Навчально-науковий інститут інформаційних технологій
Харківський національний економічний університет
імені Семена Кузнеця

Звіт
З Виконання лабораторної роботи №2
за дисципліною: “ Безпека банківських систем ”
на тему: “ВИВЧЕННЯ СИСТЕМИ ЗАХИСТУ ДАНИХ TRUECRYPT”

Виконав: студент кафедри
Кібербезпеки та інформаційних
технологій
4 курсу, спец. Кібербезпека,
групи 6.04.125.010.21.2
Бойко Вадим Віталійович
Перевірив:
Лимаренко Вячеслав Володимирович

ХНЕУ ім. С. Кузнеця
2024

Мета: вивчити алгоритми симетричного шифрування та одностороннього хешування. Ознайомитись з можливостями сучасних програм шифрування даних на прикладі програми TrueCrypt.

Завдання:

1. За допомогою програми TrueCrypt створити звичайний том, захищений звичайним паролем.
2. За допомогою програми TrueCrypt створити звичайний том, захищений ключовим файлом.
3. За допомогою програми TrueCrypt створити прихований том у вже створеному звичайному томі.
4. Створити текстовий файл із певною послідовністю символів, помістити файл на змонтований носій, розмонтувати, спробувати виявити послідовність під час перегляду файлу TrueCrypt звичайними засобами перегляду.
5. Змонтувати прихований розділ та скопіювати створений у п.4 файл на цей розділ.
6. Спробувати змонтувати основний розділ при неправильному паролі.
7. За допомогою програм md5sum або sha1sum отримати хеш файлу з п.4. Скопіюйте цей файл на змонтований диск і отримати хеш там. Порівняти
   отримані результати та зробити висновки.
8. Перенести том TrueCrypt на інший комп'ютер із встановленою програмою TrueCrypt та спробувати його змонтувати (не обов’язково, при наявності технічної можливості).

Контрольні питання:

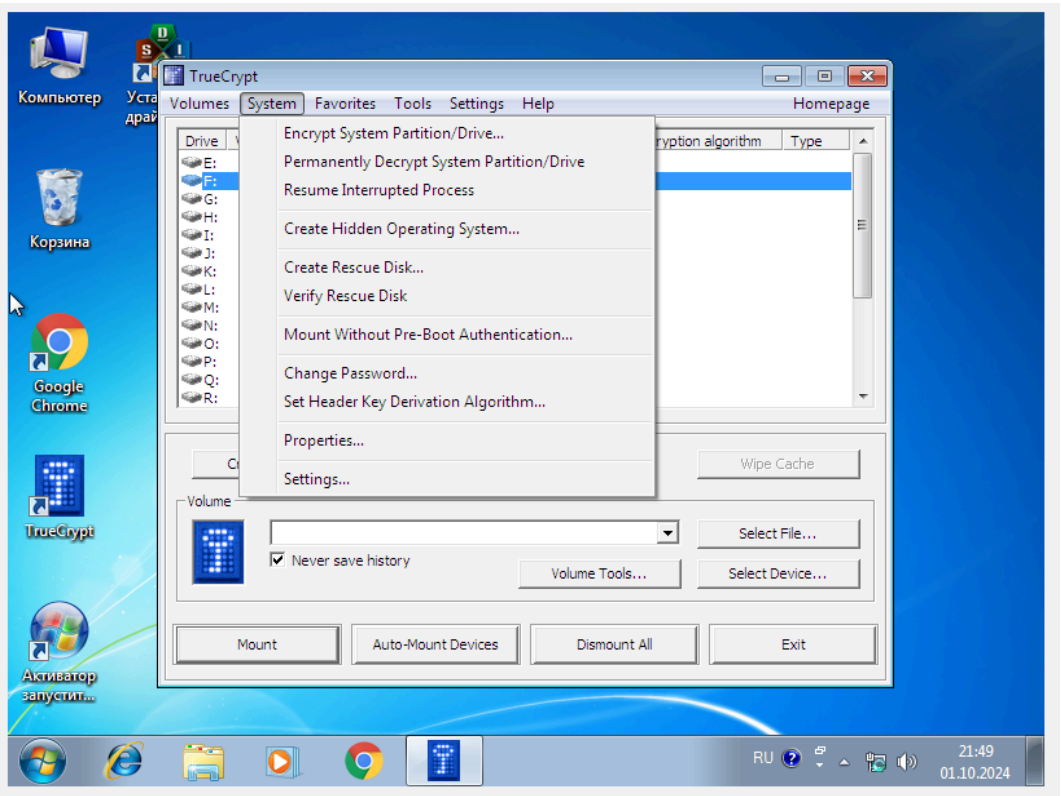
1. Що таке симетричні алгоритми шифрування? Наведіть приклади.
2. Які типи симетричних алгоритмів є?
3. Що таке хеш-функції? Навіщо вони застосовуються?

