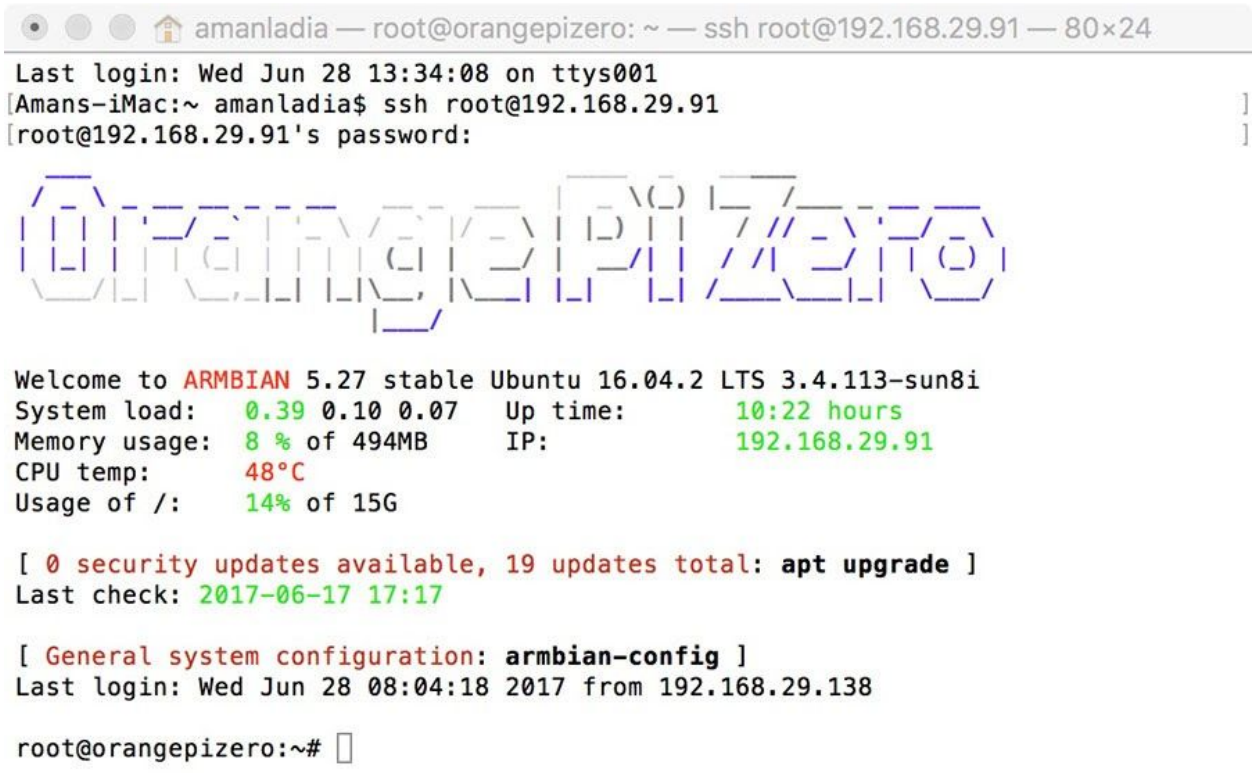
Как работи SSH

Какво е SSH

SSH (Secure Shell) е протокол за отдалечена администрация, който позволява на потребителите да контролите и модифицират отдалечени сървъри, чрез Интернет. SSH е създаден като по-сигурна алтернатива на некриптирания Телнет и използва криптография, за да се увери, че всичката комуникация към и от отдалечения сървър се случва в криптирана среда. SSH дава механизъм за удостоверяване на отдалечени потребители, трансфер на входни данни от клиента към сървъра и връщане на отговор от сървъра обратно към клиента.

По-долу може да видите как изглежда един типичен SSH прозорец. Който и да е потребител на Линукс дистибуция или macOS може да ползва SSH, за да достъпи отдалечен сървър директно от терминала на своята машина. За Windows съществуват също SSH клеинти от типа на Putty. SSH ни позволява да пускаме команди по същия начин, по който бихме, ако управлявахме отдалечената машина на място.



