TD 3 – Symmetric encryption

Exercise 1. *ECB is not IND-CPA secure*

— Prove that ECB mode of operation does not yield an IND-CPA secure symmetric encryption scheme, no matter how good the underlying block cipher is. *Write the definitions!*

Exercise 2. *CBC ciphertext stealing*

Recall that using the CBC mode of operation with a block cipher E and key k, the message M is split into length-n blocks $m_1\|\cdots\|m_\ell$, and encrypted as $C = c_0\|\cdots\|c_\ell$ where c_0 is a random IV, and $c_i = E_k(m_i \oplus c_{i-1})$ for $i > 0$. This assumes that m_ℓ has length n. Otherwise, one can define $m'_\ell = m_\ell\|10^{n-r-1}$ and $c_\ell = E_k(m'_\ell \oplus c_{\ell-1})$.

1. Write the decryption algorithm for CBC mode of operation.
2. Let $M = m_1\|\cdots\|m_{\ell-1}\|m_\ell$ where each block has size n, but m_ℓ which has size $r < n$. Let C be the encryption of M, where m_ℓ has been padded to length n.
   - **i.** What is the bit length L of M, as a function of n, ℓ and r?
   - **ii.** What is the bit length of C, as a function of L, n and r?

We now present an elegant technique to avoid the padding and reduce the size of C. We first modify the padding of m_ℓ and define $m'_\ell = m_\ell\|0^{n-r}$. Let $C = c_0\|\cdots\|c_\ell$ be the ciphertext obtained as before but with this new padding. Then we define $c'_{\ell-1} = c_\ell$ and c'_ℓ as the first r bits of $c_{\ell-1}$. Finally, we let $C' = c_0\|\cdots\|c_{\ell-2}\|c'_{\ell-1}\|c'_\ell$.

3. What is the bit length of C', as a function of L, n and r?
4. Explain how to recover m_ℓ and $c_{\ell-1}$ from c'_ℓ and the decryption of $c'_{\ell-1}$, and then how to decrypt C'.

Exercise 3. *CTR mode*

We consider the encryption scheme $(\mathsf{Enc}, \mathsf{Dec})$ obtained from a block cipher E of block size n, using the CTR mode of operation.

1. Write the decryption algorithm.

One characteristic of a good encryption scheme is that the ciphertext should be hard to distinguish from random bits. Formally, we define the following experiment: An adversary sends a message m of ℓ blocks to a challenger; The challenger either compute $c \leftarrow \mathsf{Enc}_k(m)$, or $c \twoheadleftarrow \{0,1\}^{n(\ell+1)}$ and sends back c to the adversary; The adversary must tell which of the two happened.

2. Prove that an adversary that sends a 2^n-block message is able to distinguish with very high probability. Compute this probability. *Hint. Use the fact that E_k is a permutation.*
3. Use the birthday bound to prove that the adversary already has a good probability of success with a $2^{n/2}$-block message.
4. Since the the problem of the previous questions is that E_k be a permutation, one can define $F_k(x) = E_k(x) \oplus x$, so that F_k is not a permutation, and encrypt m as $IV\|m_1 \oplus F_k(IV+1)\|\cdots\|m_\ell \oplus F_k(IV+\ell)$. Does this solve the problem?