

KRISTÓF ZSOLT – CSAJBÓK ZOLTÁN – TAKÁCS PÉTER –
BODNÁR KÁROLY – DR. KÖDMÖN JÓZSEF

Azonosítón alapuló kriptográfiai rendszerek alkalmazása eLearning környezetben

*Debreceni Egyetem Egészségügyi Kar,
Egészségügyi Informatika Tanszék*
kristofzs@de-efk.hu, csajzo@de-efk.hu, vtp@de-efk.hu,
bcharles@de-efk.hu, kodmonj@de-efk.hu

Az oktatói és hallgatói elektronikus rendszerek fejlődése számos új vonással gazdagodott az elmúlt évtizedben. Az új lehetőségek jelentősen megnövelik az oktatás hatékonyságát. Egyre inkább beépülnek a mindennapi oktatás tevékenységébe, illetve kiszélesítik a tradicionális oktatás formáit. A fejlesztések mindeddig elsősorban a didaktikai, oktatás-módszertani és -szervezési szempontok mentén történtek. Az alkalmazások széles körű elterjedése sürgető igényt vet fel adatvédelmi és adatbiztonsági kérdéseket.

Megoldásra váró feladatok közé tartozik például a jelenleg leggyakrabban használt jelszavas felhasználó azonosítás erősítése vagy alternatív eszközökkel történő helyettesítése és/vagy kiegészítése. Hasonló módon korszerűsítésre vár a hozzáférés védelem és jogosultság kezelés is. Mindezeket túl az eLearning rendszerek számos további korszerű védelmi, biztonsági funkciókkal egészíthetők ki a kriptográfia eszköztárának alkalmazásával – mint például titkos kommunikáció, letagadhatatlanság, adatintegritás stb.

Előadásunkban az utóbb felsorolt funkciók megvalósítására teszünk javaslatot egy új kriptográfiai eszközrendszer, az azonosítón alapuló kriptográfia (Identity Based Cryptography – IBC) alkalmazásával. Röviden vázoljuk az IBC lényegét, bemutatjuk alkalmazási lehetőségeit, előnyeit eLearning, konkrétan az ILIAS keretrendszer környezetben. A bemutatott megoldás természetesen rugalmasan alkalmazható más keretrendszer feltételei között is.

Kulcsszavak: eLearning, ILIAS, adatbiztonság, adatvédelem, azonosítón alapuló kriptográfia