Cvičení 26.2.2024

1. Naimplementujte zobecněnou Caesarovu šifru, tedy šifrovací algoritmus označovaný jako **Shift cipher**. Pracujte s přípustnou abecedou obsahující jen znaky anglické abecedy bez mezery, a to velká písmena. Implementujte jak šifrování, tak dešifrování. Ošetřete situaci, kdy v otevřeném textu budou nepřípustné znaky a malá písmena.

2. Jaký je správný otevřený text pro tento šifrový? Tedy implementujte útok hrubou silou pro Shift šifru.
   SFEFONXYJSNPDGJWSJYNHPJGJEUJHSTXYNRNXYWTAXYANXAJYFNNMKAQJISNRMTPJONGZIJ
   XUTQZUWFHTAFYSFWTISNZWFIUWTPDGJWSJYNHPTZFNSKTWRFHSNGJEUJHSTXYADUQDAFY
   TERJRTWFSIFPYJWJUTIJUXFQNWJINYJQSZPNGQZPFXPNSYWFUWJENIJSYHJXPJMTXAFEZQJISN
   MTMTPJOJFQTNXMFIFRHENPXFRUNTSFYGZIJQJYTXAPAJYSZMTXYNYUWFMFFTXYWFAF

3. Naimplementujte **Obecnou substituční šifru**. Klíčem bude libovolná náhodná permutace anglické abecedy bez mezery (vámi vygenerovaná (napište si vlastní metodu)).

4. Naimplementujte **Vigenerovu šifru**. Pracujte s přípustnou abecedou obsahující jen znaky anglické abecedy bez mezery. Implementujte jak šifrování, tak dešifrování. Pro kontrolu použijte klíč K=ZIMA a zašifrujte tento otevřený text:
   SLUNECNEATEPLEPOCASICTVRTKEMPROZATIMKONCIVNASLEDUJICICHDVOUDNECHSEZATAH
   NEVETSINUUZEMIZASAHNEDESTNAHORACHANASEVEROVYCHODEVEVSECHPOLOHACHSNIH
   OVIKENDUBUDEPOLOJASNOTEPLOTYVNOCIKLESNOUPODNULUPRESDENBUDEMAXIMALNES
   ESTSTUPNU
   Měli byste obdržet šifrový text
   RTGNDKZEZBQPKMBOBIEIBBHRSSQMOZAZZBUMJWZCHDZARTQDTRUCHKTDUWGDMMOHR
   MLASITNDDQTRQZUTHQMHHMSZPZECMETMITOQIOHZVMSDDQRNDKCGWPEUMHSDKTPNT
   AHZKTSMQTOUQWEMLGBTLQPNTAJZAZOSMBLNBKVMWOIJTQSMWGPNLZUKCBRDAPEMJG
   DDUMXHUMLMMEERBETTXZU