AZ ADATREJTÉS ÉS TITKOSÍTÁS TÉMAKÖRÉNEK OKTATÁSI TAPASZTALATAI GÉPÉSZMÉRNÖK SZAKOS HALLGATÓKNÁL

Kiss Gábor
Óbudai Egyetem

Kulcsszavak: adatrejtés, titkosítás, oktatási tapasztalatok

Az informatika alapjai című tárgy keretén belül az egyetemen a hallgatók megismerkednek a történelemben leggyakrabban használt adatrejtési és titkosítási módszerekkel, valamint a mai alkalmazási lehetőségekkel. Ezek nagy részének szemléltetése tábla mellett elég nehézkes, a modern szteganográfiánál lehetetlen. A kép, illetve hang formátumban való információrejtés a táblán megmutathatatlan, csak részben lehet elmagyarázni a működését, ezért szükség van egy multimédiás alkalmazás használatára. A jobb megértést elősegítendő készítettem egy célprogramot, mely segítségével be lehet mutatni a mai szteganográfiai (adatrejtési) módszereket kép, illetve hang fájlok esetében. Ezzel nemcsak teljes egészében mutatható meg az algoritmus, de látható, illetve hallható eredményt is ad amellett, hogy a diákok könnyebben elsajátítják ezeket az ismereteket. A kriptográfia témaköréhez is készítettem alkalmazásokat, melyekkel a történelem során használt fontosabb titkosítási algoritmusok bemutatása, illetve a titkosított adatok visszafejtése lehetségessé válik. Szemléltethető például a cézár-kód használata és feltörésének egyszerűsége. Kipróbálható a monoalfabetikus titkosítás használata és meg lehet kísérelni az ezzel a módszerrel titkosított szöveget visszafejteni. A Vigenére-titkosítást szemléltető program folyamatosan kiemeli, mely sorokat és oszlopokat használjuk a kódolásnál. A Cardano-rács szemléltetéséhez készült programmal készíthető egy megfelelő kialakítású forgatható rács, melynek alkalmazásával lehet a titkosítandó üzenet betűit a megfelelő helyre tenni.

Az általam készített programok hasznosságának megismerésére lehetőséget nyújtott az intézménybe felvett diákok nagy létszáma. A gépész szakos hallgatók számára az előadás két külön csoportban és időpontban zajlott. Az egyik előadáson az oktatás során használtam az elkészített programokat, a másik előadáson ezek használata nélkül tárgyaltam az anyagot. A zárthelyi eredményeket elemezve kiderült, hogy abban a csoportban, ahol a multimédiás programok az előadás részei voltak, a diákok több mint egy jeggyel jobb eredményt értek el átlagosan, szemben azzal a csoporttal, akiknél az említett alkalmazásokat nem használtam a szemléltetés során. A szóráshányados kiszámításával meghatároztam, hogy hány százalékban indokolják az előadáson használt programok a zárthelyin elért eredményt. A kiszámított értékek azt mutatják, hogy az előadáson bemutatott programok körülbelül 32%-ban indokolják a jobb eredmény elérését, mely közepesen erős kapcsolatot jelent. Ennek fényében indokolt ehhez a témakörhöz a multimédiás szemléltetőprogramok használata a tananyag sikeresebb elsajátíttatásának érdekében.