Úloha č. 1

1. Mějme zprávu $m \in M$ a ciphertext $c \in C$ délky 1. Pro substituční šifru s klíčem k nahlédneme, že

$$\Pr[E_k(m) = c] = \Pr[k(m) = c] = \frac{1}{n},$$

kde n je velikost abecedy. Šifra tedy pro tyto zprávy splňuje perfect indistinguishability.

2. Pro Caesarovu šifru se zprávou délky 1 platí

$$\Pr[E_k(m) = c] = \Pr[m + k \equiv c] = \Pr[k \equiv c - m] = \frac{1}{n}.$$

Tato šifra tudíž také splňuje p.i. pro tyto zprávy.

3. Substituční šifra má časově efektivní šifrovací funkci (vyhledání zprávy v tabulce může být konstantí operace), ovšem generování klíče je jak časově, tak paměťově velice náročné - musí se pro každou zprávu postavit a udržovat v paměti permutace na 2^{1000} prvcích.

Caesarova šifra a one-time pad naproti tomu generují klíče snáze jako náhodné 1000bitové číslo a liší se pouze v (de)šifrovací operaci. Jelikož XOR je jednodušší operace než modulární sčítání, snáze se paralelizuje a umožňuje použít stejnou funkci pro šifrování i dešifrování, one-time pad se zdá být nejlepší volbou schématu.

Úloha č. 2

Mějme zprávu m, ciphertext c, klíč k a šifrovací funkci E. Potom pro schéma platí

$$\begin{aligned}
\Pr[E_k(m) = c] &= \Pr[E_k(M) = c \mid M = m] \\
&= \frac{\Pr[M = m \mid E_k(M) = c] \cdot \Pr[E_k(M) = c]}{\Pr[M = m]} && \text{(Bayes)} \\
&= \frac{\Pr[M = m] \cdot \Pr[E_k(M) = c]}{\Pr[M = m]} && \text{(Shannon secrecy)} \\
&= \Pr[E_k(M) = c].
\end{aligned}$$

Tato hodnota nezávisí na m a je tím pádem shodná pro všechny zprávy, z čehož vyplývá, že schéma splňuje perfect indistinguishability.