Domácí úkol 6: AES a falešné klíče

Úloha 1. Spočtěte hodnotu, na kterou by S-box šifry AES zobrazil bajt $(\texttt{4b})_{16}$, kdyby se operace v tělese $\mathrm{GF}(2^8)$ prováděly modulo jiný ireducibilní polynom $p(x)$, než který je uvedený ve standardu. **Polynom $p(x)$ dostanete emailem.** Nezapomeňte zkontrolovat, že jste správně spočítali inverzní hodnotu k $(\texttt{4b})_{16}$.

Úloha 2. Nechť $x, y \in \{0,1\}^{64}$. Nechť dále $\pi : \{0,1\}^{64} \to \{0,1\}^{64}$ je permutace, která je vybrána náhodně z $S_{\{0,1\}^{64}}$ s rovnoměrným rozdělením pravděpodobnosti. Jaká je pravděpodobnost, že $\pi(x) = y$?

Úloha 3. Předpokládejme, že pokud je klíč $k \in \{0,1\}^{168}$ vybírán náhodně s rovnoměrným rozdělením pravděpodobnosti, pak $\mathrm{3DES}_k$ se chová jako permutace na množině $\{0,1\}^{64}$ vybraná náhodně s rovnoměrným rozdělením. Mějme neznámý klíč k, otevřený text x a šifrový text $y = \mathrm{3DES}_k(x)$. Spočtěte střední hodnotu počtu falešných klíčů, tj. klíčů k', pro něž platí, že $\mathrm{3DES}_{k'}(x) = y$ a přitom $k' \neq k$.

Úloha 4. Mějme t různých párů otevřeného a šifrového textu (x_i, y_i), $i = 1, 2, \ldots, t$, zašifrovaných jediným neznámým klíčem $k \in \{0,1\}^{168}$, tj. $y_i = \mathrm{3DES}_k(x_i)$ pro všechna i. Jaká je střední hodnota počtu falešných klíčů pro jednotlivá t? Pro jakou hodnotu t můžeme očekávat, že klíč bude určen jednoznačně?