В този урок ще разгледаме как работи SSH, както и какви технологии се използват за криптиране на информацията.

Как работи SSH

Ако използвате която и да е Линукс дистрибуция или Mac, то употребата на SSH много проста. Ако използвате Windows, то ще трябва да си инсталирате SSH клиент. Идеален за целта е PuTTY, **ето тук може да намерите повече информация**.

Под Линукс, отворете терминала и следвайте процедурите по-долу:

SSH командата се състои от 3 различни части:

```
ssh {user}@{host}
```

SSH командата показва на вашата система, че искате да отворите криптирана Secure Shell връзка. **{user}** показва потребителя, който искате да достъпите (този потребител трябва да е добавен на отдалечения сървър). Например, може да искате да достъпите потребител **pgee**. **{host}** показва адреса към машината, която искате да достъпите - това е IP адрес **(примерно 244.235.23.19)** или домейн (примерно www.xyzdomain.com).

Когато натиснете ентер, ще ви бъде поискана парола за съответния потребителски профил. Не забравяйте, че когато пишете парола, тя няма да излиза на екрана, но въпреки това тя се предва. Когато сте написали паролата, натиснете Enter отново. Ако паролата е била правилна, ще видите съобщение от терминала на отдалечения сървър.

Как работи криптирането?

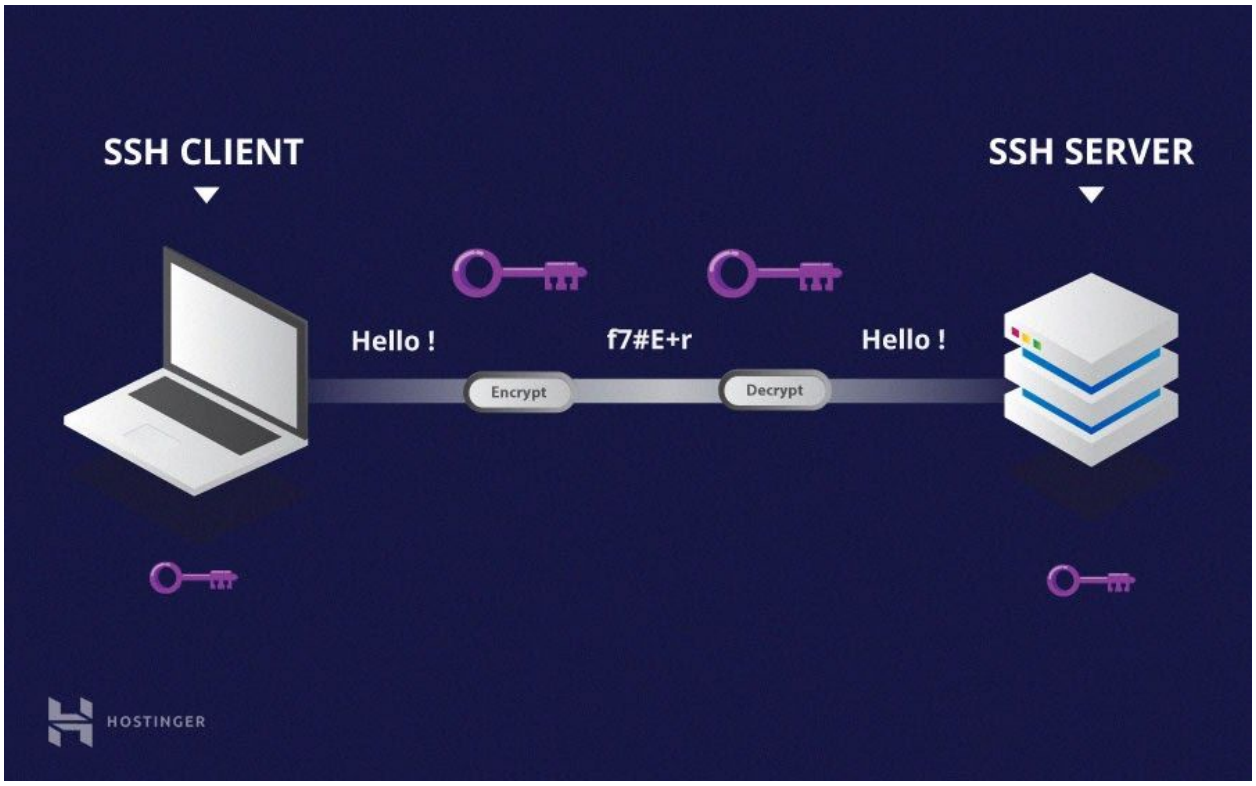
Главното предимство на SSH е използването на криптиране, за да се гарантира сигурното предаване на информацията между хоста и клиента. **Хост** ще наричаме отдалечения сървър, който искаме да достъпим, а **клиент** е компютъра, който ние ползваме, за да осъществим достъпа до хоста. С други думи - хостът е машината, която евентуално е далеч от нас, а клиент е машината, на която работим ние физически. SSH използва три различни криптиращи технологии:

