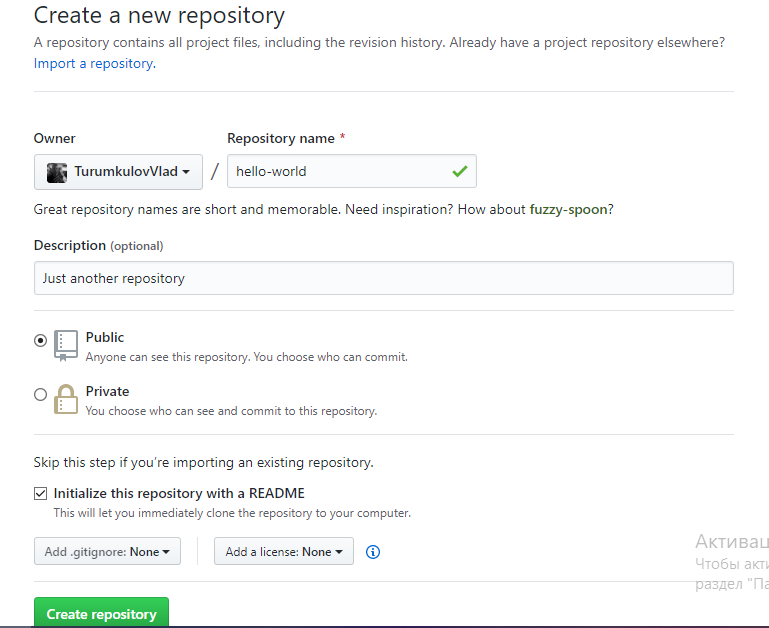
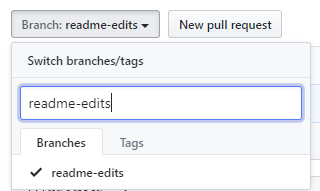
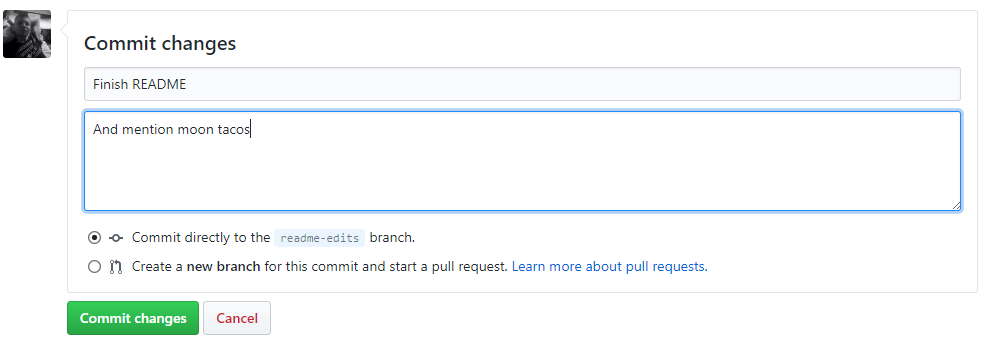
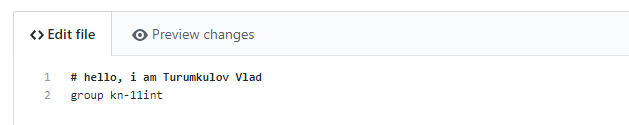
1. Створення репозиторію.

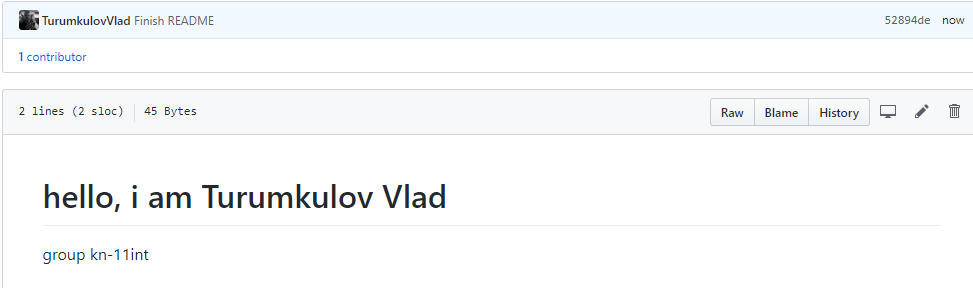


1. Створення нової гілки.