4. Назвіть основні можливості TrueCrypt.
5. Який принцип роботи TrueCrypt?
6. Для чого потрібні приховані томи TrueCrypt?

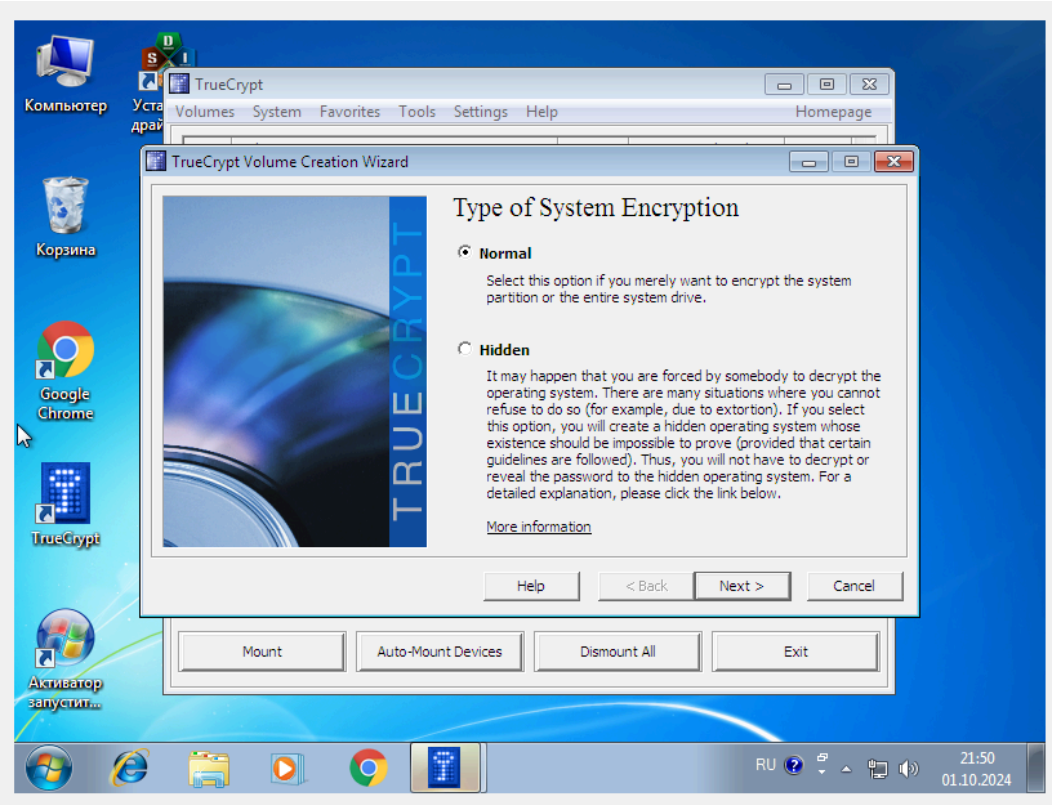
Хід роботи:

Завдання № 1, 2

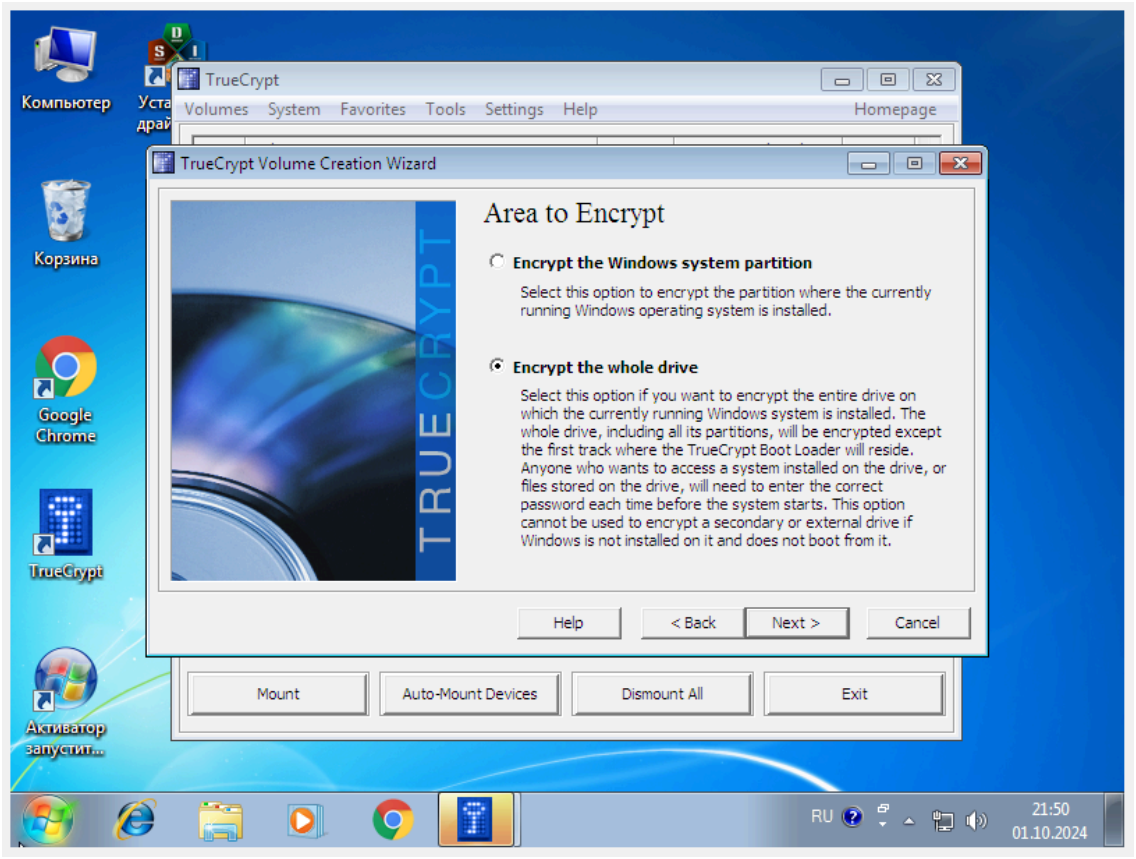
Запускаю програму й обираю перший пунк в меню “System”



