11Y2KK – Kódování a základy kryptografie

Okruhy k zápočtu pro ZS 2013/2014

Lucie Kárná
Jan Přikryl

31. ledna 2014

Témata, na něž se můžeme ptát při zápočtu:

1. Základy teorie informace. Sdělovací kanály, sum. Entropie. Binární symetrický kanál. Pravděpodobnost nezachycené (zbytkové) chyby.

2. Algebraická tělesa. Vlastnosti. Tělesa Z_p. Charakteristika, řád prvku, primitivní prvek, minimální polynom. Diskrétní logaritmus. Galoisova tělesa.

3. Kódování zpráv. Základní pojmy – abeceda, zpráva, kód, kódování, dekódování. Prefixové kódy. Blokové kódy. Informační poměr, redundance. Informační a kontrolní znaky. Systematické kódování.

4. Bezpečnostní kódy. Objevování a opravování chyb. Hammingova vzdálenost, minimální vzdálenost. Shluky chyb. Lineární kódy. Generující a kontrolní matice.

5. Polynomy, okruhy polynomů, kořeny, ireducibilita. Cyklické kódy. Generující a kontrolní polynom. Generující kořeny.

6. Konstrukce kódů. Rozšíření, zúžení, zvětšení, zmenšení, direktní součin, direktní součet, prokládání. Některé praktické aspekty. Volba vhodného kódování. Příklady kódů použitých v praxi.

7. Kódy pro kompresi dat. Huffmanovo kódování. Shannon-Fanovo kódování, aritmetické kódování (zmínka). Slovníkové metody komprese dat (pro informaci a srovnání, pouze stručná zmínka). Používané programy pro kompresi dat (zmínka, případně použité kódování).

8. Jemný úvod do kryptografie: Jednoduchá záměna, transpozice, knižní šifry. Enigma, kód Navaho. Symetrické a asymetrické šifry. Blokové šifry, proudové šifry.

9. Diskrétní matematika (okrajově, pro informaci doporučujeme stránky předmětu 11MAG). Prvočísla. Faktorizace. Modulární aritmetika. Čínská věta o zbytcích. Malá Fermatova věta. Eulerova věta. Totient.

10. Symetrická kryptografie: Blokové šifry. Operační módy. S-boxy, P-boxy, zásady návrhu. Feistelovská síť. Substitučně-permutační síť. DES a popis jeho šifrování a dešifrování. AES a popis jeho šifrování, dovolená délka bloku a klíče, popis rundy, specifika Rinjdaelovského tělesa.

11. Asymetrická kryptografie: RSA. Diffie-Hellmanova výměna klíčů pro symetrické šifry.