Úloha č. 1

a)

Předpokládejme, že F' není pseudonáhodná funkce. Mějme distinguishera D pro funkci F s orákulem O a distinguishera D' pro F'. D poté sestrojíme následujícím způsobem:

- Když D' vygeneruje zprávu m, dotážeme se orákula na $0||m$ a $1||m$ a vrátíme D' hodnotu $O(0||m)||O(1||m)$.
- D má stejnou návratovou hodnotu D'

Z předpokladu existuje polynomiální D' nezanedbatelně rozlišující $F(0||m)||F(1||m)$. Jelikož na každý dotaz D' generuje D právě dva dotazy, vytvořili jsme polynomiálního distinguishera nezanedbatelně rozlišujícího F, čímž dostáváme spor s její pseudonáhodností.

b)

Mějme $x_0 = 0^{n-2}||1$ a $x_1 = 0^{n-1}$. Vidíme, že prvních n bitů $F'_k(x_0)$ je shodných s posledními n bity $F'_k(x_1)$, jelikož jsou obě hodnoty rovny $F_k(0^{n-1}||1)$. Pravděpodobnost, že tato rovnost platí u náhodné funkce, je $1/2^n$. Distinguisher tedy dokáže rozlišit F'_k s nezanedbatelnou pravděpodobností $1 - 1/2^n$, tudíž F' není pseudonáhodná funkce.

Úloha č. 2

Nechť F je pseudonáhodná funkce. Mějme následující schéma:

- $G(1^n)$ generuje náhodné k, j délky n.
- $Enc_{j,k}(m)$ pro n-bitovou zprávu m nejprve vygeneruje náhodné n-bitové číslo r. Poté, pokud $m = j$, vrátí zprávu $(0^{2n}||j)$, jinak vrátí $(r||m \oplus F_k(r)||j)$.
- $Dec_{j,k}(c)$ je přirozený inverz Enc.

Ze skript víme, že konstrukce typu $(r||m \oplus F_k(r))$ je CPA-bezpečná a tudíž má i indistinguishable multiple encryptions. Pokud si adversary nevybral za jednu ze zpráv j, nepřidává tento suffix žádnou rozlišovací hodnotu. Pravděpodobnost zvolení j je pouze $2t/2^n$ a tudíž zanedbatelná.

Adversary v CPA indistinguishability experimentu naproti tomu může nejprve od orákula snadno zjistit hodnotu j zašifrováním libovolné zprávy a poté zašifrovat např. $m_0 = j$ a $m_1 = \text{not}(j)$. Výsledné b' je pak rovno 0 právě tehdy, když $c = 0^{2n}||j$. Snadno nahlédneme, že tento adversary selže pouze v případě, že náhodné $r = 0^n$ a $F_k(r) = \text{not}(j)$, tedy se zanedbatelnou pravděpodobností $1/2^{2n}$.

Vytvořili jsme tedy schéma, které má indistinguishable multiple encryptions, ale není CPA-bezpečné.