Pécsi Tudományegyetem
Pollack Mihály Műszaki Kar
Villamosmérnöki Szak

A tantárgy címe			**Nyilvántartási kódja**
ALKALMAZOTT KRIPTOGRÁFIA			**PMAUNB790**
Ellenőrzés típusa	**Félév**		**Előfeltétel**
	ősz	**tavasz**	
vizsga		x	MANB926VM
Tantárgy felelős tanszék	**Felelős oktató**		
Automatizálási	Dr. Sárvári Csaba		

A tantárgy heti tanóra száma			**Kredit**
Előadás	Gyakorlat	Labor	
2	2	0	4

A tárgy oktatásának célja

Az alkalmazott kriptográfia alapvető fogalmainak, eljárásainak megismerése. A titkosítási rendszerek alapjául szolgáló algebrai-, számelméleti ismeretek jártasság szintű ismerete.

A foglalkozáson való részvétel követelményei és a távolmaradás pótlása

A foglalkozásokon való részvételt a TVSZ 126§ szabályozza.
Távollét pótlására általában nincs lehetőség, a tananyag pótlásáról a hallgatónak kell gondoskodnia.
Az előadásokon, gyakorlatokon, gyakorlati számonkéréseken való részvétel kötelező.

Igazolás módja

Foglakozások:	**Vizsga:**
Hivatalos okmánnyal, hét napon belül.	-

Félévközi ellenőrzések:

Témaköre:	**Időpontja:**	**Pótlása és javítása:**
1-6. hét tananyaga	7. héten	15. héten
7-13. hét tananyaga	14. héten	15. héten

Egyéni munkával megoldható feladatok	
Típusa: Házi feladatok	**Kritériuma:** A tárgy teljesítésének szükséges feltétele a házi feladatok elkészítése, határidőre történő beadása.

Kritériumkövetelmények és teljesítésük határideje

A hallgatók felkészültségükről gyakorlati ZH keretében adnak számot a gyakorlatokon.
Aláírás
Feltétele a foglalkozásokon való részvétel és a félévközi ellenőrzéseken, témakörönként elért 40%-os teljesítmény.

Az érdemjegy kialakításának módja vizsgakövetelmények

Vizsga: Értékelése a félévközi ellenőrzések és a vizsgán mutatott teljesítmény 50%-50% arányú figyelembevételével történik. A vizsgán mutatott minimális teljesítménynek meg kell felelnie az 50%-os szintnek.	50%	elégséges
	65%	közepes
	80%	jó
	90%	jeles

Pótlási lehetőség

Aláírás:
A vizsgaidőszak első hetében egy alkalommal.
Vizsga:
TVSZ szerint.

Felhasználható jegyzet, segédlet, szakirodalom

Jegyzet, tankönyv, ajánlott irodalom:

Buttyán-Vajda: Kriptográfia és alkalmazásai, Typotex 2004.

Ködmön József: Kriptográfia, ComputerBooks 1999/2000.

Virrasztó Tamás: Titkosítás és adatrejtés, NetAkademia Kft. 2004.

Simon Singh: Kódkönyv, A rejtjelezés és rejtjelfejtés története, Park Könyvkiadó, 2001

Maróti György: Előadások algoritmikus számelméletből, Livermore 2008.

Cryptography with Coding Theory, by Trappe and Washington (second edition, ISBN-13: 978-0131862395)

Felhasználható fontosabb segédeszközök

A zárthelyi dolgozatok írásakor a feladatok egy részét a Maple számítógépes algebrai rendszer használatával oldják meg a kurzus résztvevői.

A tantárgy tananyagának leírása

Kritográfiai alapfogalmak, Kerckhoffs elvek, kriptográfia és biztonság, titkosítási rendszerekkel szembeni követelmények.

Néhány példa a történelemből (Caesar módszere, affin titkosító, helyettesítő és keverő titkosítók, Vigenére titkosító, egyéb módszerek, az Enigma és a Hagelin), titkosítási rendszerek generációi.

Kriptoanalízis, támadásfajták, a fenti módszerek feltörése, az egyszeri hozzáadásos módszer (OTP, avagy Vernam titkosító), tökéletes titkosság (perfect secrecy), a módszer hátrányai, véletlen és álvéletlen sorozatok, blokktitkosítók és folyamtitkosítók.

Szimmetrikus kulcsú módszerek: a szimmetrikus titkosítás modellje, helyettesítő-keverő hálózatok az AES pályázat, AES (Rijndael).

Nyilvános kulcsú módszerek: a kulcselosztás problémája, háromutas kulcsforgalom, Diffie-Hellman kulcscsere, a nyilvános kulcsú titkosítás modellje, a faktorizálás problémája, az RSA, RSA kulcsgenerálás, megfelelő prímek választása, támadások az RSA ellen.

A titkos és nyilvános kulcsú módszerek összevetése, PGP.

Digitális aláírások, hitelességi bizonyítványok, üzenetpecsétek, adatrejtés (szteganográfia), titokmegosztás..

Heti bontású tematika

1. Kriptográfiai alapfogalmak.
2-3. Klasszikus titkosítások
4-5. Matematikai alapok
6-7. A DES az AES
8-9. Nyilvános kulcsú kriptográfia. Az RSA
10-11. A titkos és nyilvános kulcsú módszerek összevetése, PGP.
12-13. Hitelesítés, digitális aláírás