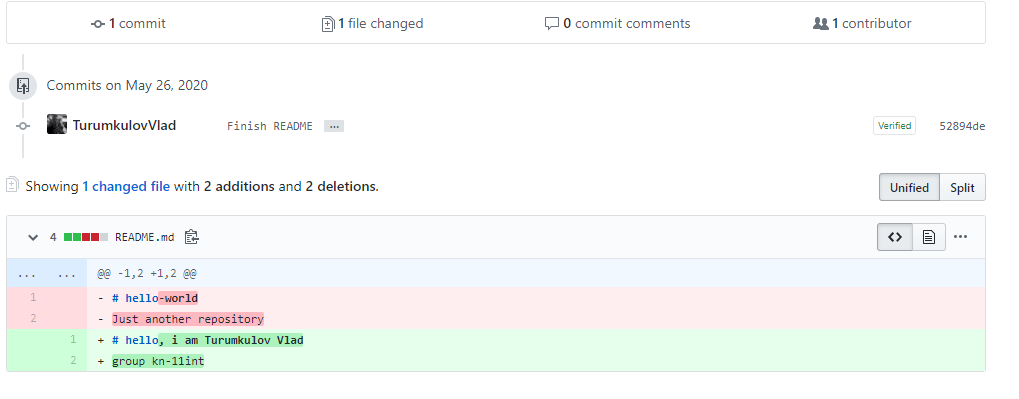


1. Внесення змін у файл README.md.

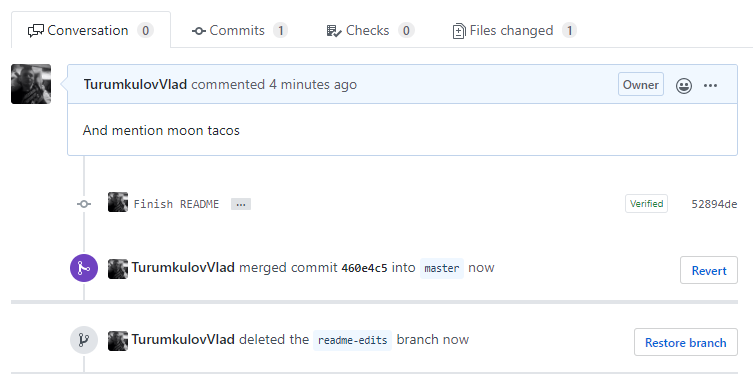




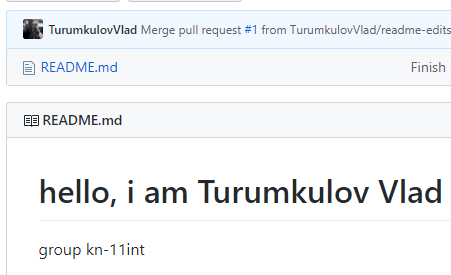
1. Процес злиття гілок.



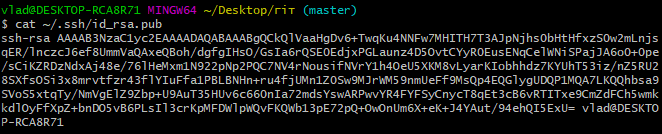
1. Закінчення злиття та видалення гілки readme-edits.



1. Файл README.md після злиття гілок .

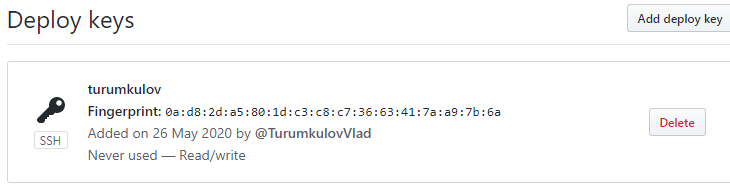


1. Створили папку на локальному ПК для подальшого створення репозиторію. Створили на локальному ПК нову пару SSH-ключів та перейменували їх.

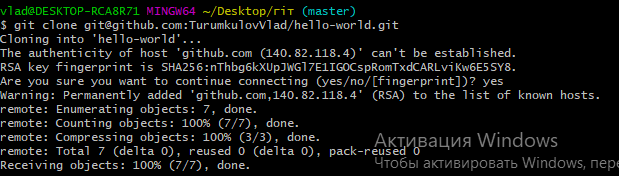




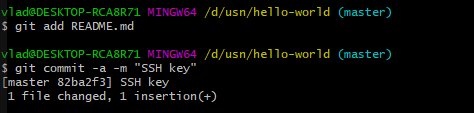
1. Додали SSH ключ у наш репозиторій на GitHub.

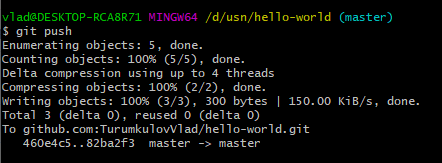


1. Клонували репозиторій з використання ssh ключа.