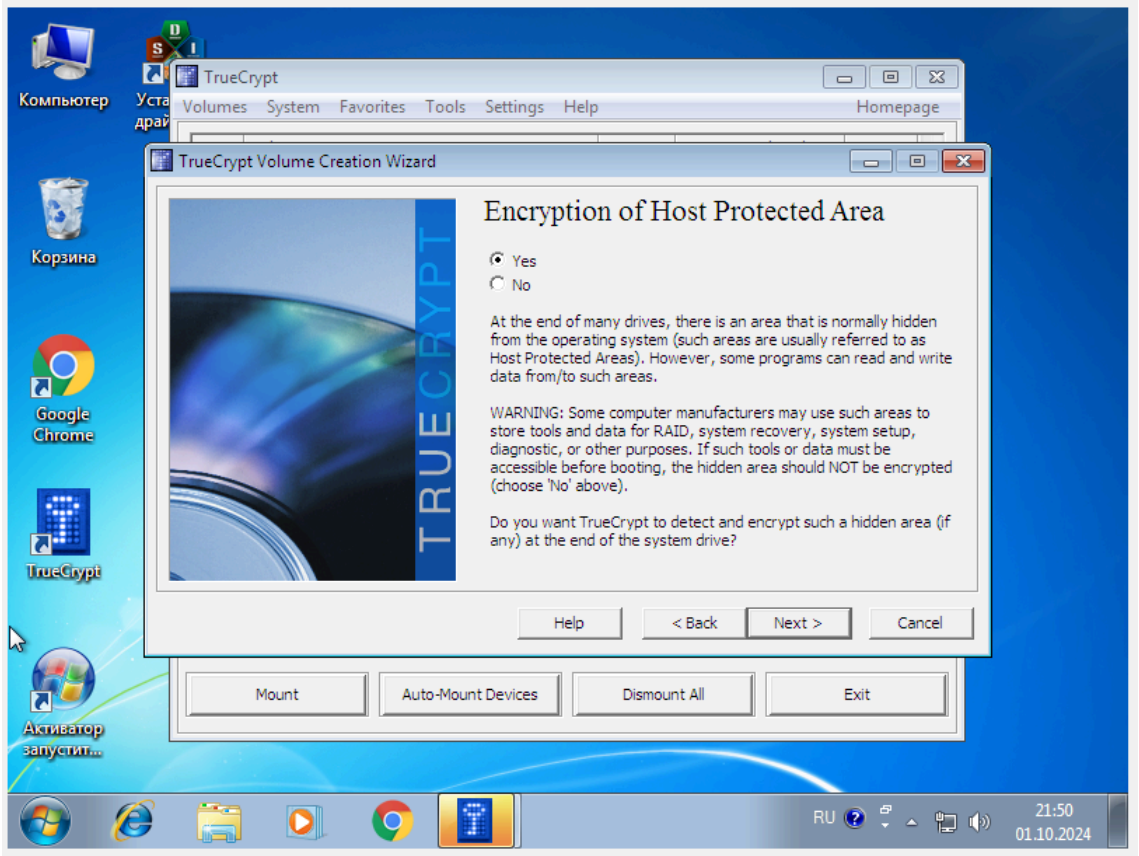
Наступним кроком обираю тип шифрування



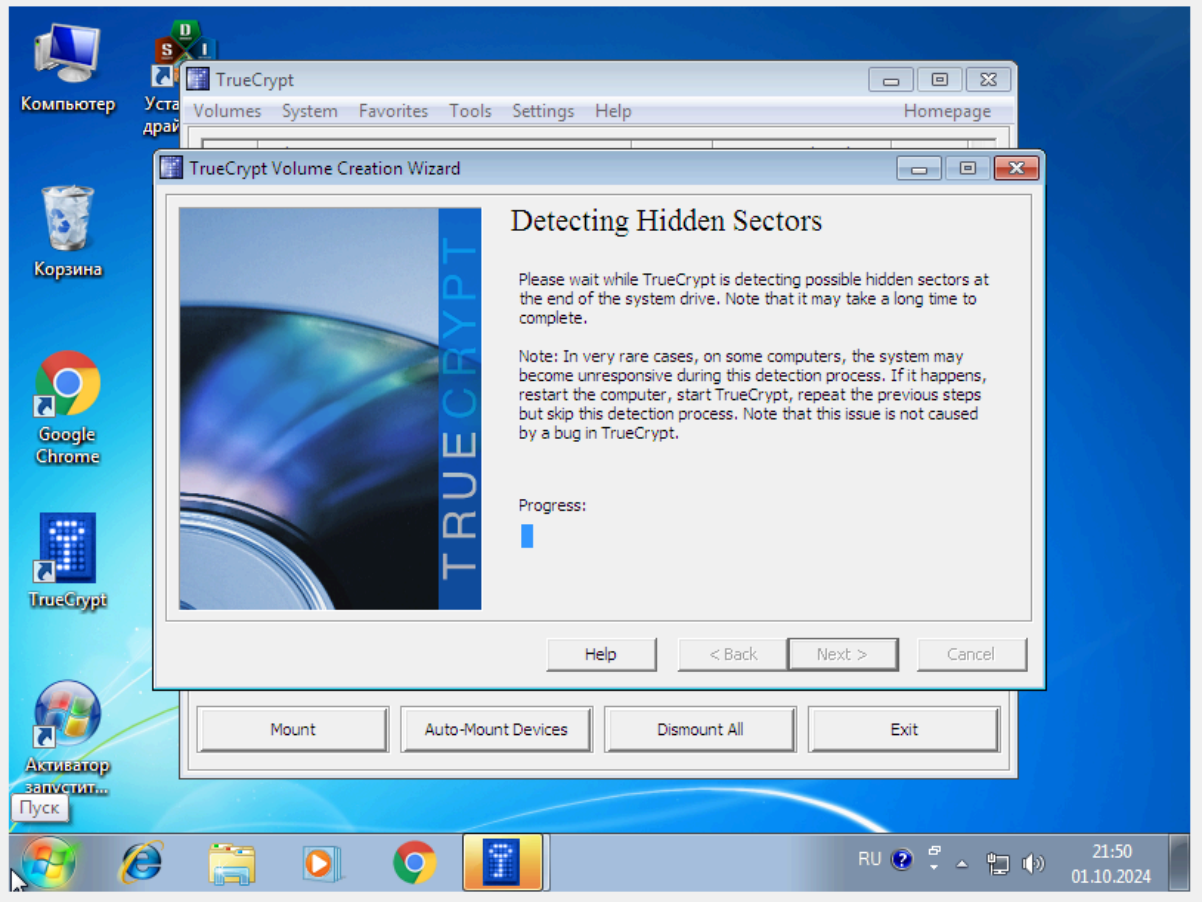
