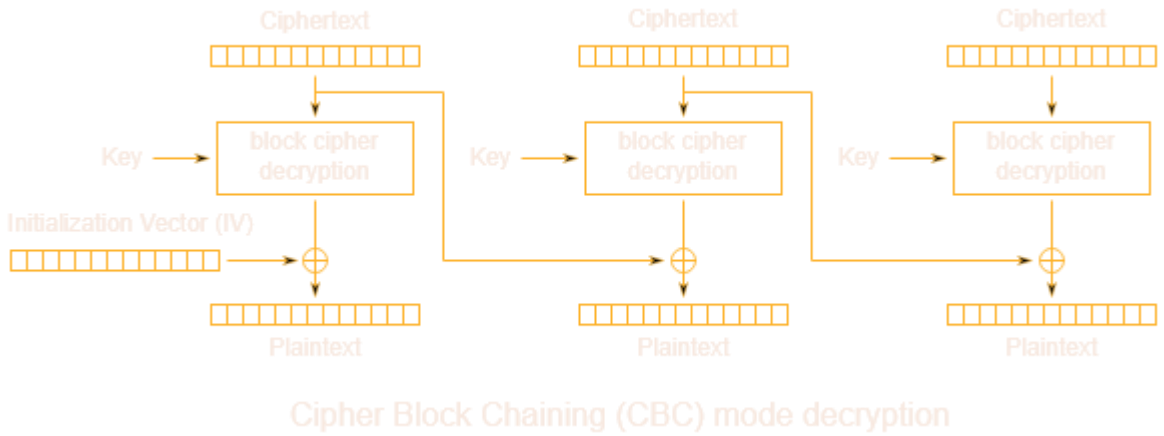
Lazy CBC

הבעיה: $IV == Key$ ואפשר לפענח ולהצפין

מה יקרה אם נפענח 2 בלוקים של אפסים?



הבלוק הראשון לאחר פענוח יהיה $D(0x0) \oplus IV = D(0x0) \oplus KEY$

הבלוק השני לאחר פענוח יהיה $D(0x0) \oplus 0x0 = D(0x0)$

ואם נעשה ביניהם XOR נקבל $D(0) \oplus D(0) \oplus KEY = KEY$

```
[04:40 PM]-[liam@liampc]-[~/ctfs/cryptohack]- |main ✓|
$ python3 lazy_cbc.py
crypto{50m3_p30pl3_d0n7_7h1nk_IV_15_1mp0r74n7_?}
```