- Симетрично криптиране
- Асиметрично криптиране

- Хеширане

Симетрично криптиране

Симетричното криптиране е форма на криптиране, при която се използва **таен ключ (secret key)**, както за криптиране, така и за декрептиране едновременно и от клиента, и от хоста. На практика, всеки, който притежава ключа може да декриптира съобщението, което се предава.



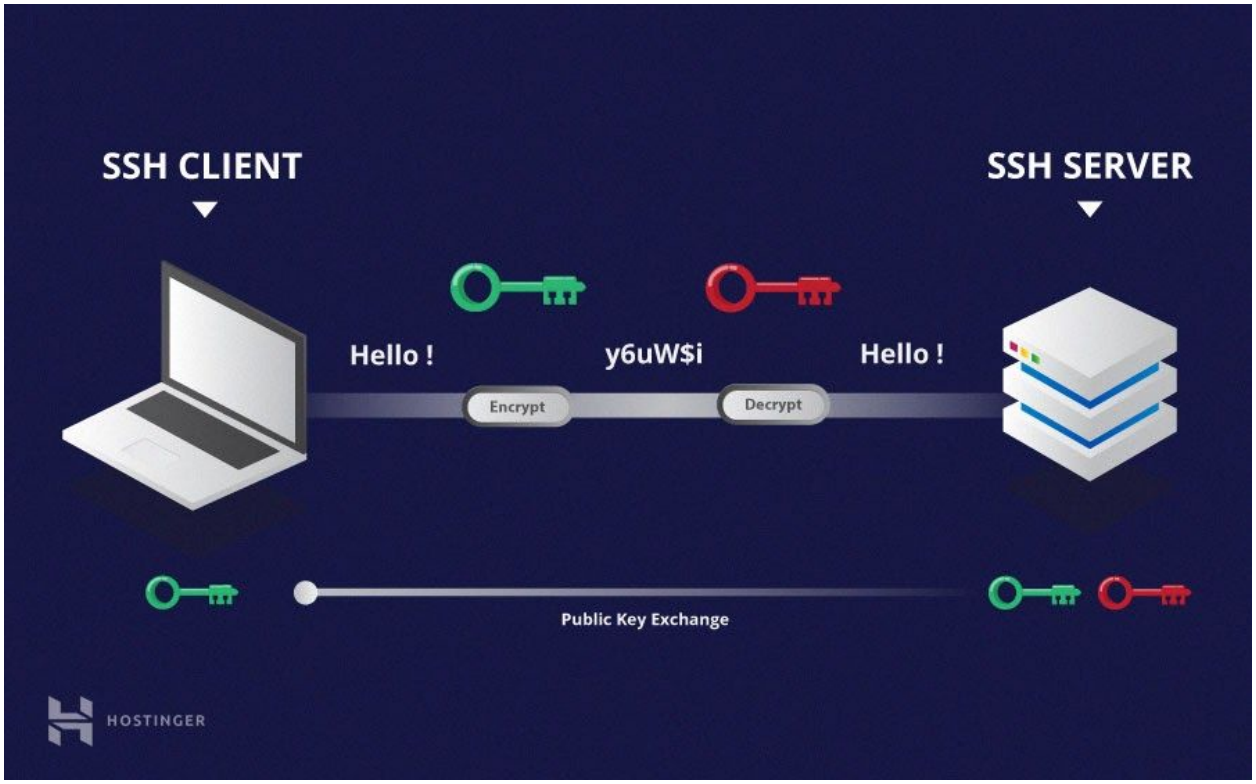
Симетричното криптиране се нарича често криптиране със **shared key (споделен ключ)** или криптиране със **shared secret (споделена тайна)**. Обикновено се използва само един ключ или понякога двойка ключове, като при това единия ключ лесно може да се изчисли, ако притежаваме другия.

