

D – Charakteristika studijního předmětu				
Název studijního předmětu	Diskrétní matematika			
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				
Aktivní účast na cvičeních, zápočet, znalosti odpovídající sylabu. Zkouška je písemná a ústní.				
Vyučující				
doc. RNDr. Miroslav Koucký, CSc.				
Stručná anotace předmětu				
Předmět je úvodem do vybraných partií diskrétní matematiky. Seznamuje zejména se základy teorie dělitelnosti, algebry a vybranými metodami šifrování a kódování.				
Témata přednášek:				
1.–4. Základy teorie dělitelnosti. Počítání v Z_n , Eulerova a Möbiova funkce, Fermatova věta. Řetězové zlomky. Prvočísla, prvočíselné rozklady, Fermatova a Mersenova čísla. Kongruence, řešení kongruencí 1. stupně a jejich soustav, aplikace.				
5.–9. Základní algebraické struktury. Grupa, normální podgrupa, Lagrangeova věta. Abelovy grupy, cyklické grupy. Symetrická grupa. Okruh, eukleidovské obory integrity, okruhy polynomů, ireducibilita, konečná tělesa.				
10.–14. Vybrané aplikace v oblasti šifrování a kódování. Substituce, transpozice, blokové šifry, Feistel, DES. Asymetrické metody šifrování, RSA. Kraftova nerovnost, Huffmanova konstrukce nejkratšího kódu. Aritmetické kódy, metoda DFWLD. Adaptivní metody. Lineární kódy, Hammingův kód, cyklické kódy.				
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				
HANKERSON, Darrel. <i>Coding theory and cryptography: the essentials</i> . 2nd ed., rev. and expanded. New York: M. Dekker, c2000, x, 350 p. ISBN 0824704657.				
HANKERSON, Darrel, Grag HARRIS, Peter JOHNSON. <i>Introduction to information theory and data compression</i> . Boca Raton: CRC Press, c1998, xi, 332 p. ISBN 0849339855.				
KOUCKÝ, Miroslav. <i>Diskrétní matematika II</i> . Vyd. 1. Liberec: Technická univerzita, 2003. ISBN 8070837160.				
KOUCKÝ, Miroslav. <i>Sbírka příkladů z diskrétní matematiky</i> . Vyd. 1. Liberec: Technická univerzita, 2003. ISBN 8070837179.				
MATOUŠEK, Jiří a Jaroslav NESETRIL. <i>Kapitoly z diskrétní matematiky</i> . 4. upr. a dopl. vyd. Praha: Karolinum, 2009, 442 s. ISBN 9788024617404.				
STANOVSKÝ, David. <i>Základy algebry</i> . 1. vyd. Praha: Matfyzpress, 2010. ISBN 9788073781057.				