

## Tárgytematika / Course Description

### Kódoláselemélet

LGM\_TA008\_1

**Tárgyfelelős neve /**

**Teacher's name:** dr. Nagy Szilvia

**Félév / Semester:** 2016/17/2

**Beszámolási forma /**

**Assesment:** Vizsga

**Tárgy heti óraszám /**

**Teaching hours(week):** 0/0/0

**Tárgy féléves óraszám /**

**Teaching hours(sem.):** 15/0/0

---

### OKTATÁS CÉLJA / AIM OF THE COURSE

#### Célkitűzés:

A hallgatók megismertetése a mai távközlési és ipari kommunikációs rendszerekben használt digitális adatátviteli módszerekkel és a hozzájuk kifejlesztett kódolási és titkosítási eljárásokkal.

---

### TANTÁRGY TARTALMA / DESCRIPTION

#### Rövid tartalom:

Forráskódolás előírt hibavalószínűséggel. Hűségkritérium.

Transzformációs és prediktív kódolások.

A különböző hírközlési csatornákon való adatátvitel. Analóg moduláció.

Digitális jelátvitel alapjai réz érpáron, optikai szálakon és rádióhullámokkal: PCM, impulzus-amplitúdómoduláció, QAM, PSK, FSK, APSK. Órajel, fazorábrák, demoduláció, a digitális jelátvitel zajtűrése.

Csatornaosztás réz érpáron, optikai szálakon és rádiófrekvenciás közegben: idő-, frekvencia- és kódosztás, hullámhosszosztásos nyalábolás. Keretidő, csatornaidőérés, bitidőérés, PCM rendszerek kódolásai.

Alapvető kommunikációs- és hibamodellek. A hibajavító kódolás valószínűségi alapjai, csatornák, ideális megfigyelő, dekódolás, döntési sémák, döntési hibák. Javítható hibák, kódkorlátok, a hibajavító kódok optimalása.

A blokk-kódok alapvető paraméterei, ekvivalens kódok, szisztematikus kódok. A véges testek aritmetikájának rövid áttekintése, polinomgyűrű véges testek felett. Lineáris kódok. Szindrómákon alapuló dekódolás, hibacsapda-dekódolás.

Ciklikus kódolás alaptételei és alapfogalmai. Ciklikus kódok, mint ideálok véges számtesteken. Ciklikus kódok duálisa. Ciklikus kódok hibajavító dekódolása. BCH-kódok és dekódolásuk, Berlekamp-algoritmus. A Reed—Solomon-kódok generálása inverz diszkrét Fourier-transzformációval, transzformációs kódolás és dekódolás.

Kódkombinációk, kódátfüzés, szorzatkódok, kaszkád-kódok, kódmódosítások.

Konvolúciós és rekurzív konvolúciós kódolók, turbó kódolók. Viterbi-algoritmus bithiba-aránya, turbó kódok dekódolása, teljesítménye.

Algoritmikus adatbiztonság alapfogalmai, titkosság, hitelesség, hozzáférés-védelem, rejtjelezés. Feltétel nélküli

biztonságos rejtjelezés és hitelesítés fogalma. Szimmetrikus kulcsú blokk-rejtjelezők.

RSA-algoritmus, paraméterek, prímszámok szerepe, számok faktorizációja, feltörhetőség, a feltöréshez szükséges idő. Az RSA-algoritmus biztonsága, alkalmazási köre. Elliptikus görbe kriptográfia.

Kriptográfiai hash-függvények, típusok, biztonsági jellemzők. Kriptográfiai protokollok, a blokkrejtjelezés módjai, az üzenethitelesítési, digitális aláírási és partnerhitelesítési sémák és modellek, támadások osztályozása. Kulcscsere-protokollok.

Kriptográfia a gyakorlatban: az internet, a mobil távközlés és az elektronikus fizetés biztonsága, protokolljai.

---

## **SZÁMONKÉRÉSI ÉS ÉRTÉKELÉSI RENDSZERE / ASSESSMENT'S METHOD**

### **Számonkérés:**

Az aláírás feltétele: a kiadott házi feladat (egy tanult, egyeztetett kód programozása tetszőleges nyelven, tetszőleges vivőre) leadása a szorgalmi időszakban.

Vizsga: szóbeli, tételjegyzékkel. A vizsga kiváltható kiselőadás tartásával, melyért a hallgató az előadás minőségétől és tartalmától függő megajánlott jegyet kap.

---

## **KÖTELEZŐ IRODALOM / OBLIGATORY MATERIAL**

### **Kötelező irodalom:**

Györfi L., Györi S., Vajda I.: Információ és kódelmélet, Typotex, Budapest, 2005.

Buttyán L., Vajda I.: Kriptográfia és alkalmazásai, Typotex, Budapest, 2004.

### **Ajánlott irodalom:**

-

MacWilliams, F. J., Sloane, N. J. A.: The Theory of Error-Correcting Codes, New York: Elsevier, 1978.

van Lint, J. H.: An Introduction to Coding Theory, 2nd ed., New York: Springer-Verlag, 1992.

Jones, Gareth A., Jones, J. M.: Information and Coding Theory, London: Springer-Verlag, 2000.

Berlekamp, E. R.: Algebraic Coding Theory, rev. ed., New York: McGraw-Hill, 1968.

Lakatos Piroska: Algebrai kódelmélet (egyetemi jegyzet), Debreceni Egyetem Matematikai Intézet, 1999.