**Тема**: Логічна організація комп’ютерних мереж. Робота з мережними утилітами.

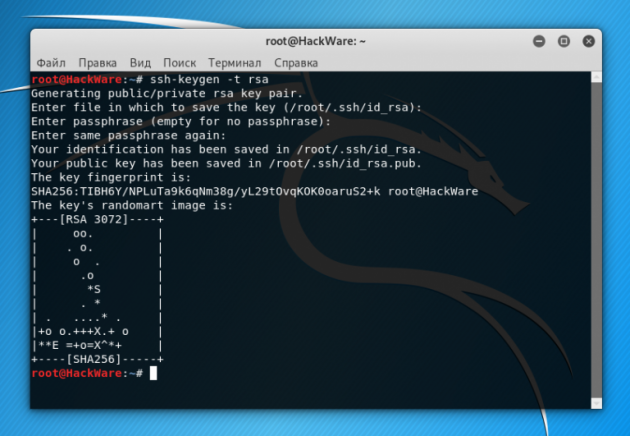
**Виконав**: 05 09

**SSH-ключі** – пара захищених шифруванням ключів (приватний та публічний), які використовуються для авторизації при підключенні до сервера за протоколом SSH. Ми рекомендуємо використовувати SSH-ключі замість пароля для підвищення надійності та безпеки підключення. Для генерації пари ключів використовується програма ssh-keygen, вона включена в пакет ssh і якщо SSH у вас вже налаштований, додатково встановлювати нічого не потрібно. Стандартні ключі SSH зберігаються в каталозі ~/. ssh. Якщо у вас немає каталогу ~/. ssh, створіть його з правильними дозволами за допомогою команди ssh-keygen. Вхід **до SSH** за публічним ключем (без пароля) дуже зручний та безпечний. Процес налаштування автентифікації за публічним ключем дуже простий: Командою створюється пара “публічний ключ – приватний ключ”.

Публічний ключ копіюється на комп’ютер із сервером SSH, тобто на комп’ютер, до якого буде здійснюватись підключення і на якому будуть виконуватися команди. А потім вже підключення виконується звичайним способом, але введення пароля не потрібно. Публічний ключ, який копіюється на віддалений сервер, не є таємним. Один і той же ключ можна використовувати на різних серверах. Головне – зберігати в секреті приватний ключ. Згененувати ключі та скопіювати їх на віддалений хост можна буквально трьома командами. Щоб прискорити процес входу та оптимізувати поведінку клієнта SSH, можна створити та налаштувати файл конфігурації SSH ~/.ssh/config. У програмі ssh-keygen багато функцій та можливостей, почнемо з розгляду процедури генерації ключів, яка виконується елементарно. Якщо ви встигли залогінитись на віддаленій системі, розлогіться.

https://hackyourmom.com/wp-content/uploads/2023/04/screenshot_25-1.png

У нас запитують ім’я файлу, не потрібно нічого вводити, буде використано стандартне ім’я. Також запитується пароль. Цей пароль дозволяє встановити додатковий захист – при підключенні за допомогою ключів не запитуватиметься пароль користувача, але запитуватиметься пароль самого ключа. Не потрібно встановлювати пароль.



**В результаті буде створено два файли:**

* **~/.ssh/id\_rsa**
* **~/.ssh/id\_rsa.pub**

Перший файл потрібно зберігати у секреті. Другий файл потрібно скопіювати на віддалений комп’ютер, де запущено сервер SSH. Тепер на дистанційній машині нам потрібно створити каталог .ssh.

Запустіть команду виду:

[https://hackyourmom.com/wp-content/uploads/2023/04/screenshot_1-4.png](https://hackyourmom.com/wp-content/uploads/2023/04/screenshot_1-4.png)

Наприклад:

[https://hackyourmom.com/wp-content/uploads/2023/04/screenshot_2-4.png](https://hackyourmom.com/wp-content/uploads/2023/04/screenshot_2-4.png)

Тепер нам потрібно скопіювати вміст файлу **id\_rsa.pub** на віддалену машину у **~/.ssh/authorized\_keys** файл.  Це дуже просто (треба поміняти дані на свої):

[https://hackyourmom.com/wp-content/uploads/2023/04/screenshot_3-4.png](https://hackyourmom.com/wp-content/uploads/2023/04/screenshot_3-4.png)

Наприклад:

[https://hackyourmom.com/wp-content/uploads/2023/04/screenshot_4-3.png](https://hackyourmom.com/wp-content/uploads/2023/04/screenshot_4-3.png)

Тепер виконуємо підключення за допомогою клієнта SSH, але пароль у нас більше не питатиметься.

**Типи ключів**

### Програма ssh-keygen може генерувати чотири типи ключів:

* **dsa**
* **ecdsa**
* **ed25519**
* **rsa**

Щоб вибрати будь-який із цих типів, використовується опція **-t.** У попередньому прикладі ми вибрали rsa – явно вказувати тип RSA необов’язково, оскільки він мається на увазі за умовчанням (тобто генерацію ключів можна запустити без опції **-t)**.