Після чого обираю зашифрувати весь диск

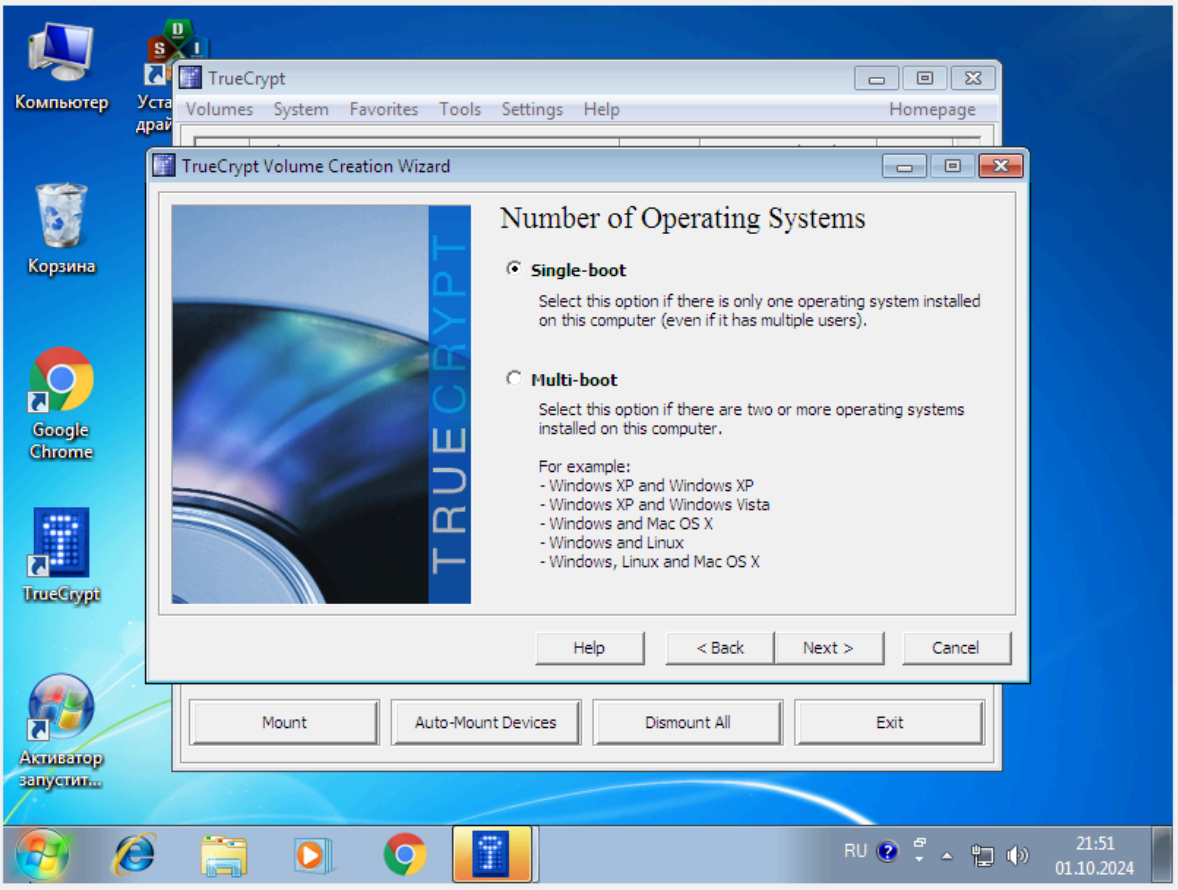


Та обираю чи потрібно шифрувати хост девайси

