Název předmětu: **Šifrování, kódování a jejich aplikace**
(platné pro ak. rok 2018/19)

Zkratka předmětu: SKA

Počet kreditů: 6 Forma studia: kombinovaná

Způsob ukončení: zkouška (písemná a ústní část)

Zápočet

- Student vypracuje zápočtový test – zadání viz níže. Řešení úloh musí být správné a dostatečně podrobně komentované. Formální stránka zpracování musí odpovídat studentu VŠ, obor informatika.
- Vyřešené úlohy je třeba zaslat elektronickou poštou na univerzitní adresu přednášejícího ve formě jednoho souboru (v některém z formátů - doc, docx, rtf, pdf; velikost max. 2 MB), a to nejpozději do konce zkouškového období ZS ak. roku 2018/19.
- O výsledku zápočtu bude student informován mailem do čtyř pracovních dnů od doručení řešení zápočtových úloh.

Zkouška

- Student s platným zápočtem se hlásí na zkoušku prostřednictvím systému stag. Zkušební termíny budou uveřejněny ve stagu nejpozději v zápočtovém týdnu ZS ak. roku 2018/19.
- Zkouška má písemnou a ústní část. K ústní části postoupí pouze student, který uspěl v písemné části (tj. získá alespoň 70 % bodů z celkového možného počtu).

20. října 2018

doc. RNDr. Miroslav Koucký, CSc.
garant, přednášející

Předpokládané znalosti

(získané v rámci předchozího Bc. studia)

- Abeceda, slovo, jazyk, délka slova, zřetězení, prefix.
- Grupy $(Z_m, +)$, $(Z_m^*, \cdot)$, $(S_n, \cdot)$; cyklické grupy; Lagrangeova věta; konečná tělesa $GF(p^k)$; polynomy nad tělesy Z_p.

Obsah samostudia

Vektorový prostor Z_2^n nad tělesem Z_2

- lineární kombinace, lineární obal, lineární (ne)závislost, hodnost matice, REF, RREF, dimenze, báze; Hammingova vzdálenost/váha.

Kódování - komprese (ztrátová, bezeztrátová), detekční/opravné

- základní pojmy, Kraftová nerovnost, McMillanova věta, důsledek (prefixové kódy stejně obecné jako všechny jednoznačně dekódovatelné kódy).

Obsah prezenční části výuky

1. **blok prezenční části výuky** (5. 10. 2018, 10:40-15:05)
   Informace o předmětu (podmínky získání zápočtu, průběh zkoušky), předpokládané znalosti, obsah samostudia.

   Úvod do šifrování
   - základní pojmy (kryptologie = kryptografie + kryptoanalýza; steganografie), základní pojmy (šifrovací systém/schéma); klasifikace šifrovacích metod (symetrické × asymetrické; transpozice × substituce; monoalfabetické × homofonní × polyalfabetické);
   - jednoduchá transpozice, jednoduchá substituce, afinní šifra, Hillova šifra, Vigenèrova šifra);
   - blokové šifry - Vernam, Feistel;
   - metoda RSA.

2. **blok prezenční části výuky** (26. 10. 2018, 8:50-13:15)
   - hash funkce (vlastnosti, typy), jednosměrná (se zadními vrátky) funkce;
   - digitální podpis, certifikát veřejného klíče, certifikační autorita; problém výměny šifrovacích klíčů (Diffie-Hellman, odolnost proti aktivnímu/pasivnímu protivníkovi);

Základy bezeztrátové komprese

- nejkratší kód, Huffmanova konstrukce nejkratšího kódu (binární + *n*-ární případ);
- konstrukce standardizovaného Huffmanova kódu (jednoznačnost kódu);

Aritmetické kódy - metoda DFWLD (kódování, dekódování); dyadické zlomky (konstrukce);

Adaptivní metody (Huffman – kódování/dekódování);

Slovníkové metody - LZ77;

3. **blok prezenční části výuky** (30. 11. 2018, 8:50-13:15)

Detekční/opravné kódy

- základní pojmy, detekce chyb, chybové slovo, kód detekuje/opravuje *t*-násobné chyby, BSC (Binary Symmetric Channel); dekódování - opravování chyb (strategie MLD (CMLD/IMLD))

Lineární binární kódy

- definice (n, k); (n, k, d)- kódu, základní vlastnosti a pojmy (informační/kontrolní znaky, systematický kód, ekvivalence kódů, počet slov), min. vzdálenost $d = \min\{w(\boldsymbol{x}) | \boldsymbol{x} \in K - \{\mathbf{0}\}\}$, kód generovaný množinou slov *S* (lineární obal: $K = \langle S \rangle$), duální kód $K^{\perp}$;
- generující matice G, vlastnosti; kontrolní matice H, vlastnosti, vztah mezi G, H;
- rozklad ${}^{Z_2}/_{K}$, základní vlastnosti tříd rozkladů $\boldsymbol{e_i} + K$ (všechna slova z jedné třídy stejný syndrom) počet tříd rozkladů, jejich mohutnost; standardní dekódování; zásady volby chybových slov $\boldsymbol{e_i}$; nevýhody standardního dekódování;
- Základní nerovnosti (Hammingův, Singletonův, Gilbert-Varshamovův odhad), využití;
- Rozšířený kód, definice, vlastnosti, tvar G^*, H^*;

4. <u>blok prezenční části výuky</u> (14. 12. 2018, 8:50-13:15)

Perfektní kódy, definice, existenční věta, vlastnosti (perfektní pro opravy *t*-násobných chyb).

- Hammingův kód, dekódování.
- Golayův kód, vlastnosti, dekódování; rozšířený Golayův kód, vlastnosti, dekódování
- Reed-Mullerovy kódy R(r,m), rekurentní definice kódu i generující matice G(r,m), vlastnosti, dekódování RM(1,m)

Cyklické kódy

- základní pojmy: cyklický posun slova, polynomiální reprezentace slov, věta o dělení polynomů se zbytkem, $f(x) \equiv g(x)\ mod\ q(x);\ f(x) = \big(g(x)\ mod\ q(x)\big)$
- definice cyklického kódu, generující polynom; informační polynom, kontrolní polynom, syndrom;

<u>Doporučená literatura</u> (dostupná na vyžádání u přednášejícího)

Menezes, Oorschot, Vanstone: Handbook of applied cryptography. CRC Press

Hankerson, Hoffman: Coding theory and cryptography: the essentials. Marcel Dekker

Hankerson, Harris, Johnson: Introduction to Information Theory and Data Compression. CRC Press

Odstavec 3.2 Transition probabilities and binary symmetric channels (str. 50);
Odstavce 4.1 Encoding and decoding (str. 71 – 74)
Odstavce 4.2 Prefix-condition codes and the Kraft-McMillan inequality (str. 75 – 78)
Odstavec 4.3 Average code word length and Huffman's algorithm (str. 79 – 83)
Kapitola 5 Lossless Data Compression by Replacement Schemes (str. 119 – 124, 131 – 133)
Kapitola 6 Arithmetic Coding (str. 141 – 145, 150 – 153)
Odstavec 8.1 Adaptive Huffman encoding (str. 206 – 208)
Odstavec 9.1 LZ77 (sliding window) schemes (str. 229 – 233)

Koucký, M.: Matematika pro informatiky I/II, Skripta TUL, 2017 (elektronicky)