

## Seminar 28.2.2024

1. Send solution (only source code) to my email address until the end of seminar [eliska.ochodkova@vsb.cz](mailto:eliska.ochodkova@vsb.cz)
2. Implement (the choice of programming language is up to you) the Generalized Caesar Cipher (Shift Cipher). The permissible alphabet is English alphabet without spaces (uppercase only). Inputs must be entered from standard input (keyboard), outputs will be written to standard output (console). You must handle any impermissible characters that would appear in the input. The key will also be entered from the standard input. No GUI is needed yet, it can be a simple console application.
3. (With the previously implemented Shift Cipher) implement the brute force attack against the Generalized Caesar Cipher (Shift Cipher). Break the given ciphertext. What is the obtained plaintext and the key?

GMXMIWLEZISJXIRFSYRGIHFEGOJVSQGVMMWIWJVSQTERHIQMGWERHIEVXLUYEOIWXSJPSSHWERHJ  
MVIWXLIASVPHWYVFERTSAIVLSYWIWLEZIIQIVKIHWWXSRKIVALIRJEGIHAMXLEHZIVWMXCEJXIVXLIKVI  
EXJMVISJPSRHSRHIWXVSCIHQSWXSJXLIGMXCEVEJXSJMMVIWEJIXCVIKYPEXMSRWAIVIYWLIVIHMRFY  
MPHIVWWAETTIHXMQFIVJSVFMGOSVWXSRIAEPWAIVIQEHIKXLMGOIVWVXVIXWFIGEQIAMHIVALIR  
GLSPIVEXSVIXLVSYKLEQIVMGERIACSVOERHSXLIVGMXMIWMRXVSHYGIHWIAEKIWCWXIQWERHTYFP  
MGTEVOWXSHECWYVFEREVIEWJEGIEGLEPPIRKISJEHMJJIVIRXWSVXAMXLXLIQEWVIXYVRXSSJMMGI  
ASVOWXMPPYRGIVXEMRXLITERHIQMGLEWWLEVTIRIHHIFEXIEFSYXALEXXLIJYXVILSPHWJSVXLIMVG  
SQQIVGMEPLYFWOICFYWMRIWWHMWXVMGXWPMOIQERLEXERXLIGMXCSJPSRHSRXSOCSWQEVY  
RSYGLMERHPEHÉJIRWIMRTEVMWLEZIFSVRXLIFVYRXSJXLISJMMGIIBSHYW