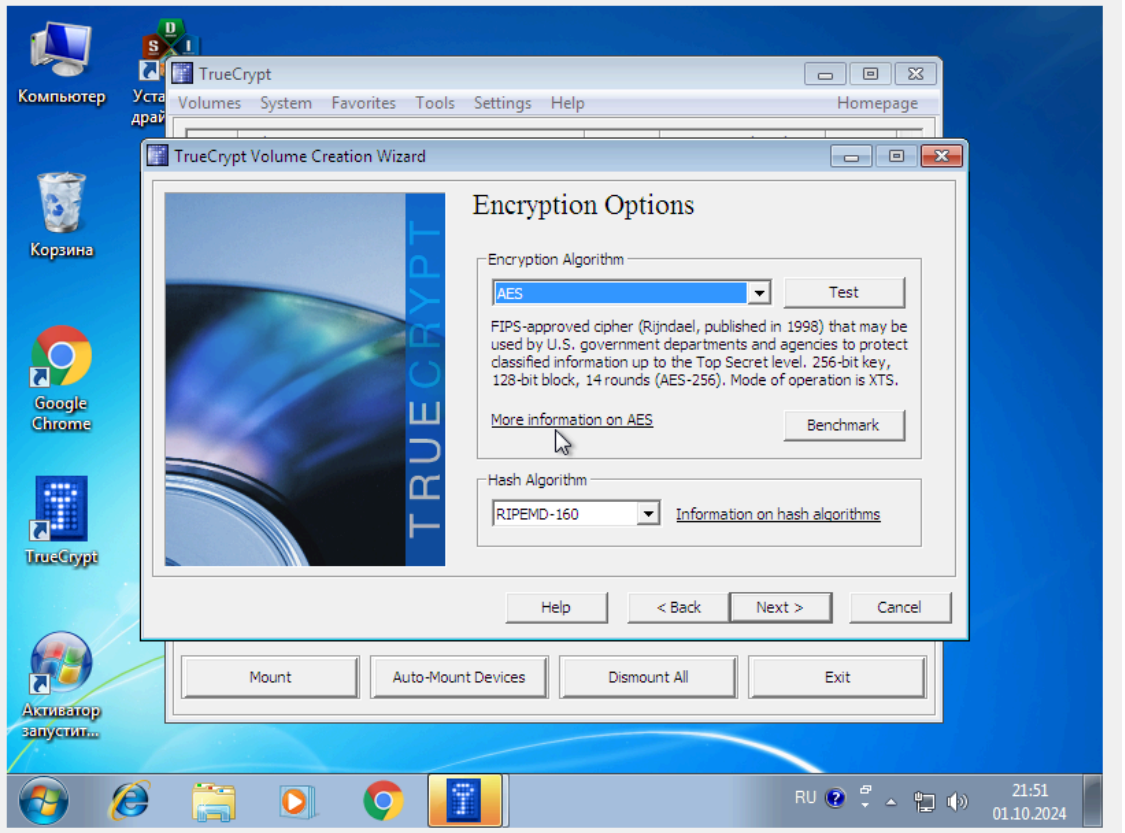


Після чого чекаю та обираю “Single Boot”

