Homework 7

Homework is due by **11pm of Nov 4**. Send by email to both "regev" (under the cs.nyu.edu domain) and "des480" (under the nyu.edu domain) with subject line "CSCI-GA 3210 Homework 7" and name the attachment "YOUR NAME HERE HW7.tex/pdf". There is no need to print it. Start early!

1. (3 points) *(Feistel.)* Show that if we repeat the Feistel construction any number of times *with the same function* f, the result is not a PRP. (In contrast, in class we showed that if we use three functions f_1, f_2, f_3 independently chosen from a PRF family, the result is a PRP)I need a hint! (ID 91716)

2. *(Security definitions of SKE.)*[1]

   (a) (1 point) Multi-message *non-adaptive* security for a symmetric-key encryption scheme $(\mathsf{Gen}, \mathsf{Enc}, \mathsf{Dec})$ says that for any $q = \mathrm{poly}(n)$ and any tuples $(m_1, \ldots, m_q), (m'_1, \ldots, m'_q) \in \mathcal{M}^q$, it should be the case that

   $$(\mathsf{Enc}_k(m_1), \ldots, \mathsf{Enc}_k(m_q)) \stackrel{c}{\approx} (\mathsf{Enc}_k(m'_1), \ldots, \mathsf{Enc}_k(m'_q)), \tag{IND1}$$

   where in both cases the distribution is over the choice of $k \leftarrow \mathsf{Gen}$ and the randomness in the encryption procedure. Show that the encryption procedure in multi-message non-adaptive secure scheme must be randomized (in contrast to that in single-message secure schemes).

   (b) (3 points) Show that multi-message non-adaptive security can be equivalently defined as saying that for any $q = \mathrm{poly}(n)$ and any $m_1, \ldots, m_q, m_0, m'_0 \in \mathcal{M}$, it should be the case that

   $$(\mathsf{Enc}_k(m_1), \ldots, \mathsf{Enc}_k(m_q), \mathsf{Enc}_k(m_0)) \stackrel{c}{\approx} (\mathsf{Enc}_k(m_1), \ldots, \mathsf{Enc}_k(m_q), \mathsf{Enc}_k(m'_0)), \tag{IND2}$$

   where in both cases the distribution is over the choice of $k \leftarrow \mathsf{Gen}$ and the randomness in the encryption procedure. I need a hint! (ID 17499)

   (c) (3 points) A stronger definition of security is *adaptive* (or *IND-CPA*) security, defined as the oracle indistinguishability

   $$(\mathsf{Enc}^0_k(\cdot,\cdot)) \stackrel{c}{\approx} (\mathsf{Enc}^1_k(\cdot,\cdot)), \tag{INDCPA1}$$

   where $\mathsf{Enc}^b_k(m_0, m_1)$ outputs $\mathsf{Enc}_k(m_b)$ and $k \leftarrow \mathsf{Gen}$. Show that an equivalent definition is

   $$(\mathsf{Enc}_k(\cdot), C^0_k(\cdot,\cdot)) \stackrel{c}{\approx} (\mathsf{Enc}_k(\cdot), C^1_k(\cdot,\cdot)), \tag{INDCPA2}$$

   where $C^b_k(m_0, m_1)$ outputs $\mathsf{Enc}_k(m_b)$ on receiving the first query and then ignores all further queries (this represents the "challenge"), and $k \leftarrow \mathsf{Gen}$. I need a hint! (ID 17499)

   (d) (4 points) Give a separation between the non-adaptive and the adaptive security definitions, i.e., construct a (possibly contrived) scheme and prove it secure according to the former definition (under some standard assumption), while showing that it is definitely insecure according to the latter definition. I need a hint! (ID 17495)

   (e) (2 points) (Extra credit)[2] Consider the weakening of the definition of multi-message non-adaptive security in which we take q to be some fixed polynomial, say, $q = n^2$. Show a separation between this definition and the original one.

[1] Based on a question from Peikert's class.

[2] A question asked in class by Konstantinos Vamvourellis