

INVESTICE DO ROZVOJE VZDĚLÁVÁNÍ

**METODICKÝ LIST** k **DUM VY\_32\_INOVACE\_08308dum – Kryptografie** ze šablony 08 – Internet sada 03, tematický okruh sady: Ostatní služby internetu

**NÁZEV DUM:** **Kryptografie**

<b>Anotace:</b>	Výkladový dokument s pracovním listem vysvětluje hlavní principy ochrany dat šifrovacími metodami a na příkladech studenta vede použitím základních substitučních šifer. Některé příklady mají otevřený konec pro doplnění studentem. Výuka v počítačové laboratoři s přístupem na internet
<b>Autor:</b>	Tomáš Vokoun
<b>Datum vytvoření DUM:</b>	10. dubna 2013
<b>Klíčová slova:</b>	kryptografie, šifra, kryptoanalýza, frekvence, šifrogram
<b>Jazyk:</b>	Čeština
<b>Druh učebního materiálu:</b>	Výkladový dokument s pracovním listem
<b>Stupeň a typ vzdělávání:</b>	Střední odborné vzdělávání
<b>Ročník:</b>	4
<b>Typická délka použití:</b>	cca 40 min
<b>Očekávaný výstup:</b>	Žák rozeznává rozdíly mezi šifrovacími metodami, rozeznává jednotlivé základní typy šifer. Ovládá použití substituční šifry a omezeně kryptoanalytické metody
<b>Speciální vzdělávací potřeby</b>	Žádné

**Řešení samostatných úkolů:**

- a) kdo zvladne desifrovat tento text přihlaste se u vyucujicoho o bod za aktivitu
- b) MULTIDISCIPLINARNI OBOR KRYPTOGRAFIE PREDPOKLADA DOBROU ZNALOST MATEMATIKY
- c) ... (pokračuje text preambule Listiny základních práv a svobod v Ústavě ČR)...
- d) HBSKOMFOYI CYBERGVIUE KUCWNAU
- e) INFORMATIKA NAS BAVI