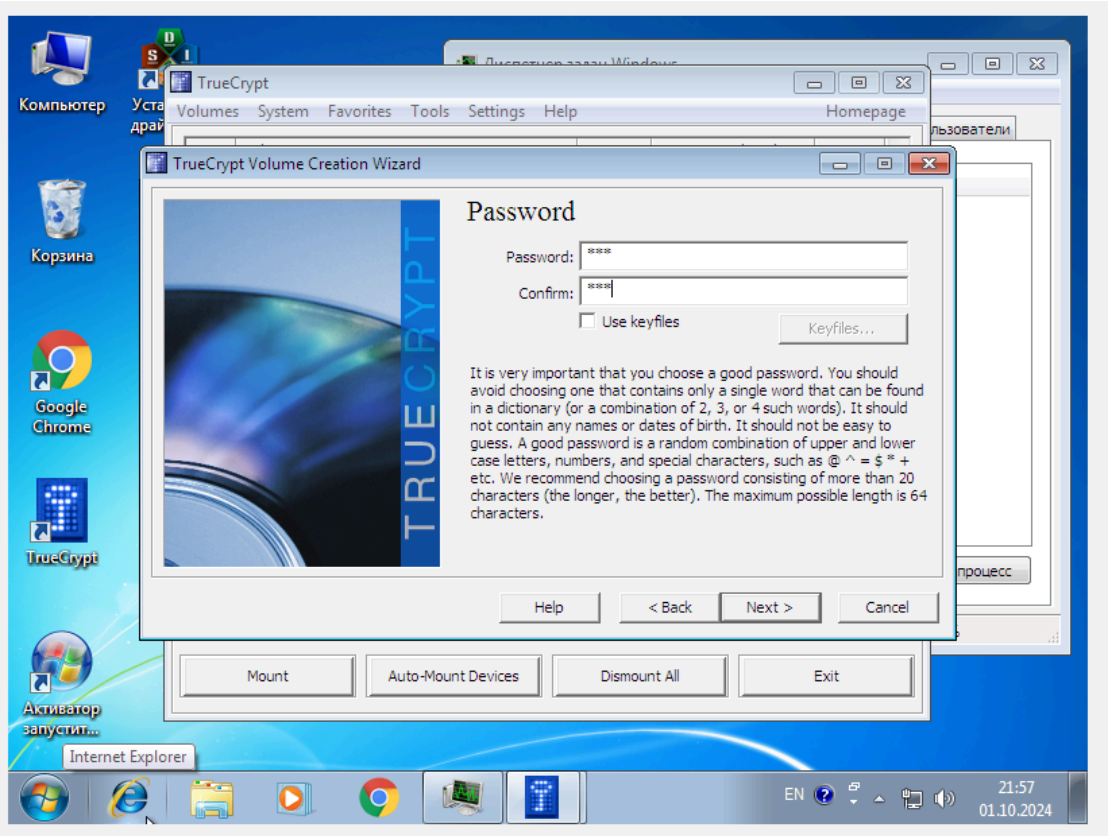




Наступним крококм обираю тип шифрування



Та задаю пароль, або можу обрати “Use keyfiles”



