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	Základy kryptografie
Kód kurzu	M2.4.33
Zahájení	2011
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	21 252/2009-25-417
Garantující odborná katedra	Centrum CŽV
Garant kurzu	Ing. Pavel Smolka
Anotace	Kurz nabízí základy problematiky kryptografie. Seznamuje účastníky se základními koncepty šifrovacích systémů, popisuje historické šifrovací algoritmy a objasňuje moderní šifrovací algoritmy. V úvodu kurzu budou účastníci seznámeni se základními matematickými základy, potřebnými pro objasnění algoritmů šifrování. V dalších částech budou prezentovány konkrétní příklady šifrovacích algoritmů. Na závěr budou diskutovány různé možnosti praktického využití kryptografie v běžném životě a pro potřeby ve výuce na středních případně základních školách.
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	Ing. Pavel Smolka

Plán studia / rámcový harmonogram	**Téma**	**Počet hodin prezenční**	**Počet hodin distanční**
	Seznámení s obsahem kurzu, zopakování matematických základů, potřebných pro objasnění algoritmů šifrování.	4	-
	Historické algoritmy, jednoduché příklady šifrování	1	3
	Moderní algoritmy šifrování	1	3
	Šifrování s veřejnými klíči – metoda RSA	1	3
	Kryptografie v bezpečnosti informačních systémů	2	1
	Využití kryptografie	2	1
	Ukázky kryptografických aplikací z běžného života a prezentace praktického využití ve výuce, diskuse	4	4
	Celkem	**15**	**15**