# 1. A szoftver létrejöttének okai, céljai, tervezési alapelvei

Rengeteg olyan szoftverrel találkozhatunk a piacon, amely képes virtuális magánhálózatokat létrehozni, valamint amely képes ezen magánhálózatokon belüli számítógépek között fájlmegosztásra és/vagy üzenetváltásra. Habár ezen szoftvereket kiváló biztonsági megoldások jellemzik, azonban van egy alapvető hibájuk. Ezen hiba pedig az, hogy központi szerverrel kezelik a kapcsolatokat, épp ezért az internetszolgáltató által biztosított sávszélességre korlátozza az átvitel sebességét/hatékonyságát. Azonban az otthoni hálózatot gyakran egy router esetleg bridge osztja meg a felhasználók között, amelynek sávszélessége jelentősen nagyobb(mivel kis távolságokat kell összekötni), mint amelyet a szolgáltató biztosít számunkra távolsági kommunikációra. Ezt a sávszélességet célszerű volna kiaknázni. Az otthoni felhasználók azonban nem szoktak rendelkezi szerverrel, épp ezért a kialakítandó architektúra peer-to-peer struktúrát kell kövessen.

További hátránya a piaci szoftvereknek, hogy nem ingyenesek, vagy ha pénzt nem is kell fizetnünk érte, azonban a képességeknek csak egy korlátozott halmazát birtokolhatjuk, azokat is korlátozott mértékben. Ez egy átlagos felhasználó számára kedvezőtlen lehet.

Ezen okokból célunk egy olyan szoftver elkészítése, amely képes mindezen hátrányokat elhárítani, mindeközben nagy hangsúlyt fektetve a biztonságra. A megvalósításban törekedünk az egyszerű kezelhetőségre, illetve automatikus konfigurációra, ezzel is levéve egy terhet a felhasználó válláról.

Adataink védelme rendkívül fontos. Az otthoni hálózat általában vezeték nélküli kapcsolatot biztosít a felhasználók számára. Egy átlagos felhasználó nem rendelkezik alapos informatikai ismeretekkel, és gyakran fordul elő hogy illetéktelen felhasználók a router hatáskörzetében felcsatlakoznak hálózatunkra, mivel az nincsen jelszóval védve. Azonban azt sem érdemes elfelejteni, hogy a Wifi protokollok nem túl biztonságosak, könnyen lehallgathatók illetve néhány elfogott csomagból könnyedén feltörhetők.

Mindezen okok miatt, az adatok küldése során szükséges megfelelő tit-

kosítást alkalmazni. A választás az AES-128 kriptorendszerre esett, mivel manapság ez nagy népszerűségnek örvend, köszönhetően annak, hogy kiválóan párhuzamosítható, amellyel a mai többmagos processzorok esetében jelentős teljesítményjavulást érhetünk el, ezenkívül jelen számítási keretek között feltörhetetlennek bizonyult (brute force módszerrel természetesen ez is törhető).

További problémaként jelentkezik a felhasználók körében, hogy nem szeretnek sokat várni, míg egy-egy fájl átküldésre kerül, illetve azt is szeretik, ha teljes jegyzékeket küldhetnek, anélkül hogy minden egyes fájlt különkülön kellene elküldeniük. Éppen ezért alkalmazni fogunk tömörítési eljárást, amelynek segítségével kisebb adatmennyiséget kellesz mozgatni az egyes gépek között, illetve ezzel elérjük, hogy jegyzékeket is lehessen küldeni. A tömörítési eljárás teljesen automatikus lesz, a fájlok küldése előtt ez meg fog történni, ezzel a felhasználónak nem kellesz törődnie.

Mivel szoftverünket tetszőleges hardver-szoftver architektúrára kívánjuk elkészíteni, így fontos, hogy platformfüggetlen eszközöket használjunk. Épp ezért esett a választásunk a Java nyelvre. A használat során a felhasználónak csupán arra kell ügyelnie, hogy a számítógépén legyen Java futtató környezet. A szoftver minden telepítés és konfigurálás nélkül használható.

Összefoglalva: A szoftverünk egy otthoni hálózati környezetben futó alkalmazás amely képes fájlok és jegyzékek, illetve üzenetek küldésére a hálózat számítógépei között. A küldés során az adatok előbb tömörítésre, majd titkosításra kerülnek, mindezt a felhasználó számára teljesen transzparens módon. A szoftver Java nyelven készül el, telepítésre és konfigurációra nem lesz szükség a futtatáshoz.