Operační program Vzdělávání pro konkurenceschopnost
Globální grant: CZ.1.07/1.3.05 - Další vzdělávání pracovníků škol a školských zařízení
Modulový systém dalšího vzdělávání pracovníků škol a školských zařízení v Moravskoslezském kraji

Název kurzu	Kódy a šifry - jejich matematický základ a historie
Kód kurzu	M2.3.1
Zahájení	ZS 2009
Organizační jednotka	Centrum celoživotního vzdělávání na Přírodovědecké fakultě
Cílová skupina	Pracovníci škol a školských zařízení v MSK
Cena	Tento projekt je spolufinancován Evropským sociálním fondem a státním rozpočtem ČR. Kurz je pro pedagogické pracovníky škol a školských zařízení MSK bezplatný.
Forma	Prezenční výuka kombinovaná s distanční (výukové materiály v prostředí Moodle).
Organizace kurzu	Prezenční výuka probíhá v budově Ostravské univerzity (ul. 30. dubna 22 nebo v učebně, která bude účastníkům před zahájením kurzu upřesněna). Kurz je v rozsahu 30 hodin, prezenční část – minimálně 15 hodin výuky. Kurz bude otevřen při minimálním počtu 15 účastníků. Materiály, připravené jednotlivými vyučujícími (pro prezenční formu kombinovanou s distanční), jsou poskytovány účastníkům následujícími způsoby: • Na prezenčních hodinách výuky probíhá výuka standardním způsobem s využitím textových materiálů, které jsou připraveny vyučujícím. • Materiály v elektronické podobě jsou navíc pro účastníky kurzů umístěny v LMS Moodle. Všem účastníkům je do daného kurzu zaveden přístup – jméno a heslo, takže

	mohou využívat ke studiu další materiály, které jsou v systému umístěny, včetně toho, že je využita komunikace mezi účastníky navzájem (diskusní fórum) a mezi učitelem. • Struktura kurzů je v LMS Moodle je navržena pro všechny kurzy tak, aby účastníci, kteří absolvují jeden kurz již v dalších kurzech přesně věděli jak se mohou v kurzu orientovat apod. • Učitel/lektor umisťuje do systému rovněž úkoly, které účastníci v rámci kurzu samostatně řeší. Lektor může průběžně zpracované úkoly vyhodnocovat a na další prezenční výuce se řeší připomínky, chyby, návrhy. • Účastníkům kurzů je rovněž nabídnut seznam doporučené a rozšiřující literatury, kterou mohou ke studiu daného kurzu využít.
Číslo akreditace DVPP	22 993/2007-25-434
Garantující odborná katedra	Centrum CŽV
Garant kurzu	RNDr. Petra Konečná, Ph.D.
Anotace	Kurz uvede účastníky do problematiky kódů a šifer. Tématicky jej lze rozdělit do dvou základních oblastí, kódování a kryptologie. V části kódování se účastníci seznámí, jak převést informace do lépe přenositelné formy, při dodržení dalších požadavků na úspornost či bezpečnost přenášené informace. Dále je kurz věnován problematice kryptologie, která je rozdělena na oblast kryptografie a kryptoanalýzy.
Způsob ukončení studia	
Výstupní doklad	Osvědčení o absolvování kurzu
Předpoklady pro přijetí	Včas a řádně podaná přihláška a včasná komunikace mailem – odpověď na zařazení do kurzu. Potvrzení účasti v kurzu.
Přihlášky	http://projekty.osu.cz/projekt-dvpp/esf/prihlaska.doc
Uzávěrka přihlášek	
Kontakt/další informace	Gabriela.burianova@osu.cz
Vyučující	RNDr. Petra Konečná, Ph.D., Mgr. Wrublová, Mgr. Vavříčková

Plán studia / rámcový harmonogram	**Téma**	**Počet hodin**
	Úvod do kódování kód a kódování, dekódování, kdy je dekódování jednoznačně dekódovatelné	2
	Úvod do kryptologie kryptologie, kryptografie, šifrování, stenografie, pojem otevřený text a šifra, kryptoanalýza a dešifrování	2
	Šifry a jejich historie transpoziční šifry, monoalfabetické, polyalfabetické substituční šifry, frekvenční analýza jako metoda dešifrování, absolutně bezpečná šifra, šifrovací stroje	3
	Veřejný klíč a systém RSA asymetrické šifry, veřejný klíč, jak funguje systém RSA	2
	Obecné vlastnosti kódů délka kódu, blokové kódy, kódy s proměnlivou délkou, optimální kódy a jejich konstrukce	3
	Bezpečnostní kódy – obecná charakteristika a základní vlastnosti	2
	Lineární kódy – algebraický základ, vlastnosti, generující a kontrolní matice	2
	Cyklické kódy – algebraický základ, generující a kontrolní polynom	2
	Perfektní kódy – vlastnosti, Hamningovy kódy, Golayův kód	2