

Mi is az ssh/RSA?

Az ssh (Secure Shell) egy protokoll, ami távoli gépek között biztonságos csatornán keresztül kommunikációra (akár parancsok végrehajtására) fejlesztettek ki. Hitelesítéshez nyilvános kulcsú (RSA) titkosítást használ. Ennek lényege, hogy minden résztvevő rendelkezik két kulccsal: egy titkossal és egy nyilvánossal (privát és publikus, ha valakinek úgy jobban tetszik). A két kulcs egymást kiegészítve működik, a nyilvánossal lezárt szöveget csak a titkos nyitja ki, és fordítva, a titkossal lezártat a nyilvánossal nyithatjuk ki.

Használata ssh paranccsal

Ahhoz, hogy jelszó nélkül, RSA-hitelesítéssel be tudjunk lépni, először kulcsokat kell generálni az `ssh-keygen -t rsa` paranccsal. A kulcsokra ekkor jelszavas védelem tehető (opcionális). A publikus kulcsok (`id_rsa`) azon a gépen kell lennie, ahova be akarunk lépni (pl: omnibus), a home-ban, egy `.ssh` könyvtárban, a publikusnak pedig azon, ahonnan be akarunk lépni, a `.ssh/authorized_keys` -ben. Ez utóbbiba be kell másolnunk az imént létrehozott `id_rsa` tartalmát. *Fontosak a jogosultságok:* `ssh` könyvtár 700, a távoli gépen a home könyvtár: 755 (tudjátok, `chmod` parancs)

Maga a belépés egyszer?, parancssorban gépeld be az `ssh felhasználóneved@másik.gép.neve` parancsot (ha csak `ssh másikgép` parancsot adod ki, akkor automatikusan azzal a felhasználónévvel próbál belépni, amelyen éppen be vagy jelentkezve)

A beállításokat a `~/.ssh/config` fájl tartalmazza, meg lehet változtatni pl, hogy melyik gépre milyen felhasználónévvel próbáljon

Példák, leírások

<http://linuxbox.hu/sshkey>

<http://www.inf.bme.hu/hogyan/ssh.html>

<http://www.suso.org/docs/shell/ssh.sdf>

Farbas