В результаті буде створено зашифрований диск

Відповіді на контрольні запитання:

1. Що таке симетричні алгоритми шифрування? Наведіть приклади.

Симетричні алгоритми шифрування – це такі алгоритми, де для шифрування та дешифрування даних використовується один і той самий ключ. Тобто, той самий ключ, який використовується для перетворення відкритого тексту в шифротекст, також використовується для перетворення шифротексту назад в відкритий текст.

Приклади симетричних алгоритмів: AES (Advanced Encryption Standard), DES (Data Encryption Standard), Blowfish, Twofish, RC4.

2. Які типи симетричних алгоритмів є?

Симетричні алгоритми зазвичай поділяють на два основних типи:

Блокові шифри: Оперують з фіксованими блоками даних. Приклади: AES, DES.

Потокові шифри: Шифрують дані побітово або побайтово. Приклади: RC4, Salsa20.

3. Що таке хеш-функції? Навіщо вони застосовуються?

Хеш-функція – це математична функція, яка перетворює вхідні дані довільної довжини в вихідну послідовність фіксованої довжини (хеш). Ця послідовність називається хеш-сумою або просто хешем.

Застосування хеш-функцій:

Перевірка цілісності даних: Якщо хеш-сума обчисленого файлу збігається з раніше обчисленою і збереженою, то файл не був змінений.

Створення паролів: Замість зберігання паролів у відкритому вигляді, зберігається їх хеш.

Цифрові підписи: Хеш-функції використовуються для створення цифрових підписів.
Структури даних: Хеш-таблиці використовують хеш-функції для швидкого пошуку даних.

4. Назвіть основні можливості TrueCrypt.
TrueCrypt (хоча і більше не підтримується) був потужним інструментом для шифрування дисків і створення віртуальних зашифрованих дисків. Основні його можливості включали:

Шифрування цілих дисків: Можливість шифрування системного диска або будь-якого іншого розділу.
Створення віртуальних зашифрованих дисків: Можливість створення файлів, які працюють як зашифровані диски.
Приховані томи: Можливість приховати один або кілька томів всередині іншого тома.
Шифрування системного розділу: Можливість завантаження операційної системи з зашифрованого розділу.
Підтримка різних алгоритмів шифрування: TrueCrypt підтримував широкий спектр симетричних і асиметричних алгоритмів.

5. Який принцип роботи TrueCrypt?
TrueCrypt використовував каскадне шифрування для забезпечення високого рівня безпеки. Дані на диску спочатку шифрувалися одним алгоритмом, а потім результат шифрувався ще одним алгоритмом. Це ускладнювало криптоаналіз. Крім того, TrueCrypt використовував різні техніки для приховування зашифрованих томів, що робило їх важковиявлюваними.

6. Для чого потрібні приховані томи TrueCrypt?

Приховані томи в TrueCrypt дозволяли створити додатковий шар безпеки. Прихований том був зашифрованим томом всередині іншого, більшого тома. Зовнішній том міг бути виявлений і розшифрований, але прихований том залишався недоступним для зловмисника, який не знав про його існування. Це було особливо корисно для захисту найважливіших даних.

Важливо зазначити: Хоча TrueCrypt був потужним інструментом, його розробка була припинена, і деякі експерти висловлювали занепокоєння щодо його безпеки. Тому, якщо вам потрібен інструмент для шифрування даних, рекомендується розглянути сучасні альтернативи, такі як Veracrypt, який є форком TrueCrypt і вважається більш безпечним.