### Залежно від вибраного типу, назви створених файлів ключів можуть відрізнятися:

* **~/.ssh/id\_dsa**
* **~/.ssh/id\_ecdsa**
* **~/.ssh/id\_ed25519**
* **~/.ssh/id\_rsa**

Ці файли потрібно тримати в секреті, вони мають бути доступні лише для власника.

### Відповідні публічні ключі матимуть таку саму назву, але з додатковим розширенням .pub:

* **~/.ssh/id\_dsa.pub**
* **~/.ssh/id\_ecdsa.pub**
* **~/.ssh/id\_ed25519.pub**
* **~/.ssh/id\_rsa.pub**

Ці файли не є секретними, їх вміст потрібно скопіювати у файл **~/.ssh/authorized\_keys** на комп’ютер із сервером **SSH.**

**Утиліта ssh-keygen**

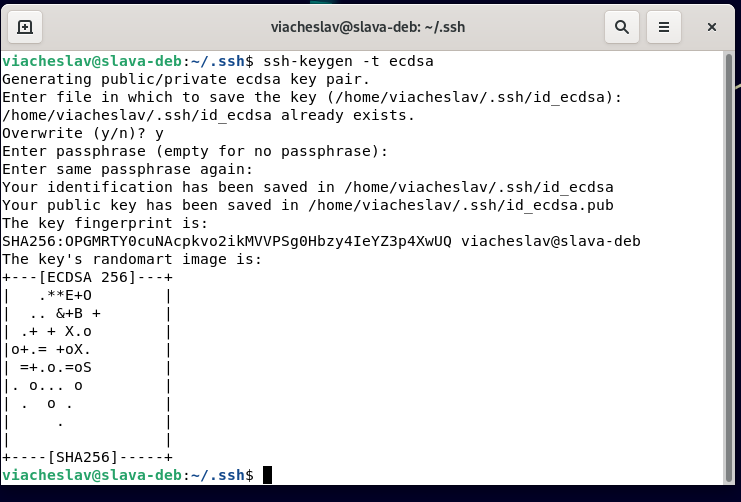
Ми застосували **ssh-keygen** для створення ключів. Крім цього вона призначена для керування та конвертації ключів аутентифікації для **ssh**. Далі розглянуті лише деякі функції цієї програми, з повним переліком опцій можна ознайомитись командою:

[https://hackyourmom.com/wp-content/uploads/2023/04/screenshot_5-3.png](https://hackyourmom.com/wp-content/uploads/2023/04/screenshot_5-3.png)

**Як змінити кількість бітів у ключах ssh-keygen?**

Для цього використовується опція: **-b** Вона визначає кількість біт у створюваному ключі. Для ключів **RSA** мінімальний розмір становить 1024 біти, а за замовчуванням **– 2048 біт**. Як правило, **2048 біт** вважається достатнім. Ключі **DSA** повинні мати довжину **1024** біта, як зазначено у **FIPS 186-2.** Для ключів ECDSA прапор **-b** визначає довжину ключа, вибираючи один із трьох розмірів еліптичної кривої: **256, 384** або **521** біт. Спроба використовувати бітові довжини, відмінні від цих трьох значень, для ключів **ECDSA** зазнає невдачі. Ключі **Ed25519** мають фіксовану довжину і прапор **-b** ігноруватиметься.

**ssh-keygen –t ecdsa**

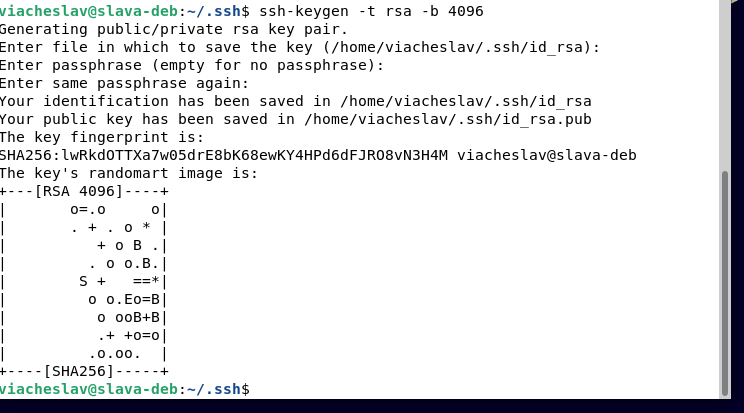


Розміри ECDSA ключів зазвичай варіюються від 256 до 521 біт.

**RSA** (Rivest-Shamir-Adleman): RSA є асиметричним алгоритмом шифрування, підпису та аутентифікації, який отримав свою назву за першими літерами прізвищ його творців. RSA ключі є досить універсальними і широко підтримуються різними протоколами та програмним забезпеченням. Розмірість RSA ключів може варіюватися від 1024 до 4096 біт, але 2048 біт вважається рекомендованим розміром для більшості застосувань.

**ssh-keygen -t rsa -b 4096**

Ця команда запускає ssh-keygen з параметрами -t rsa (тип ключа RSA) та -b 4096 (розмір ключа 4096 біт).

****