



evropský
sociální
fond v ČR



EVROPSKÁ UNIE



MINISTERSTVO ŠKOLSTVÍ,
MLÁDEŽE A TĚLOVÝCHOVY



OP Vzdělávání
pro konkurenceschopnost

INVESTICE DO ROZVOJE VZDĚLÁVÁNÍ

Pracovní list – Šifry

- 1) Vysvětlete rozdíl mezi kryptogramem a kryptologem.

- 2) Zašifrujte větu „Karel Čapek je autorem knihy Válka s mlouky“
 - a. Césarovou šifrou s posunem $a \rightarrow k$
 - b. Vigenèrovou šifrou, jejímž řídicím slovem je vaše jméno

- 3) Jakým způsobem šifroval stroj Enigma? Který matematik stál za prolomením těchto šifer?

- 4) Stručně vysvětlete princip RSA šifry a veřejného a soukromého klíče. Jaká je základní myšlenka této šifry?