

## SOLUTION OF EXERCISESHEET 6

## Exercise 6-1

(a)

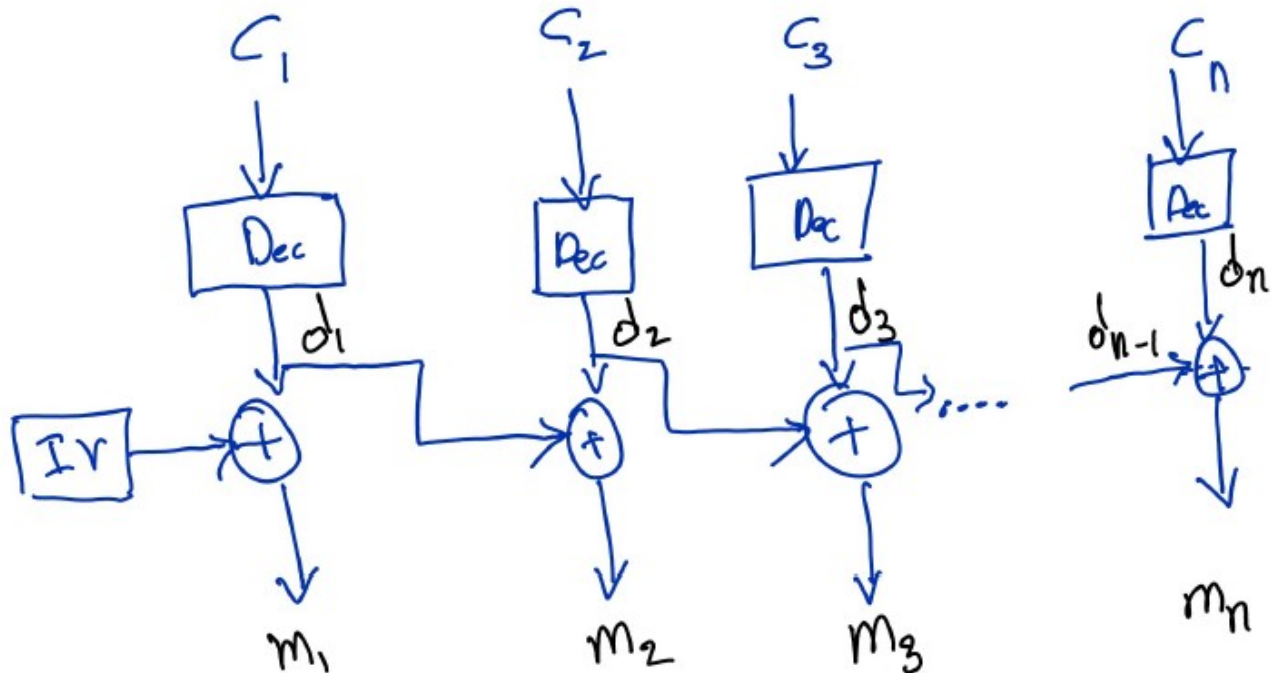


Figure 1: Decryption for CBC\* mode

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

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

So

$$\begin{aligned} m_1 &= d_1 \oplus IV \\ m_2 &= d_2 \oplus d_1 \dots \end{aligned}$$

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

Let us consider  $A$  choose two messages i.e.,  $m_1$  and  $m_2$

$$\begin{aligned} m_1 &= m_{1_1} || m_{1_2} || m_{1_3} || \dots || m_{1_n} \\ m_2 &= m_{2_1} || m_{2_2} || m_{2_3} || \dots || m_{2_n} \end{aligned}$$

## SOLUTION OF EXERCISESHEET 6

And  $m_1$  is chosen in such a way that  $m_{1_1} == m_{1_2} == m_{1_3} == \dots == m_{1_n}$  and  $m_2$  is chosen in such a way that  $m_{2_1} \neq m_{2_2} \neq m_{2_3} \neq \dots \neq m_{2_n}$

With these kind of messages chosen,  $A$  can distinguish  $m_1$  and  $m_2$  by checking

$$\begin{aligned} c_1 &== c_3 == \dots == c_i \\ c_2 &== c_4 == \dots == c_{i+1} \\ \text{where } i &\text{ is an odd number } \leq n \end{aligned}$$

If the above check is satisfied then the cipher  $c$  corresponds to  $m_1$ . Else it corresponds to  $m_2$ . With this construction  $A$  can distinguish between the messages with a probability equal to 1.

### Exercise 6-2

**Task:** Show that  $\Pi_{CBC}$  is not CCA-secure by demonstrating a successful adversary.

The adversary  $\mathcal{A}$  can choose the two messages  $m_0 = m_0^1 || m_0^2 = 0^n 0^n$  and  $m_1 = m_1^1 || m_1^2 = 1^n 1^n$  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  $\mathcal{A}$  flips the last bit from  $c_b^2$ , so  $(c_b^2)' = c_b^2 \oplus 0^{n-1}1$  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 received ciphertext  $c_b$  is the encoding for  $m_0$  or  $m_1$ .

$\Rightarrow \Pi_{CBC}$  mode is not CCA-secure

### Exercise 6-3



## SOLUTION OF EXERCISESHEET 6

a)

Let  $F$  be a pseudorandom permutation. Then  $F$  and  $F^{-1}$  are pseudorandom permutations.

$\Pi_M = (\text{Gen}, \text{Mac}, \text{Vrfy})$

$\frac{\text{Gen}(1^\lambda)}{k \leftarrow \text{Gen}(1^\lambda)}$   
**return**  $k$

$\frac{\text{Mac}_k(c)}{t \leftarrow F_k^{-1}(c)}$   
**return**  $t$

$\frac{\text{Vrfy}_k(c, t)}{\text{if } t = \text{Mac}_k(m)}$   
**return** 1  
**return** 0

$\Pi_E = (\text{Gen}, \text{Enc}, \text{Dec})$

$\frac{\text{Gen}(1^\lambda)}{k \leftarrow \text{Gen}(1^\lambda)}$   
**return**  $k$

$\frac{\text{Enc}_k(m)}{r \leftarrow \{0, 1\}^{\frac{n}{2}}}$   
 $m \in \{0, 1\}^{\frac{n}{2}}$   
 $c \leftarrow F_k(m \parallel r)$   
**return**  $c$

$\frac{\text{Dec}_k(c)}{v := F_k^{-1}(c)}$   
**return** first  $\frac{n}{2}$  bits of  $v$

Because  $\text{Enc}_k(m), \text{Mac}_k(\text{Enc}_k(m)) = F_k(m \parallel r), F_k^{-1}(F_k(m \parallel r)) = F_k(m \parallel r), (m \parallel r)$

TODO Beweise