Симитричните ключове се използват, за да се криптира цялата комуникация по време на SSH сесия. И клиента и сървъра се сдобиват с тайния ключ по сходен метод, като резултатния ключ никога не се предоставя на трета страна. Процесът по създаването на симетричен ключ се случва чрез **key exchange algorithm (алгоритъм за размяна на ключове)**. Това, което прави алгоритъма особено сигурен е фактът, че ключа никога не

се предава от клиента към хоста. Вместо това двете машини споделят публични парчета информация и след това я манипулират, за да изчислят независимо споделения ключ. Дори и друга машина да получи публичната информация, тя няма да може да изчисли тайния ключ, защото за нея точния key exchange algorithm, който се ползва от двете машини не е известен.

Асиметрично криптиране

За разлика от симетричното криптиране, асимитричното криптиране използва два отделни ключа за криптиране и декриптиране. Тези два ключа са известни като **public key (публичен ключ)** и **private key (частен ключ)**. Заедно тези ключове формират **public-private key pair (публично-частна двойка ключове)**.



Публичния ключ, както предполага името се споделя отворено с всички страни. Въпреки че е тясно свързан с частни ключ от гледна точка на функционалност, частния ключ не може да се изчисли математически на базата на публичния. Връзката между двата ключ е доста сложна: съобщение, което е криптирано от публичния ключ на дадена машина, може да бъде декриптирано само от нейния частен ключ. Това означава, че публичния

ключ не може да декриптира съобщенията, които са били криптиране с него, нито пък да декриптира каквото и да е криптирано с частния ключ.

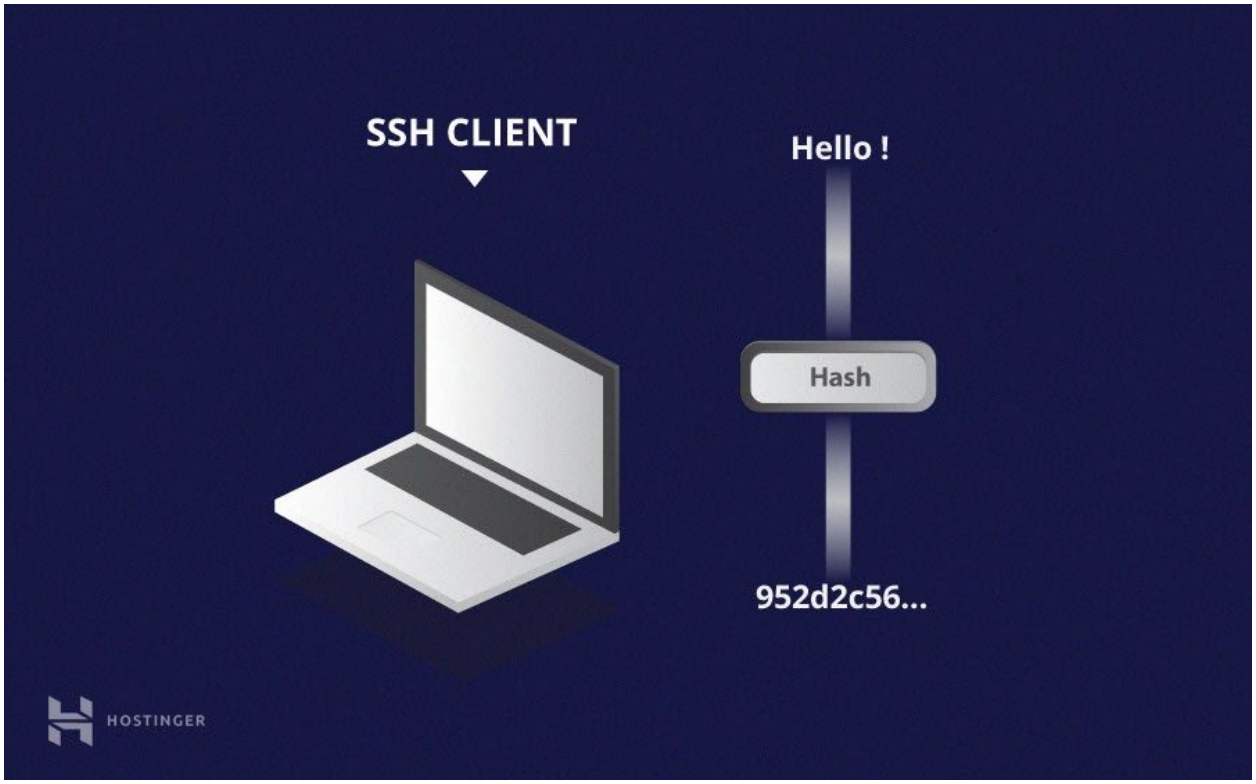
Частния ключ трябва да си остане личен, т.е. Не трябва да става известен на никой друг освен на притежателя му, за да не се наруши сигурността на връзката. Силата на цялата връзка се държи на факта, че частния ключ никога не се разкрива, т.като това е единствения компонент, който е способен да декриптира съобщения, които са били критпирани от съответния публичен ключ.

