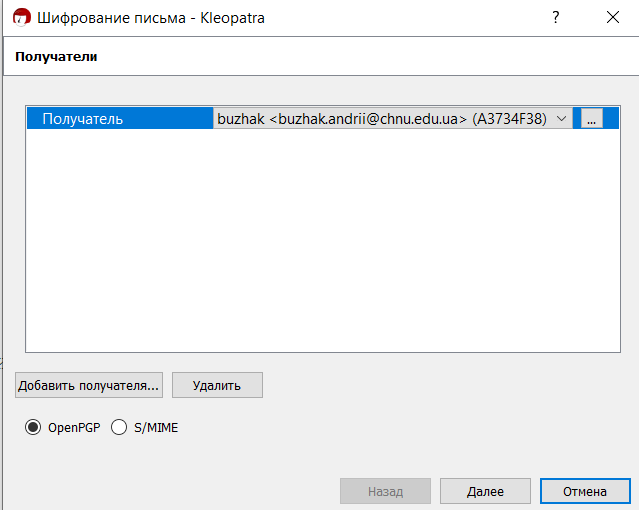


* Зашифруємо текст з буфера обміну

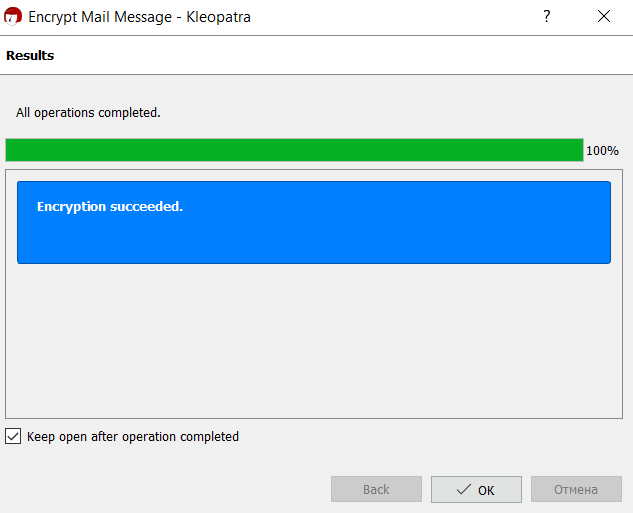


* Виберемо одержувача

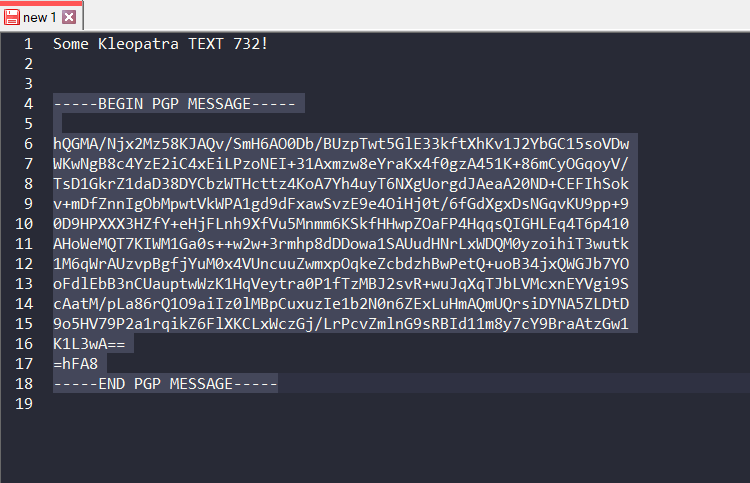




* Шифрування успішно завершене

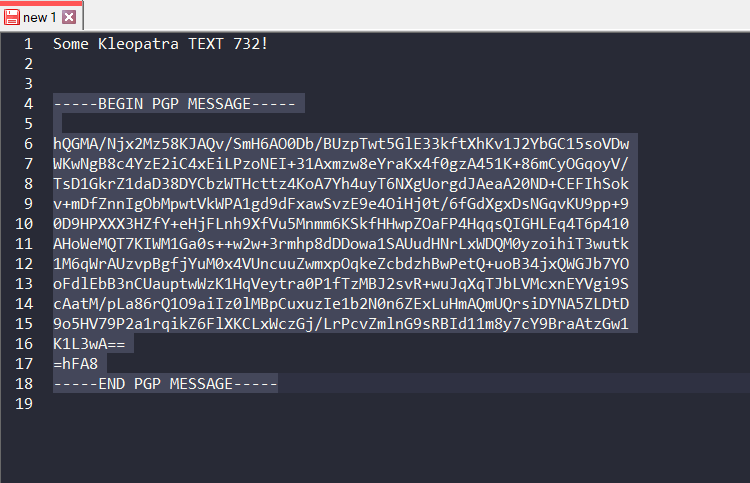


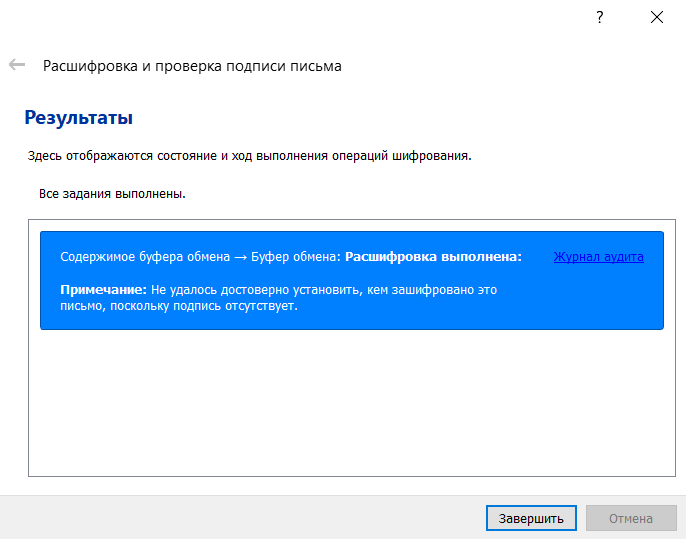
Вставимо результат шифрування в документ



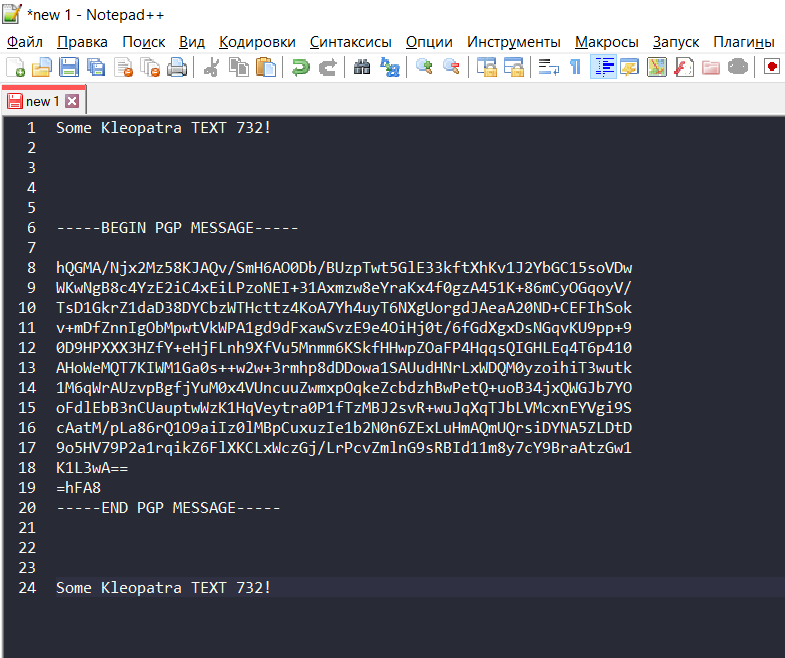
Як видно з рисунку, документ зашифровано асиметричним криптоалгоритмом, в даному випадку – RSA, оскільки саме його обуло обрано під час створення ключової пари. Цифровий підпис також буде виконано цим алгоритмом.

Проведемо розшифрування виділеного на рисунку зашифрованого тексту





Вставимо розшифрований текст в документ і отримаємо



***Відповіді на контрольні запитання***

1. Охарактеризуйте призначення GPG та Kleopatra.

GNU Privacy Guard (GnuPG або GPG) — відкритий програмний засіб для шифрування та цифрового підписування даних, вільний аналог Pretty Good Privacy (PGP). GnuPG повністю сумісний із стандартами OpenPGP (RFC-4880 організації IETF) і S/MIME, і надає утиліти для шифрування даних, роботи з електронними підписами, управління ключами і доступу до публічних сховищ ключів.

