# 1

TODO

# 2

Invert viz python kód.

Inverz `0xF3` v tělese $\mathbb{Z}_2[x]/(x^8 + x^7 + x^2 + x + 1)$ je `0x85`. Pokud tento prvek vynásobíme (jako vektor) maticí z AES dostaneme `0xEC` a po přičtení vektoru dostaneme výsledek `0x8F`.

# 3

Ze schématu šifrování plyne $DES_b(c) = DES_a(p)$, kde $p$ je daný plaintext a $c$ daný ciphertext. Provedeme meet-in-the-middle útok. Počet různých klíču $a$ je díky jeho vlastnostem $(\frac{256}{2})^3 = 128^3 \approx 2 \cdot 10^6$ (počet $k_i$ s lichou paritou je pouze polovina), což není tolik. Vygenerujeme všechny různé ciphertexty, které je možné získat šifrováním plaintextu $p$ klíčem $a$. Celkem nagenerujeme $\approx$ 2 milionu ciphertextů, které si někam uložíme společně s příslušným klíčem $a$.

Poté provedeme druhou část útoku, která bude zase naopak šifrovat ciphertext $c$ různými klíči $b$, kterých je také zhruba 2 miliony. Ty si však nemusíme ukládat (ani pravděpodobně nevygenerujeme všechny 2 miliony). Pokaždé stačí zkontrolovat, jesliže příslušný zašifrovaný ciphertext již máme v tabulce. Pokud najdeme shodu, tak víme, jaké jsou oba klíče $a, b$. Tedy známe klíč $k$.

Výsledný klíč $a =$ `07:07:07:01:01:01:01:01`

$b =$ `0B:0B:0B:01:01:01:01:01`

Celkem tedy $k =$ `07:07:07:0B:0B:0B`

Zbytek viz Java kód `main.java` + `DES.java`

# 4