Асиметричното криптиране на се използва за критпирането на цялата SSH сесия, въпреки всеобщата заблуда, че това е така. Вместо това, то се използва само по време на key exchange algorithm на симетричното криптиране. Преди да се инициализира сигурна връзка, двете страни генерират временни публично-частни двойки ключове и си споделят съответните частни ключове, за да генерират общ споделен таен ключ, който е нужен за симетричното криптиране.

Веднъж щом се установи сигурна връзка чрез симетрична комункация, сървъра използва публичния ключ, за да генерира предизвикателство (challenge) и го изпраща към клиента за удостоверение. Ако клиента може да декриптира успешно съобщението, то това означава, че притежава частния ключ за връзката. Тогава започва SSH сесията.

Хеширане

Еднопосочното хеширане е друга форма на криптография, която се използва от SSH. Еднопосочните хеш функции се различават от горните две форми на криптиране по това, че те не се очаква да се декриптират. Те генерират уникална стойност с определена дължина за различни входни данни и нямат определен принцип, по който да се предскаже каква ще бъде генерираната стойност или коя генерирана стойност на коя входна стойност съответства. Това ги прави почти невъзможни за декриптиране.



Много лесно можем да генерираме такава уникална стойност (хеш) на базата на дадени входни данни, но е невъзможно да получим входните данни, имайки хеш.

