Úloha č. 1

Zpráva se rozdělí na 8 bloků po 128 bitech. K samotné zprávě ještě musíme přidat jeden blok IV a jelikož je délka zprávy přesným násobkem délky bloku, nejspíše i jeden blok paddingu. Výsledný ciphertext tedy má délku 10 bloků, neboli 1280 bitů. Délka klíče pro velikost zprávy nehraje roli.

Úloha č. 2

Ukážeme, že pokud by existoval adversary A, pro nějž by tato pravděpodobnost nebyla zanedbatelná, dokážeme z něj sestrojit distinguishera D pro F.

Mějme orákulum O. Distinguishera sestrojíme následovně:

1. Spustíme $A(1^n)$.
2. Když si A vyžádá od šifrovacího orákula ciphertext zprávy m, vygenerujeme náhodné $IV \in \{0,1\}^n$ a zašifrujeme m v CTR módu pomocí O jako šifrovací funkce. Výsledný ciphertext vrátíme A.
3. Když A vygeneruje dvě zprávy m_0, m_1, zvolíme si náhodný bit $b \in \{0,1\}$ a vrátíme zprávu m_b zašifrovanou stejným postupem jako výše.
4. Odpovídáme na dotazy A jako výše, dokud nedostaneme výsledný bit b'. Vrátíme 0 právě tehdy, když $b = b'$.

Pokud je O pseudonáhodná funkce, adversary se chová stejně jako v experimentu $\mathsf{PrivK}^{\mathsf{cpa}}_{A,\Pi}(n)$, a tudíž

$$\Pr_{k \leftarrow \{0,1\}^n}\left[D^{F_k(\cdot)}(1^n) = 1\right] = \Pr\left[\mathsf{PrivK}^{\mathsf{cpa}}_{A,\Pi}(n) = 1\right],$$

kde k je zvoleno rovnoměrně náhodně.

Pokud je naproti tomu O zcela náhodná funkce, chová se A stejně jako v experimentu $\mathsf{PrivK}^{\mathsf{cpa}}_{A,\tilde{\Pi}}(n)$, z čehož dostáváme

$$\Pr_{f \leftarrow \mathsf{Func}_n}\left[D^{f(\cdot)}(1^n) = 1\right] = \Pr\left[\mathsf{PrivK}^{\mathsf{cpa}}_{A,\tilde{\Pi}}(n) = 1\right],$$

kde f je zvolena rovnoměrně náhodně. Jelikož předpokládáme, že šifra není CPA-secure, bude pro nějakého adversary platit

$$\left|\Pr\left[\mathsf{PrivK}^{\mathsf{cpa}}_{A,\Pi}(n) = 1\right] - \Pr\left[\mathsf{PrivK}^{\mathsf{cpa}}_{A,\tilde{\Pi}}(n) = 1\right]\right| > \mathsf{negl}(n). \tag{1}$$

Spojením z rovnostmi výše pak dostáváme, že musí rovněž platit

$$\left|\Pr_{k \leftarrow \{0,1\}^n}\left[D^{F_k(\cdot)}(1^n) = 1\right] - \Pr_{f \leftarrow \mathsf{Func}_n}\left[D^{f(\cdot)}(1^n) = 1\right]\right| > \mathsf{negl}(n).$$

Tím jsme dostali spor s pseudonáhodností F a tudíž dokázali, že nerovnice (1) nemůže platit.