Kleopatra - менеджер сертифікатів та графічний інтерфейс для GnuPG. Програмне забезпечення зберігає ваші сертифікати та ключі OpenPGP. Він доступний для Windows та Linux.

1. Які способи захисту інформації підтримують ці засоби?

GPG зашифровує повідомлення використовуючи асиметричні алгоритми та згенеровані користувачем ключі. Отримані відкриті ключі можуть обмінюватись різноманітними шляхами, наприклад, через сервери ключів. Обмін відкритих ключів слід виконувати дуже уважно, аби уникнути підміни ідентичності відправника під час надсилання ключа. Також можливо додавати цифровий підпис до листів для того, щоб можна було підтвердити цілісність повідомлення та автентичність відправника.

3. Охарактеризуйте криптографічні алгоритми, які використовуються у цьому програмному забезпеченні.

GPG є програмою з гібридним шифруванням, в тому сенсі, що для підвищення швидкості роботи використовуються симетричні алгоритми шифрування, та асиметричні алгоритми шифрування для полегшення процедури обміну ключами, як правило, використовуючи відкритий ключ отримувача повідомлення для шифрування ключа сеансу, який використовується лише один раз. Цей режим роботи є частиною стандарту OpenPGP, і використовувався в PGP, починаючи з його першої версії.

