Decrypting CBC with simple XOR (10 points)

Number : 199606131115

We first retrieve the IV block which is the first 12 bytes of the encrypted text.

Then we can deduce the key by doing the operation $key = IV \oplus C_0 \oplus M_0$ (because we have $C_i = key \oplus (M_i \oplus C_{i-1})$ and here with $i = 0 : C_{i-1} = IV$).

We can then decrypt the message by deducing M_i for each i : $M_i = key \oplus C_i \oplus C_{i-1}$.

For the input generated for 199606131115, we obtain :

```
Recovered message: 199606131115I decrypted a CBC message and all I got was this lousy sentence.00000000
```