Cryptology complementary
Exercices#2

2018-W07

Exercise 1: PRPs

Q.1: Let $\mathscr{E} : \{0,1\}^\kappa \times \{0,1\}^n \to \{0,1\}^n$ be a block cipher for which there is a subset $\mathscr{K}' \subset \{0,1\}^\kappa$ of *weak keys* of size 2^w such that if $k \in \mathscr{K}'$, $\mathscr{E}(k,\cdot) : x \mapsto x$.

Give a lower-bound for $\mathbf{Adv}^{\mathrm{PRP}}_{\mathscr{E}}(1,1)$.

Q.2: Some mode of operation of block ciphers rely on the fact that $\mathscr{E}(k,0)$ is an unpredictable value when k is random and secret (with 0 denoting the all-zero binary string).

Show that this is a reasonable assumption. More precisely, give a lower-bound on $\mathbf{Adv}^{\mathrm{PRP}}_{\mathscr{E}}(1,1)$ assuming that one can predict this value with unit time and success probability p.

Q.3: Assume that $\mathscr{E}$ is a "good" block cipher. Define a related cipher $\mathscr{E}'$ for which $\mathscr{E}(k,0)$ is trivially predictable for any key (several constructions are possible).

Exercise 2: Meet-in-the-middle attack

Let $\mathscr{E} : \{0,1\}^\kappa \times \{0,1\}^n \to \{0,1\}^n$ be a block cipher. Assuming that κ is too small to provide adequate security against generic attacks, one wishes to define another cipher $\mathscr{E}'$ with larger keys. A possible construction is to use "double-encryption" and have $\mathscr{E}' : \{0,1\}^\kappa \times \{0,1\}^\kappa \times \{0,1\}^n \to \{0,1\}^n$ defined as $\mathscr{E}'(k,k',\cdot) : x \mapsto \mathscr{E}(k,\mathscr{E}(k',x))$.

Q.1: Show that double-encryption only marginally increases the "effective" key length by giving an attack that works with time 2^κ, memory 2^n, a negligble amount of queries, and success probability 1.

Hint: Observe that the outer and inner keys are used in sequence. Try to find a partially encrypted value that can be obtained by partial encryption with k' or partial decryption with k. Use this to "meet in the middle".

Q.2: The attack of the previous question can be interrupted after t steps in a "natural way". How? What is the probability of successfully finding (k,k') in function of t and κ. How does this compare with $\mathscr{E}$ (assuming that $\mathscr{E}$ is "good", i.e. $\mathbf{Adv}^{\mathrm{PRP}}_{\mathscr{E}}(q,t) \approx t/2^\kappa$)?