TD 2 – Block ciphers

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. *From the slides*

Prove that the four following informal security definitions for a block cipher E are encompassed by the security notion PRP or SPRP. *For each of them, show that an efficient adversary can be used to get a large advantage in either the PRP or SPRP game.*

1. Given $c = E_k(m)$, computing m without knowing k is *hard*.
2. Given m, computing $c = E_k(m)$ without knowing k is *hard*.
3. Given oracle access to E_k, it is *hard* to find k.
4. Given oracle access to $E_k^{\pm}$, it is *hard* to find k.

Exercise 3. *Meet-in-the-middle and PRP advantage*

Let $E : \mathcal{K} \times \mathcal{M} \to \mathcal{M}$ be a block cipher, where $\mathcal{K} = \{0,1\}^\kappa$ and $\mathcal{M} = \{0,1\}^n$. Let $EE : \mathcal{K}^2 \times \mathcal{M} \to \mathcal{M}$ defined by $EE_{k_1\|k_2}(m) = E_{k_2}(E_{k_1}(m))$. The meet-in-the-middle attack allows an adversary to compute the key $k_1\|k_2$ from a pair $(m, EE_{k_1\|k_2}(m))$ in time $O(2^\kappa)$.

1. We translate this attack into a *lower* bound on the PRP advantage function. Let $\mathcal{A}$ be an adversary that performs the meet-in-the-middle attack. Consider $\mathcal{A}$ playing the PRP game, making one query to the oracle.
   - **i.** What is the running time of $\mathcal{A}$?
   - **ii.** If the oracle is $EE_{k_1\|k_2}$, prove that $\mathcal{A}$ detects it.
   - **iii.** If the oracle is a random permutation, prove that $\mathcal{A}$ fails to detect it with probability $\leq 1/2^{n-2\kappa}$.
   - **iv.** Deduce a lower bound on $\mathsf{Adv}^{\mathsf{PRP}}_{EE}(q,t)$ for well-chosen q and t.

Can we say that double encryption is *not* a good block cipher?

2. We define a space-efficient variant of the meet-in-the-middle attack, parametrized by a length $\ell \leq \kappa$. For a given *prefix* $s \in \{0,1\}^\ell$, the adversary runs the attack but restricted to keys k_1 that starts with s (and all keys $k_2 \in \{0,1\}^\kappa$). The complete attack is running this restricted attack with all possible length-ℓ prefixes s.
   i. Analyze the time and space complexity of this attack.
   ii. Describe the attack in the two extremal cases $\ell = 0$ and $\ell = \kappa$.

Exercise 4. *Format-preserving encryption*

Consider a set $\mathcal{M}$ of message, distinct from $\{0,1\}^n$: say $\{0,1\}^{\leq n}$ or the set of prime numbers $\leq 2^{128}$, etc. A *format-preserving* block cipher is a block cipher for such an arbitrary set $\mathcal{M}$.

Assume that $\mathcal{M} \subset \{0,1\}^n$ for some n, and that we know an efficient algorithm that, given $m \in \{0,1\}^n$, determine whether $m \in \mathcal{M}$. The *cycle walking* algorithm converts a block cipher $E : \{0,1\}^\kappa \times \{0,1\}^n \to \{0,1\}^n$ to a format-preserving block cipher $E' : \{0,1\}^\kappa \times \mathcal{M} \to \mathcal{M}$. To encrypt $m \in \mathcal{M}$ using E' with a key k, compute $m' = E_k(m)$; If $m' \in \mathcal{M}$, return $c = m'$; Otherwise iterate with $m'' = E_k(m')$, etc.

1. Give the decryption algorithm $E'^{-1} : \{0,1\}^\kappa \times \mathcal{M} \to \mathcal{M}$.
2. Why is the existence of an efficient algorithm to test the appartenance to $\mathcal{M}$ not sufficient for E' to be efficient?
3. Prove that the expected number of calls to E in the random oracle model is $(2^n + 1)/(\#\mathcal{M} + 1)$. *Hint. Prove (or admit) the following: given a size-t subset U of a size-N set S, the expected number of elements we need to sample (without replacement) from S to get an element of U is $(N+1)/(t+1)$.*