# 6. Blokové šifry a operační módy, implementace v OpenSSL

Účelem dnešního cvičení je seznámit se s použitím blokových šifer a jejich operačních módů. Přitom si také ukážeme šifrování delšího souboru. Za splnění celého zadání dostanete **5 bodů**.

## Zadání

1. Stáhněte si např. tento obrázek ve formátu TGA (rozbalte zip): obrazek.zip (../media/tutorials/06/obrazek_tga.zip). (homer-simpson.zip (../media/tutorials/06/homer-simpson_tga.zip), ucm8.tga (../media/tutorials/06/UCM8.TGA))
2. Napište program, který zkopíruje hlavičku a **zašifruje** část souboru s obrazovými daty pomocí AES v módu ECB. Výstupní soubor se bude jmenovat `(původní_jméno)_ecb.tga`.
3. Napište program, který **dešifruje** obrázek zašifrovaný prvním programem. Výstupní soubor se bude jmenovat `(původní_jméno)_dec.tga`
   - Porovnejte původní obrázek a jeho zašifrovanou podobu a vysvětlete svá zjištění.
4. Změňte pro šifrování i dešifrování použitý operační mód na **CBC** a vytvořte `(původní_jméno)_cbc.tga` a `(původní_jméno)_cbc_dec.tga` (upřesní cvičící).
   - Porovnejte původní obrázek a jeho zašifrovanou podobu a vysvětlete svá zjištění.
5. **Na první řádek zdrojáku dejte komentář se jménem autora**!

Volbu šifry a operačního módu zjistěte z dokumentace `EVP_EncryptInit_ex` (`man EVP_EncryptInit_ex`).

### Formát obrázků TGA (zjednodušeno)

Jednotky: bajty (slabiky)

| Pozice | Délka | Význam |
|---|---|---|
| 0 | 1 | Délka obrazového ID |
| 1 | 1 | Typ barevné mapy |
| 2 | 1 | Typ obrázku |
| 3 | 2 | Počátek barevné mapy |
| 5 | 2 | Délka barevné mapy |
| 7 | 1 | Bitová hloubka položek barevné mapy |
| 8 | 10 | Specifikace obrázku |
| 18 | … | Obrazový identifikátor (nepovinné)<br>Barevná mapa (nepovinné) |

**x** do konce souboru **Obrazová data**

Pořadí bytů je little-endian. Barevnou mapu ani obrazové ID není potřeba dále zpracovávat, je potřeba je jen správně přeskočit a nešifrovat je. Šifrovat se musí až samotná obrazová data, nic jiného.

Detailní popis formátu obrázku je dostupný například zde (http://www.paulbourke.net/dataformats/tga/) .

## Postup šifrování delšího souboru, pole, atd.

1. Inicializace knihovny, alokace kontextu (viz minulé cvičení)
2. `EVP_EncryptInit_ex(ctx, type, NULL, key, iv);`
3. Cyklus: dokud mám data
    a. Přečti obrazová data do pole `ot` (např. `fread`, ...), délka přečtených dat je `otLength`.
    b. `EVP_EncryptUpdate(ctx, st, &stLength, ot, otLength);`
    c. Zapiš do výstupního souboru obsah pole `st` délky `stLength` (může se lišit od `otLength`).
4. `EVP_EncryptFinal_ex(ctx, st, &stLength);` – dokončení šifrování posledního bloku
5. Zapiš do výstupního souboru obsah pole `st` délky `stLength`

U blokových šifer je ve výchozím nastavení zapnuto zarovnání (padding). Proto může být šifrovaný soubor větší než původní.