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 ≈ 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

Pro k musí platit $k <= 255 = \mathtt{FF}_{16}$. To je maximální hodnota, která jde uložit do jednoho bajtu. Tedy pro šifry s blokem délky > 255 bajtů tento padding nelze použít.

5

Nechť x, y jsou nějaké zprávy, nechť $|x|$ je délka zprávy x (pro y stejně).

Buď $x \neq y$ a $|x| = |y|$, poté padding p je stejný pro obě zprávy. Výsledné zprávy jsou tedy $x||p$ (zpráva x, ke které je přidán padding) a $y||p$. Ale $x \neq y$ z předpokladů, tedy nemůže platit, že se výsledné zprávy budou rovnat (tedy $x||p \neq y||p$).

Nebo $x \neq y$ a $|x| \neq |y|$. Poté každá zpráva má jiný padding $p_x \neq p_y$. Tedy zase nemůže platit, že $x||p_x \neq y||p_y$ (již poslední bajt zprávy je různý, protože padding má různou délku).

6

Blok je tedy 8 bajtový, padding má délku tedy maximálně 8 bajtů. Zpráva má 16 bajtů. Tedy buď padding je délky 8 $\Rightarrow$ 8 z 16 bajtů zprávy je určeno. Celkový počet různých zpráv je 256^{16} a v tomto případě nám zbývá 256^8 možností, jak vybrat prvních 8 bajtů zprávy. Pravděpodobnost toho, že náhodná zpráva bude mít správný padding délky 8 je $\frac{256^8}{256^{16}} = 256^{-8}$.

Padding může mít délku $1 \ldots 8$ bajtů. Výsledná pravděpodobnost je tedy:

$$\sum_{i=1}^{8} 256^{-i} \approx 0.4\ \%$$

Pokud náhodná zpráva má dobrý padding, tak nejpravdědpobněji bude mít padding délku 1 bajt, protože takových zpráv je nejvíce (256^{15} z 256^{16}). Pravděpodobnost takové zprávy je $\frac{1}{256}$.