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*

Let E be a block cipher with block size n, used with the CBC mode of operation. To encrypt a message m of length multiple of n, we write $m = m_1\|\cdots\|m_\ell$ where each m_i has bit length n, and encrypt it 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 $i > 0$.

To handle messages of any lengths, we use padding. Let now $m = m_1\|\cdots\|m_\ell$ where m_ℓ has length $r \leq \ell$. It is padded as $\mathrm{pad}(m) = m\|10^{n-1-(r \bmod m)}$: m_ℓ is padded to length n or a full block of padding is added if it already has length n. Then $\mathrm{pad}(m)$ is encrypted instead of m.

1. **i.** Write the decryption algorithm for CBC mode of operation.
   ii. Why a full block of padding is needed when m_ℓ has size n?
   iii. What are the bit lengths of m and c, as functions of n, ℓ 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 $c' = c_0\|\cdots\|c_{\ell-2}\|c'_{\ell-1}\|c'_\ell$.

2. **i.** What is the bit length of c', as a function of L, n and r?
   ii. Explain how decrypt c'. *Hint. How can we compute m_ℓ and $c_{\ell-1}$ from c'_ℓ and $E_k^{-1}(c'_{\ell-1})$?*

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 game: 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 problem of the previous questions is that E_k is a permutation, one can define $F_k(x) = E_k(x) \oplus x$, so that F_k is not a permutation anymore, 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?