Cryptology complementary
Final Examination

2018-05-17

Instructions

The duration of this examination is one hour. Answers to the questions must be detailed and complete to get maximum credit. The full scale is not determined yet: it may not be necessary to answer all questions in order to obtain a perfect mark.

Unique Exercise: Block cipher block size extension

In all of the following, $\mathcal{E} : \{0,1\}^\kappa \times \{0,1\}^n \to \{0,1\}^n$ is a publicly-known block cipher with κ-bit keys and n-bit blocks. (In particular, this means that anyone is able to efficiently evaluate $\mathcal{E}(\cdot,\cdot)$ and its inverse $\mathcal{E}^{-1}(\cdot,\cdot)$.) We recall the following definition.

Definition 1. PRP Advantage. The *PRP advantage* of a block cipher $\mathcal{E}$ is a function that returns the maximum advantage of any algorithm with bounded resources trying to distinguish $\mathcal{E}$ with a random key from a random permutation. Formally, it is given by:

$$\begin{aligned}\mathbf{Adv}_{\mathcal{E}}^{\mathrm{PRP}}(q,t) = \max_{A_{q,t}} | \Pr[A_{q,t}^{\mathcal{O}}() = 1 : \mathcal{O} \xleftarrow{\$} \mathsf{Perms}(\{0,1\}^n)] \\ - \Pr[A_{q,t}^{\mathcal{O}}() = 1 : \mathcal{O} = \mathcal{E}(k,\cdot), k \xleftarrow{\$} \{0,1\}^\kappa]|\end{aligned}$$

In the above, $A_{q,t}^{\mathcal{O}}$ denotes an algorithm with *oracle access* to $\mathcal{O}$, running in time t (for an unspecified time unit, common to all algorithms) and making q queries to its oracle. Also, for a finite set $\mathcal{S}$, $X \xleftarrow{\$} \mathcal{S}$ means that X is drawn uniformly at random from $\mathcal{S}$, and $\mathsf{Perms}(\mathcal{S})$ denotes the set of permutations over $\mathcal{S}$.

Q. 1: Assume that $\mathbf{Adv}_{\mathcal{E}}^{\mathrm{PRP}}(t,q) \approx t/2^\kappa$ when $q \geq c$, c a (small) constant and the time unit is the time necessary to evaluate $\mathcal{E}$ once.

1. Explain why it is not possible to have a block cipher $\mathcal{E}' : \{0,1\}^\kappa \times \{0,1\}^n \to \{0,1\}^n$ such that $\mathbf{Adv}_{\mathcal{E}'}^{\mathrm{PRP}}(t,q) \ll \mathbf{Adv}_{\mathcal{E}}^{\mathrm{PRP}}(t,q)$?
2. Can $\mathcal{E}$ be considered to be a "good" block cipher?
3. Would $\mathcal{E}$ be a practically useful block cipher if one had $\kappa = 32$, $n = 128$?
4. Same question with $\kappa = 128$, $n = 128$?
5. Same question with $\kappa = 256$, $n = 8$?

We now wish to use $\mathcal{E}$ to build a new block cipher $\mathcal{F}$ with a larger block size $2n$.

Q. 2: Let $k \in \{0,1\}^\kappa$; x_L, $x_R \in \{0,1\}^n$; $\cdot||\cdot$ denote string concatenation. We first define $\mathcal{F}(k, x_L||x_R)$ as $\mathcal{E}(k, x_L)||\,\mathcal{E}(k, x_R)$.

1. What can you say about $\mathcal{F}(k, x_L||x_R)$ and $\mathcal{F}(k, x_L||x'_R)$, when $x'_R \neq x_R$?
2. Using the above property, show that $\mathcal{F}$ can easily be distinguished from a random permutation by an algorithm with small time and query complexity (you don't need to precisely analyse the advantage of your algorithm).
3. Explain why $\mathcal{F}$ is not a good block cipher.

Q. 3: We redefine $\mathcal{F}$ as following. Let $c_R = x_L \oplus \mathcal{E}(k, x_R)$, $c_L = x_R \oplus \mathcal{E}(k, c_R)$, then $\mathcal{F}(k, x_L||x_R) = c_L||c_R$.

1. Show that $\mathcal{F}(k, \cdot)$ is efficiently invertible by anyone knowing k, by giving an expression for x_R in function of c_L and c_R (and k) and an expression for x_L in function of c_R and x_R (and k). Is $\mathcal{E}^{-1}$ needed to compute $\mathcal{F}^{-1}$?
2. Show that in fact, $\mathcal{F}$ is its own inverse (i.e. is an involution).
3. Let a be an arbitrary element of $\{0,1\}^n$. What is the probability $p_a = \Pr[\mathcal{P}(a) = a : \mathcal{P} \xleftarrow{\$} \mathsf{Perms}(\{0,1\}^n)]$ that a is a fixed point of a randomly drawn permutation $\mathcal{P}$?
4. Let a be as above; what is the probability $q_a = \Pr[\mathcal{P}(\mathcal{P}(a)) = a |\, \mathcal{P}(a) \neq a : \mathcal{P} \xleftarrow{\$} \mathsf{Perms}(\{0,1\}^n)]$ that a is in a cycle of length two, conditioned on the fact that a is not a fixed point?
5. Show that $\mathcal{F}$ is not a good block cipher, by specifying an algorithm with $q = 1$, $t = 2$ that distinguishes it from a random permutation. Give an analysis of the advantage of your algorithm. (Hint: compare the values $\mathcal{O}(\mathcal{O}(a))$ in function of how $\mathcal{O}$ is instantiated. Then find in which cases your algorithm fails, and the probability of failure (or equivalently of success) in function of p_a and q_a.)
6. Give a reasonable alternative defintion for PRP advantage (that only changes the definition of $\mathcal{O}$) where the algorithm of the previous question has advantage zero.

Q. 4: In order to make $\mathcal{F}$ non-involutory, one suggests to use two keys for the two internal calls to $\mathcal{E}$. That is, one redefines $\mathcal{F}$ as following. Let k_1, $k_2 \in \{0,1\}^\kappa$, $c_R = x_L \oplus \mathcal{E}(k_1, x_R)$, $c_L = x_R \oplus \mathcal{E}(k_2, c_R)$, then $\mathcal{F}(k_1||k_2, x_L||x_R) = c_L||c_R$.

1. Show that if $k_1 \neq k_2$, then $\mathcal{F}$ is not (necessarily) an involution.
2. Let $c_L||c_R = \mathcal{F}(k_1||k_2, x_L||x_R)$; $c'_L||c'_R = \mathcal{F}(k_1||k_2, x'_L||x_R)$ with $x'_L \neq x_L$. Give a simple expression for $c_R \oplus c'_R$.
3. Show that $\mathcal{F}$ is not a good block cipher, by specifying an efficient algorithm to distinguish it from a random permutation (you don't need to precisely analyse the advantage of your algorithm).

Q. 5: The structure of the two previous questions can be generalized to more *rounds*. Let $k_1|| \ldots ||k_r \in \{0,1\}^{r\kappa}$, $x_L||x_R \in \{0,1\}^{2n}$. One defines x_L^0 and x_R^0 as x_L and x_R respectively; $x_R^i = x_L^{i-1} \oplus \mathcal{E}(k_i, x_R^{i-1})$, $x_L^i = x_R^{i-1}$; $c_L = x_R^r$, $c_R = x_L^r$.

1. Give a lower bound for the number of round r for such a structure to result in a good block cipher.

Note: The structure studied in **Q. 3** $\sim$ **Q. 5** is a *Feistel* structure/network/ladder.