ŠIFROVANIE, CERTIFIKÁTY, DIGITÁLNY PODPIS

Tematický celok / Téma	*ISCED / Odporúčaný ročník*
Informačná spoločnosť: • bezpečnosť a riziká	SŠ / 3.ročník
Ciele	
Žiakom osvojované vedomosti a zručnosti	***Žiakom rozvíjané spôsobilosti***
Bezpečnosť a riziká • **zabezpečiť svoje údaje a komunikáciu proti zneužitiu.** Bezpečnosť IT • rozlíšiť symetrické a asymetrické šifrovanie, • uviesť výhody a nevýhody symetrického a asymetrického šifrovania, • aplikovať symetrické a asymetrické šifrovanie na údajoch, • vysvetliť význam digitálneho certifikátu, • vysvetliť význam digitálneho podpisu.	**Informatické myslenie:** Logika • (LOG1) využitím logických zdôvodnení predpokladať správanie sa algoritmov (vysvetliť postupy používania rôznych kľúčov pri komunikácii) Algoritmy • (ALG2) vykonávať algoritmus (zašifrovanie/dešifrovanie správ) Vyhodnotenie • (VYH3) posúdiť kvalitu/správnosť objektu/systému/postupu na základe vybraných/definovaných kritérií (posúdiť bezpečnosť rôznych šifrovacích postupov)
Požiadavky na vstupné vedomosti a zručnosti	
• Ovládať prácu s internetom • Poznať princíp fungovania počítačových sietí a internetu.	
Riešený didaktický problém	
Súčasný stav povedomia bezpečného správania sa na internete nie je dostatočný. Táto metodika pomáha žiakom si uvedomiť, ako funguje zabezpečená komunikácii na internete pomocou praktických ukážok a zručností. Táto oblasť je veľmi široká a nedajú sa pokryť všetky aspekty bezpečnosti na internete. Metodika upozorňuje na zabezpečenie komunikácie a dokumentov nástrojmi voľne prístupnými na webe, žiaci si prakticky vyskúšajú šifrovanie a dešifrovanie, zabezpečenie svojich dokumentov.	
Dominantné vyučovacie metódy a formy	***Príprava učiteľa a pomôcky***
• riadené bádanie • frontálna, individuálna a skupinová forma (3-4 skupiny po 3-4 žiakoch)	Softvérové vybavenie: • softvér **GoAnywhere PGP studio** na učiteľskom PC Pomôcky: • počítače, dataprojektor • pracovný list pre žiaka (**I_SS_30 _PL.pdf**) • prezentácia (**I_SS_30_prezentacia.pptx**) ☒ **Nutnosť** digitálnych nástrojov. ☐ **Bez** použitia digitálnych nástrojov. ☐ Je možné odučiť **s** aj **bez** digitálnych nástrojov.
Diagnostika splnenia vzdelávacích cieľov	
Výsledky žiackych riešení úloh z pracovného listu, sebahodnotiaci test.	

Autor(i): *Ing. Zuzana Tkáčová, Ing. Paed. IGIP*

EURÓPSKA ÚNIA
Európsky sociálny fond
Európsky fond regionálneho rozvoja

OPERAČNÝ PROGRAM ĽUDSKÉ ZDROJE

MINISTERSTVO ŠKOLSTVA, VEDY, VÝSKUMU A ŠPORTU SLOVENSKEJ REPUBLIKY

Tento projekt sa realizuje vďaka podpore z Európskeho sociálneho fondu a Európskeho fondu regionálneho rozvoja v rámci Operačného programu Ľudské zdroje