Da - Přehled předmětů nabízených k vytvoření studijních plánů a návrh témat prací					
Vysoká škola	Univerzita Karlova v Praze				
Součást vysoké školy	Matematicko-fyzikální fakulta				
Název studijního programu	Matematika (Mgr. navazující)				
Název studijního oboru	Matematické metody informační bezpečnosti				
Název předmětu	**rozsah**	**způsob zak.**	**druh před.**	**přednášející**	**dopor. roč.**
Teoretická kryptografie	4p+2c	Z, Zk	p	dr. Šedivý	1.
Aplikovaná kryptografie I	2p	Zk	p	Kadlčáková	1.
Aplikovaná kryptografie II	2p	Zk	p	Kadlčáková	1.
Datové a procesní modely	4p+2c	Z, Zk	p	doc. Souček	1.
Eliptické křivky	4p	Zk	p	doc. Drápal	1.
Standardy v kryptografii	2p	Zk	p	Vondruška	1.
Faktorizace velkých čísel	2p	Zk	pv	doc. Drápal	
Aplikace bezpeč. mechanismů	2p	Zk	pv	Beneš	
Kryptoanalytické útoky	2p	Zk	pv	doc. Tůma	
Úvod do teorie grup	2p+2c	Zk	pv	prof. Kepka	
Členění kryptograf. standardů	4p	Zk	p	Vondruška	2.
Právní aspekty bezpečnosti dat	2p	Zk	pv	doc. Tůma	
Kryptografické protokoly	2p	Zk	pv	Vondruška	
Teorie čísel a RSA	2p+2c	Z, Zk	v	doc. Drápal	
Algebraická geometrie v kladné charakteristice	4p	Zk	v	Somberg	
Další povinnosti / odb. praxe					
Návrh témat prací	Rozklady velkých čísel metodou kvadratických sít. Kryptosystémy založené na pletencové grupě. Aplikace bezpečnostních mechanismů. Útoky na hashovaci funkce. Postranní kanály.				
Návaznost na další stud. prog.	Tento obor navazuje na Bc. stud. program matematika. Lze pokračovat v doktorském studijním programu matematika.				