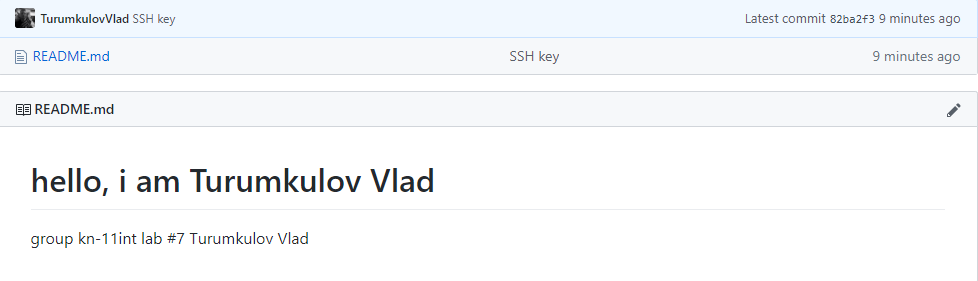


1. Внесли зміни до файлу README.md та занесли їх до глобального репозиторію .





1. Результат.



**Контрольні питання**

**1. Переваги SSH протоколу:**

1. Дозволяє працювати віддалено на комп'ютері через командну оболонку.
2. Шифрування здійснюється за допомогою різноманітних алгоритмів.
3. SSH дозволяє безпечно передавати практично будь-який мережевий протокол, це дає можливість передавати по зашифрованому каналу звукові та відеофайли.
4. Стискає файли для їх подальшого шифрування і передачі.
5. Захищає передачу даних по каналу і практично запобігає будь-яку можливість включення в установлену сесію і перехопити дані.

**2. Чим з’єднання по протоколу SSH відрізняється від з’єднання по протоколу HTTPS?**

1. Зазвичай SSH використовує порт 22, а HTTPS - порт 443.
2. HTTPS використовується переважно для надійної передачі критичної інформації, наприклад, у кредитних картках та банківській справі. З іншого боку, SSH призначений для безпечного виконання команд через Інтернет.
3. SSH використовує систему автентифікації імені користувача / пароля для встановлення захищеного з'єднання, поки HTTPS не дуже сильно це турбує.
4. SSH більше стосується тунельної мережі, тоді як HTTPS - більше про сертифікати.

**3. Для чого генеруються два ключі SSH? Хто і коли ці ключі використовує?**

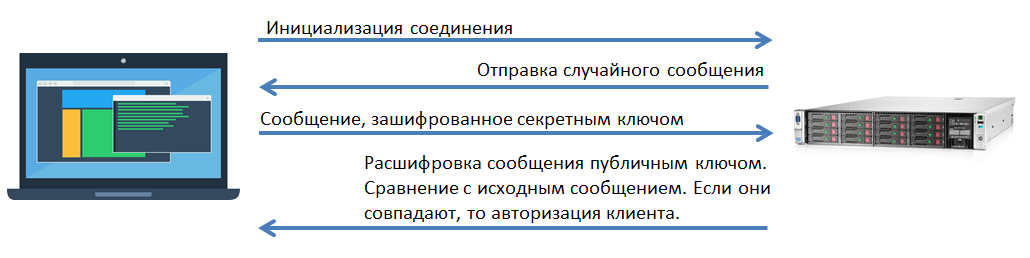
Кожна пара ключів складається з відкритого і закритого ключа. Секретний ключ зберігається на стороні клієнта і не повинен бути доступний будь-кому ще. Витік ключа дозволить зловмисникові увійти на сервер, якщо не була налаштована додаткова аутентифікація по паролю.

Відкритий ключ використовується для шифрування повідомлень, які можна розшифрувати тільки закритим ключем. Це властивість і використовується для аутентифікації за допомогою пари ключів. Відкритий ключ завантажується на віддалений сервер, до якого необхідно отримати доступ. Його потрібно додати в спеціальний файл ~ / .ssh / authorized\_keys.

Коли клієнт спробує виконати перевірку справжності через цей ключ, сервер відправить повідомлення, зашифроване за допомогою відкритого ключа, якщо клієнт зможе його розшифрувати і повернути правильну відповідь - аутентифікація пройдена.

**4. Як віддалений сервер виконує ідентифікацію по протоколу SSH?**

SSH сервер може виконувати аутентифікацію користувачів за допомогою різних алгоритмів. Найпопулярніший - це аутентифікація по паролю. Він досить простий, але не дуже безпечний. Паролі передаються по безпечному каналу, але вони недостатньо складні для протистояння спробам перебору. Обчислювальна потужність сучасних систем в поєднанні зі спеціальними скриптами роблять перебір дуже простим. Звичайно, існують інші способи додаткової безпеки, наприклад, fail2ban, але аутентифікація по ключу SSH надійніша.



**5. Навіщо слід періодично переглядати ключі SSH на віддаленому сервері?**

Для перевірки коректної роботи ключа з клієнт сервером та перевірки аутентифікації.