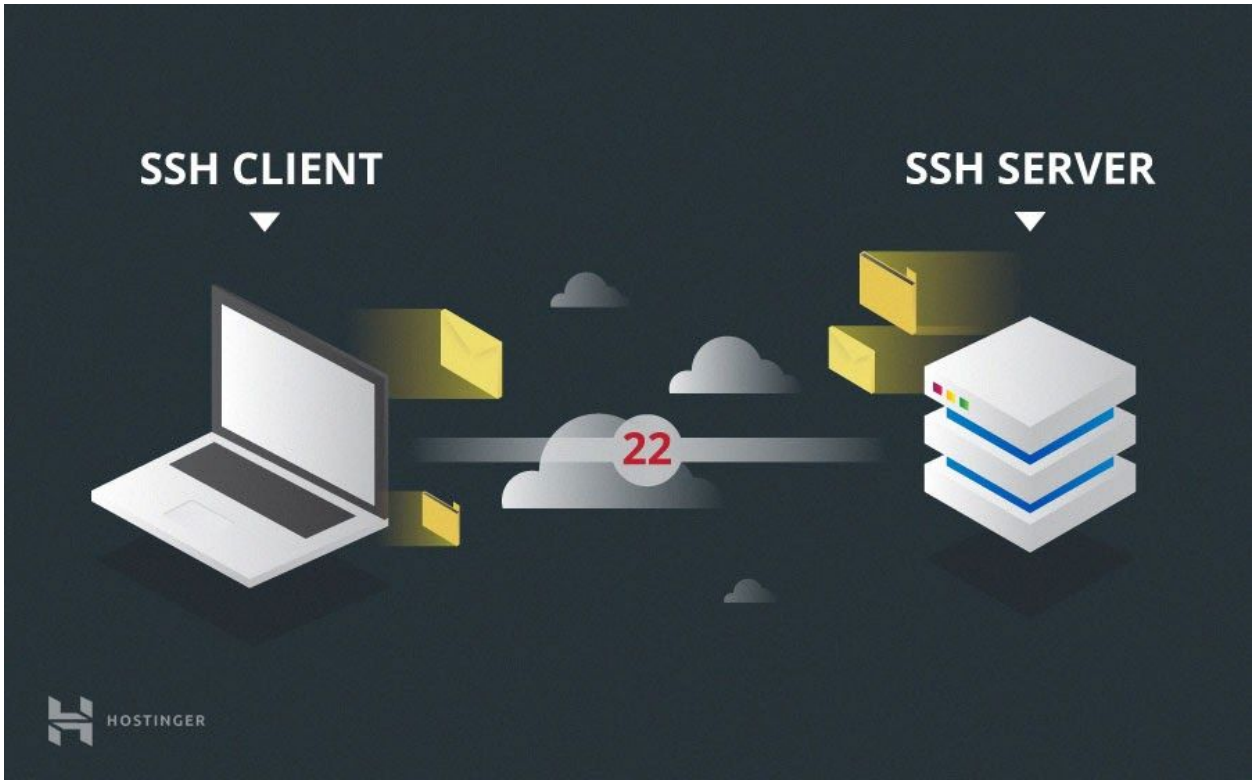
Това означа, че ако клиента притежава входни данни, те могат да генерират хеш стойността за тези данни и да я сравнят, за да потвърдят, че те притежават правилните данни.

SSH използва хеширане, за да потвърди достоверността на съобщенията. Това се прави чрез HMACs (**H**ash-based **M**essage **A**uthentication **C**odes). Това гарантира, че командата, която се получава не е била подменена по някакъв начин.

Как работи SSH с тези техники за криптиране

SSH работи чрез модела клиент-сървър, който позволява удостоверяването между две отдалечени системи и криптирането на информацията, която се предава между тях.

SSH използва TCP порт 22 по подразбиране (макар че може да се промени, ако има нужда). Хостът (Сървърът) “слуша” на порт 22 (или на съответния зададен порт) за входящи връзки. Той организира сигурната връзка, като удостоверява клиента и отваря съответната shell среда, ако данните на потребителя са правилни.



Клиентът трябва да започне със SSH връзката. В установяването на връзката има две фази: първо и двете системи трябва да фиксират кой алгоритъм за криптиране ще ползват и второ, потребителя трябва да се удостовери. Ако данните съвпаднат, то потребителя получава достъп.

Удостоверяване на потребителя

Финалната фаза преди потребителя да получи достъп до сървъра е да се потвърдят неговите потребителски данни. За тази цел, повече SSH потребители използват паролата на потребителя. Потребителя първо бива попитан да въведе потребителското си име, последователно от паролата. Тези данни минават през сигурната връзка, гарантирана от тунела, който е симетрично криптиран, което прави невъзможно засичането им от трета страна.

Въпреки че паролите се криптират, не е препоръчително да използвате пароли за сигурни връзки. Това е така защото много ботове могат да направят brute force атака и да получат достъп до акаунта. Препоръчаната алтернатива е **SSH Key Pairs**. Те представляват множество от асиметрични ключове, който удостоверяват потребителя без да има нужда да се изписва каквато и да е парола.