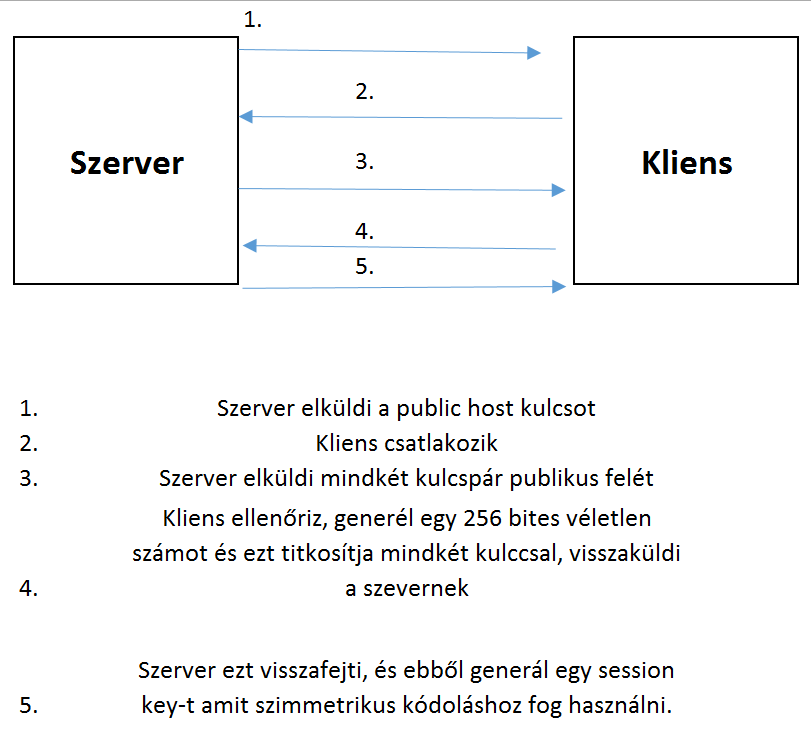
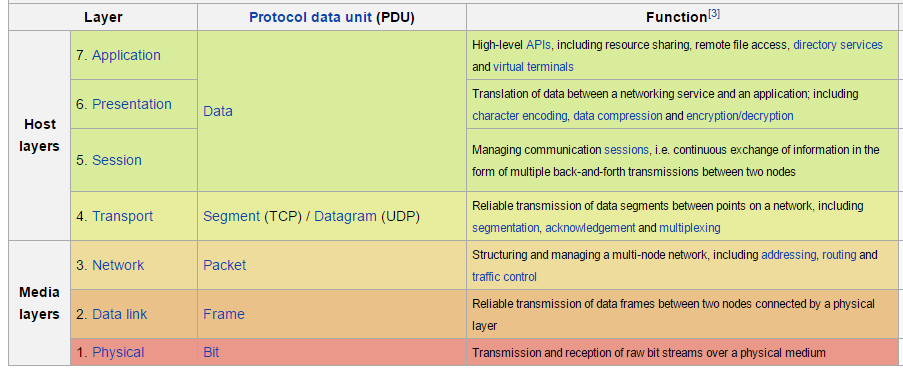
SSH – Secure Shell

**Használata:**

* titkosított hálózati protokoll internetes kommunikációra, egyike a legfontosabb biztonsági eszközöknek
* mi a shell?
  + Parancsértelmező, ugyanazt a feladatot látja el, mint MS-DOS alatt a command.com de sokkal több mindenre képes.
  + Nem része az operációs rendszernek, ez tartja a kapcsolatot az operációs rendszer és a felhasználó között.
  + Minden felhasználó bejelentkezésekor egy parancsértelmező indul el.
  + Szabványos kimenete és bemenete a terminál.
  + Egy promptot jelenít meg, jelezve hogy készen áll a feladatok végrehajtására.
* kódolt csatornát használ kommunikációhoz
* SSH-1 kódolási menete:



* a jelenleg szabványnak számító SSH-2 szintén publikus kulcsot használ a távoli számítógép hitelesítésére, szerver generál egy host kulcspárat melyből a publikussal azonosítja magát a kliens felé, ellentétben az SSH-1el itt nincsen szerver kulcspár, helyette a **Diffie–Hellman kulcscsere-protokollt** használja, mely protokoll két egymástól függő számra épül: egy nagyon nagy „p” prím számra és egy ennél kisebb „g” számra.
* Bővebben: <http://ttmk.nyme.hu/fmkmmk/gab/Documents/SSH-leiras.pdf>.
* nem csak a protokollra de a protokoll megvalósítására való eszköztárra is utal a név
* OSI (Open Systems Interconnection) modell 7. rétegében működik
* (OSI elméleti modell a hálózati kommunikáció működésének vázolására. 7 rétegből áll, a legelső rétege a fizikai réteg, ami az egyes bitek átviteléért felelős. A hetedik rétege már az alkalmazás réteg, ahol az SSH is funkcionál. Az egyes rétegek csak a közvetlenül mellettük elhelyezkedő réteggel kommunikálnak. Így épül fel a legegyszerűbb szintről a legösszetettebbig a hálózati kommunikáció rendszere. )
* A protokollt leginkább a Unix-szerű operációs rendszerek használták, már Windows is.
* Biztonságos parancsértelmező szerverekre való távoli felcsatlakozás és munkavégzéshez (úgy lehet vele munkát végezni, mint ha épp az aktuális távoli számítógép előtt ülnénk), 22-es TCP portot használja
* támogatja a tunnelinget, azaz tetszőleges TCP portok továbbítását; fájlok biztonságos átvitelére is használható a kapcsolódó SFTP (Secure FTP) és SCP (Secure Copy) protokollok segítségével.

**Története:**

* Tatu Ylönen(ülönen) (1995, Helsinki Műszaki Egyetem, Finnország) tervezte az első verzióját – célja volt az addig használatban lévő rlogin, TELNET és rsh protokolok felváltása
* 2000 óta nagyjából 2millió felhasználó élvezhette a protokoll nyújtotta előnyöket
* 1999-ben fejlesztők elérhetővé akartak tenni egy ingyenes verziót így hát visszanyúltak a Shell 1.2.12 verziójához, az utolsó open source verzióhoz és megalkották az OpenSSH-t. – 2005-től ez a legnépszerűbb SSH implementáció.
* 2006 óta az átalakított SSH-2 az elfogadott szabvány amely nem kompatibilis SSH-1el

**Miért jó nekünk?**

* github-ra való feltöltést biztonságos csatornán