TD 1 – Block ciphers and symmetric encryption

Exercise 1. *False or false*

Explain why each of the following statements is wrong.

1. It is never possible to attack an ideal block cipher.
2. A block cipher with keys of 512 bits is always secure.
3. There will never be any reason, technologically speaking, to use (block cipher) keys larger than 128 bits.
4. One should always use (block cipher) keys larger than 128 bits.
5. (*) One should always use the latest-published, most recent block cipher.

Exercise 2. *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 3. *CBC cipertext stealing*

Let $M = m_1\|\cdots\|m_{\ell-1}\|m_\ell$ be a message of length $L = (\ell-1)n + r$ with $r = |m_\ell| < n$. A first idea to apply CBC on M is to pad its last block with zeroes for its length to be n.

Recall that using the CBC mode of operation with a block cipher E and key k, the message M is then 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 $i > 0$, where we assume m_ℓ is padded to length n.

1. What is the bit length of C?
2. Write the decryption algorithm, that is explain how to compute M from C and k.

We now present an elegant technique to avoid the padding. Let us rewrite the penultimate ciphertext $c_{\ell-1} = E(k, m_{\ell-1} \oplus c_{\ell-2})$ as $c'_\ell\|P$ where c'_ℓ has r bits. Let also $m'_\ell = m_\ell\|0^{n-r}$ be the padded last block and $c'_{\ell-1} = E(k, m'_\ell \oplus (c'_\ell\|P))$.

3. What is the bit length of $C' = c_0\|\cdots\|c_{\ell-2}\|c'_{\ell-1}\|c'_\ell$?
4. Explain how to recover m_ℓ and P from the decryption of $c'_{\ell-1}$, and then $m_{\ell-1}$ from the decryption of c'_ℓ.

Exercise 4. *Birthday bound*

We draw $y_1, \dots, y_q$ uniformly and independently at random in a set of size N, with $q \le \sqrt{2N}$. We want to prove that the probability $p_{q,N}$ that there exists $i \ne j$ such that $y_i = y_j$ satisfies $q(q-1)/4N \le p_{q,N} \le q(q-1)/2N$. We say that there is a *collision* between y_i and y_j if $y_i = y_j$.

1. We first prove the upper bound.
   - **i.** Fix $i \ne j$. What is the probability that $y_i = y_j$?
   - **ii.** Prove the upper bound. *Use the union bound.*
2. For the lower bound, denote by N_i the event “there is no collision among $y_1, \dots, y_i$”.
   - **i.** Express the event “there exists at least a collision” in terms of an event N_i.
   - **ii.** Prove that $\Pr[N_q] = \Pr[N_1] \cdot \Pr[N_2|N_1] \cdots \Pr[N_q|N_{q-1}]$.
   - **iii.** What is $\Pr[N_1]$?
   - **iv.** Prove that $\Pr[N_{i+1}|N_i] = 1 - i/N$.
   - **v.** Conclude that $\Pr[N_q] \le e^{-q(q-1)/2N}$. *Use the inequality* $1 + x \le e^x$*, valid for any* x.
   - **vi.** Finish the proof. *Use the inequality* $e^{-x} \le 1 - x/2$*, valid for* $0 \le x \le 1$.