

Příloha č. 6 k č.j.: MV-152399-7/VZ-2014

Počet listů: 2

Specifikace Části 6 Principy šifrování a hashů, ale i praktické vyzkoušení jejich implementací v reálných aplikacích a serverových řešeních

**v rámci veřejné zakázky „ Školení v oblasti IT pro forenzní zkoumání “
/projekt „ Efektivní rozvoj a posilování kompetencí lidských zdrojů “ (ERP),
reg. č. CZ.1.04/4.1.00/A3.00005/**

Název kurzu	Principy šifrování a hashů, ale i praktické vyzkoušení jejich implementací v reálných aplikacích a serverových řešeních
Obecná specifikace kurzu	V kurzu se proškolené osoby naučí principům a implementacím šifrovacích metod (např. monoalfabetická substituční šifra, cézarova šifra, Atbaš, ROT13, Vigenérova šifra, ADFGVX šifra, Playfairova šifra, Enigma aj.), teorii čísel a asymetrické kryptografii (Fibonacciho posloupnost, narozeninový paradox, Diffie-Hellman, Rivest Shamir Adlema (RSA), DSA, eliptické křivky, variace eliptických křivek, Elgamal aj.). Stejně tak se naučí i praktické aplikaci šifrování (kryptoanalýza, frekvenční analýza, lineární kryptoanalýza, diferenční kryptoanalýza, integrální kryptoanalýza aj.).
Požadavky na průběh kurzu	• uchazeč zajistí výuku kurzu lektorem, který splňuje kvalifikaci dle požadavků zadavatele v ZD pro výuku kurzu, • uchazeč zajistí a dodá učební materiály v následující podobě: - v českém jazyce, - v tištěné jako oficiálně dostupnou odbornou literaturu nebo jako výukový materiál připravený uchazečem (popř. lektorem), v rozsahu a kvalitě odpovídající osnově kurzu, - opatřené publicitou dle metodiky OP LZZ (dostupné na http://www.esfcr.cz/07-13/oplzz/publicita-op-lzz), • uchazeč dodá zadavateli v elektronické i tištěné podobě do 5ti pracovních dnů po ukončení kurzu originály následujících dokumentů: - Prezenční listinu, - Evaluační dotazníky, - Evaluační zprávu, - Seznam úspěšných absolventů kurzu, • uchazeč vydá proškoleným osobám do 5ti pracovních dnů od ukončení kurzu Certifikát o absolvování kurzu při splnění podmínky minimální 85% účasti na

	kurzu, tato podmínka bude podložena Prezenční listinou a Seznamem úspěšných absolventů kurzu, • veškeré výstupy dodané uchazečem budou obsahovat minimum publicity dle pravidel OP LZZ (dostupné na http://www.esfcr.cz/07-13/oplzz/publicita-op-lzz).
Požadovaná součást kurzu	• uchazeč zajistí v ceně kurzu účastníkům občerstvení na každý den konání kurzu v následující podobě: - oběd na každý den konání kurzu, - nápoje (voda, čaj, káva) během přestávek kurzu.
Požadovaný počet proškolených osob	2
Požadovaná délka kurzu ve dnech	3 za následujících podmínek: - v pracovních dnech, které za sebou bezprostředně následují, - délka kurzu od 09:00 do 17:00 h pro každý den konání kurzu (čas ukončení může být pro každý den konání kurzu upraven dle potřeb lektora ve vztahu k probrané osnově), - se zahrnutím krátkých přestávek na oddech mezi jednotlivými částmi kurzu v každém dni konání kurzu, - se zahrnutím přestávky na oběd v délce max. 60 minut v každém dni konání kurzu.
Požadovaný jazyk výuky	čeština
Požadované místo výuky	Praha, učebna zajištěná uchazečem a vybavená hardwarovým a softwarovým zázemím potřebným pro konání kurzu, tedy dle specializace kurzu.