

Elektrotechnika a informatika - magisterské studium FM TUL

(dvouleté)

Studijní předmět

Název: Kódování a šifrování
Zkratka: KOS
Typ: povinně volitelný pro obory: AŘ, IT
Rozsah: 14 týdnů, týdně 2 hodiny přednášek + 2 hodiny seminárních cvičení
Kredity: 5
Způsob ukončení: zkouška

Katedra: katedra softwarového inženýrství FM TUL
Přednášející: Ing. Jaroslav Buchta

Stručná anotace předmětu:

Předmět seznamuje studenty se základními postupy a algoritmy pro získání, přenos a archivaci dat. Podrobně jsou rozebrány obecné principy lineárních kódů, základních bezpečnostních kódů, algoritmy pro kompresi dat, princip šifrování a standardní symetrické a asymetrické šifrovací algoritmy. Studenti provádějí v rámci cvičení praktickou realizaci vybraných algoritmů.

Získané kompetence:

Studenti získají základní vědomosti pro realizaci vlastních řešení datové komunikace, zejména na úrovni jednoduchých řídicích systémů a mikrokontrolérů.

Témata přednášek:

Přenos a archivace dat, definice kódování, vlastnosti a klasifikace kódů, kritérium dekódovatelnosti, minimální kódy, bezpečnostní kódy, redundance dat.

Zabezpečení dat paritou, lineární kódy, cyklické kódy. Konkrétní algoritmus kódování dat prostřednictvím Hammingova kódu.

Principy komprese dat, Huffmanův minimální kód, statický a dynamický model, základní princip některého z používaných kompresních algoritmů.

Kryptografie, všeobecná pravidla, definice kryptografických systémů, Charakteristika symetrických a nesymetrických šifrovacích algoritmů.

Základní principy symetrických kryptografických systémů. Schéma a princip šifrování prostřednictvím algoritmu DES. Přehled vlastností dalších v současnosti používaných symetrických šifrovacích algoritmů.

Základní principy nesymetrických kryptografických systémů s veřejným klíčem, princip a vlastnosti šifrovacího algoritmu RSA, přehled a vlastnosti dalších nesymetrických algoritmů.

Transformační funkce (hash), princip elektronického podpisu a certifikátu.

Náplň cvičení:

Realizace algoritmu komprese datového souboru prostřednictvím Huffmanova minimálního kódu se statickou kódovací tabulkou.

Modifikace kompresního algoritmu pro dynamickou kódovací tabulku Huffmanova kódu, porovnání účinnosti komprese oproti statické verzi při různých typech datových souborů.

Realizace nesymetrického šifrovacího algoritmu RSA.

Literatura:

Grošek O., Porubský Š.: Šifrování. Grada, 1992
Černý Ján: Entropia a informácia v kybernetike. Alfa, 1981
Adámek: Kódování, SNTL Praha, 1969
Adámek: Kódování a teorie informace, ČVUT Praha, 1991.

Prerekvizity: -

Navazující: -

Datum poslední změny: 26.8.2005