

D – Charakteristika studijního předmětu				
Název studijního předmětu	Kódování a šifrování			
Typ předmětu	povinný		doporučený ročník / semestr	1/Z
Rozsah studijního předmětu	2 + 2	hod. za týden	4	kreditů 5
Jiný způsob vyjádření rozsahu	—			
Způsob zakončení	zkouška		Forma výuky	př + cv
Další požadavky na studenta	Účast na cvičeních. Realizace zadané samostatné práce. Zkouška je písemná a ústní.			
Vyučující	doc. Ing. Jiřina Královcová, Ph.D.			
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.			
Témata přednášek:	<ol style="list-style-type: none">1. Přenos a archivace dat, definice kódování, vlastnosti a klasifikace kódů2. Kritérium dekódovatelnosti, princip lineárních kódů3. Minimální kódy, Huffmanův kód, princip kompresních algoritmů4. Bezpečnostní kódy, Princip dekódování a korekce chyb5. Redundance dat, zabezpečení dat paritou, repetiční kódy6. Cyklické kódy.7. Hammingův bezpečnostní kód, rozšířený Hammingův kód8. Kryptografie, všeobecná pravidla, definice kryptografických systémů9. Symetrické a asymetrické šifrovací algoritmy10. Symetrické šifrovací algoritmy, DES, SkipJack, princip zřetězení bloků, předávání klíčů11. Šifrovací algoritmy s veřejným klíčem, princip algoritmu RSA12. Šifrovací algoritmy s veřejným klíčem, princip algoritmu RSA13. Hash funkce, aplikace, princip elektronického podpisu a certifikátu14. Hash funkce, aplikace, princip elektronického podpisu a certifikátu			
Informace ke kombinované nebo distanční formě				
Rozsah konzultací (soustředění)		hodin za týden		
Rozsah a obsahové zaměření individuálních prací studentů a způsob kontroly				
Studijní literatura a studijní pomůcky				
GROŠEK, Otokar. <i>Šifrování: Algoritmy, metody, prax.</i> Praha: Grada, 1992, 268 s. ISBN 80-85424-62-2.				
ČAPEK, Jan a Peter FABIÁN. <i>Komprimace dat: principy a praxe.</i> Vyd. 1. Praha: Computer Press, 2000, viii, 173 s. Internet. ISBN 80-7226-231-9.				
ADÁMEK J. <i>Kódování.</i> SNTL, Praha, 1989.				