Solution of Exercisesheet 6

Exercise 6-1

(a)

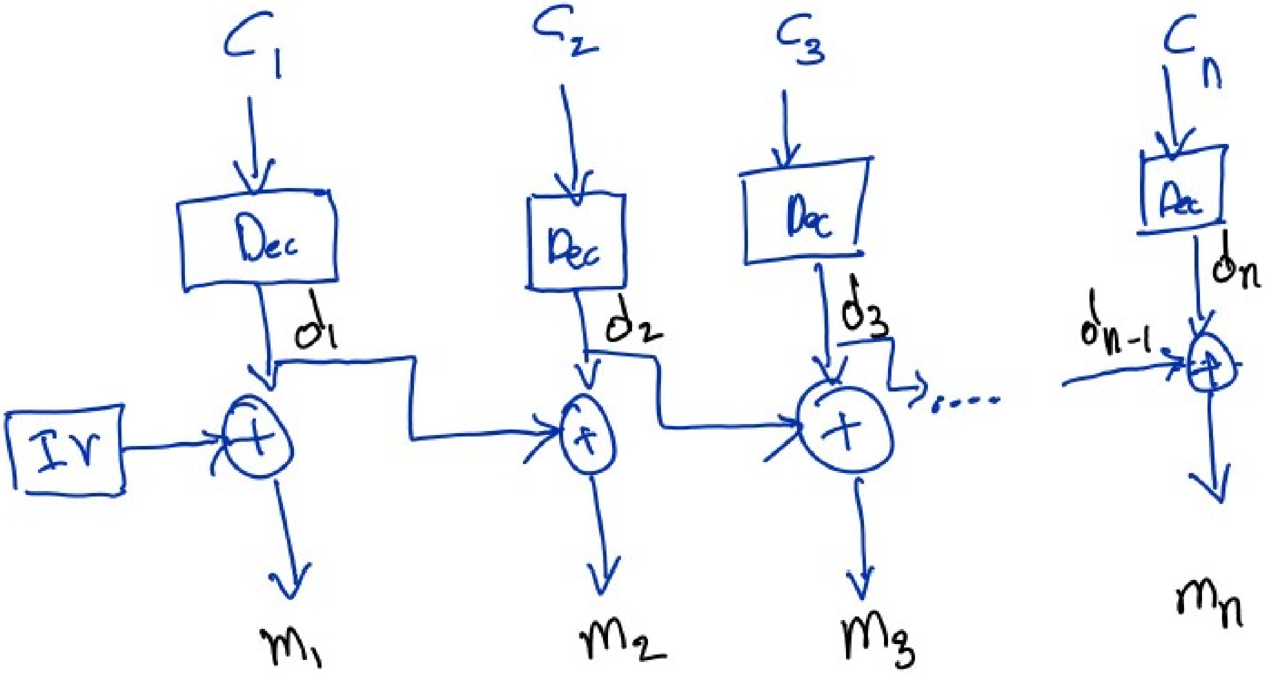

Figure 1: Decryption for CBC* mode

(b) As shown in the above figure, let us assume

$$d_i = \text{Dec}\ (c_i)$$

So

$$m_1 = d_1 \oplus IV$$
$$m_2 = d_2 \oplus d_1\ ...$$

To show that this CBC* doesn't have indistinguishable encryptions, let us consider message in the format $m = m_1||m_2||m_3||...||m_n$. Also we know for CPA, adversary A is allowed of multiple encryptions.

Let us consider A choose two messages i.e., $m1$ and $m2$

$$m1 = m1_1||m1_2||m1_3||...||m1_n$$
$$m1 = m2_1||m2_2||m2_3||...||m2_n$$

And $m1$ is choosen in such a way that $m1_1 == m1_2 == m1_3 == ... == m1_n$ and $m2$ is choosen in such a way that $m2_1 \neq m2_2 \neq m2_3 \neq ... \neq m2_n$

With these kind of messages choosen, A can distingush $m1$ and $m2$ by checking

$$c_1 == c_3 == ... == c_i$$
$$c_2 == c_4 == ... == c_{i+1}$$
where i is an odd number $\leq n$

If the above check is statisfied then the cipher c corresponds to $m1$. Else it corresponds to $m2$. With this construction A can distingush between the messages with a probability equal to 1.

Exercise 6-2

Task: Show that Π_{CBC} is not CCA-secure by demonstrating a successful adversary.
Assume n = 3
The adversary $\mathcal{A}$ can choose the two messages $m_0 = m_0^1||m_0^2 = 000\ 000$ and $m_1 = m_1^1||m_1^2 = 111\ 111$ which he sends to the challenger. Then he gets the ciphertext $c_b = (c_b^0||c_b^1||c_b^2) = (IV||f_k(IV \oplus m_b^1)||f_k(f_k(IV \oplus m_b^1) \oplus m_b^2))$ back.
Then $\mathcal{A}$ flipps the last bit from c_b^2, so $(c_b^2)' = c_b^2 \oplus 001$ and asks the decryption oracle for the decryption of $c_b' = c_b^0||c_b^1||(c_b^2)'$. Because $c_b' \neq c_b$ the decryption oracle answers with $m' = f_k^{-1}(c_b^1) \oplus c_b^0||f_k^{-1}(c_b^2) \oplus c_b^1 = f_k^{-1}(f_k(IV \oplus m_b^1)) \oplus IV||f_k^{-1}((c_b^2)') \oplus f_k(IV \oplus m_b^1) = m_b^1||f_k^{-1}((c_b^2)') \oplus f_k(IV \oplus m_b^1)$ m_b^1 is now either m_0^1 or m_1^1 because the change in $(c_b^2)'$ doesn't impact m_b^1. So the adversary can say for sure, if the recieved civertext c_b is the encoding for m_0 or m_1.
⇒ Π_{CBC} mode is not CCA-secure

Exercise 6-3