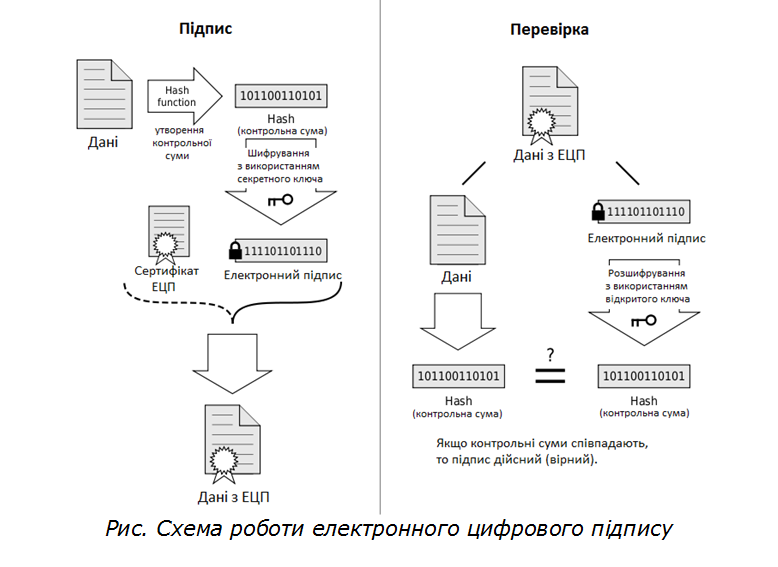
Асиметричні криптосистеми — ефективні системи, які для зашифровування даних використовують один ключ, а для розшифровування — інший (звідси і назва — асиметричні). Перший ключ є відкритим і може бути опублікованим для використання усіма користувачами системи, які шифрують дані. Розшифровування даних за допомогою відкритого ключа неможливе. Для розшифровування даних отримувач зашифрованої інформації використовує другий ключ, який є секретним (закритим). Зрозуміло, що ключ розшифровування не може бути визначеним з ключа зашифровування.

Прикладами криптосистем з відкритим ключем є Схема Ель-Гамаля (названа на честь автора, Тахера Ель-Гамаля), RSA (названа на честь винахідників: Рона Рівеста, Аді Шаміра і Леонарда Адлмана), Діффі-Геллмана і DSA, англ. Digital Signature Algorithm (винайдений Девідом Кравіцом).

4. Охарактеризуйте призначення та принципи роботи електронного цифрового підпису.

Електронний цифровий підпис (ЕЦП) — реквізит електронного документа, призначений для посвідчення джерела даних і захисту даного електронного документа від підробки.

Електронний цифровий підпис накладається за допомогою особистого ключа та перевіряється за допомогою відкритого ключа. За правовим статусом він прирівнюється до власноручного підпису (печатки). Електронний підпис не може бути визнаний недійсним лише через те, що він має електронну форму або не ґрунтується на посиленому сертифікаті ключа.



Перевірка Електронного цифрового підпису одержаного документа проводиться декількома етапами:

* На першому етапі адресат за допомогою програмного забезпечення Сертифікатом відкритого ключа автора розшифровує підписаний відбиток і одержує відбиток початкового документа.
* За допомогою програмного забезпечення і спеціальної математичної функції з документа, який був одержаний, обчислюється його відбиток.
* При перевірці ЕЦП порівнюються відбитки початкового і одержаного документів. Результат перевірки — одна з відповідей: «вірний»/«невірний».

5. Порівняйте можливості GPG та Kleopatra з Encrypted File System та BitLocker від Microsoft.

BitLocker або ж BitLocker Drive Encryption — засіб шифрування дисків, який входить до складу операційної системи Windows Vista та Windows 7 (версії Ultimate та Enterprise), а також Windows 8 (версії Pro and Enterprise), Windows Server 2008, Windows Server 2008 R2 і Windows Server 2012. BitLocker дозволяє шифрувати логічні диски операційної системи повністю. Окрім цього, у Windows 7 з'явилась додаткова можливість шифрувати USB-носії та картки пам'яті.

Можливі варіанти шифрування:

* AES 128
* AES 128 з Elephant diffuser (за умовчанням)
* AES 256
* AES 256 з Elephant diffuser

За умовчанням, для шифрування BitLocker використовує алгоритм шифрування AES зі 128-ми бітним ключем та Elephant diffuser. Обрати який із режимів шифрування використовувати можна за допомогою внесення відповідних змін у групову політику операційної системи.

Основна відмінність між GPG та Kleopatra з Encrypted File System та BitLocker від Microsoft полягає в застосуванні методів шифрування. Якщо в Kleopatra це асиметричні методи, то в BitLocker – це симетричні методи шифрування.