Selected Topics on Cryptology 2009
(Home work 2)

June 13, 2009

- Due on June 30, 10 am.
- Late submissions will not be accepted.
- Please give precise arguments for all statements that you write.
- Please do not hesitate to contact me if you do not understand the problems.

1. Let F be a pseudo-random function. Show that the following constructions are insecure as message authentication codes (in each case $K \in \{0,1\}^n$ is the private key):

   (a) To authenticate a message $m = m_1||m_2||\ldots||m_\ell$ where $m_i \in \{0,1\}^n$, compute $t = F_k(m_1) \oplus F_K(m_2) \oplus \ldots \oplus F_K(m_\ell)$ as the tag.

   (b) To authenticate a message $m = m_1||m_2||\ldots||m_\ell$ where $m_i \in \{0,1\}^n$, do the following:

$$\begin{aligned} r &\xleftarrow{\$} \{0,1\}^n \\ t &\leftarrow F_k(r) \oplus F_k(m_1) \oplus F_K(m_2) \oplus \ldots \oplus F_K(m_\ell) \\ &\quad \text{send } (r,t) \end{aligned}$$

2. Let g is an element of prime order in the group $\mathbb{Z}_p^*$. Suppose we have an efficient algorithm which computes the Diffie Hellman function in base g, i.e., we have an algorithm $\mathcal{A}$ such that $\mathcal{A}(g^x, g^y) = g^{xy}$ for all $x, y \in \{1, 2, \ldots q\}$. Let $h = g^\alpha$ for some $\alpha \in \{1, 2, \ldots, q-1\}$. Show that given α there is an efficient algorithm $\mathcal{B}$ which can compute the Diffie-Hellman problem at base h, i.e., $\mathcal{B}(h, \alpha, h^x, h^y) = h^{xy}$. Algorithm $\mathcal{B}$ can use algorithm $\mathcal{A}$ as a subroutine.

3. A natural way of applying hybrid encryption to the El-Gamal encryption scheme is as follows. The public key $pk = g^x$, where g is the generator of a group G, where G is of prime order and the DDH assumption hold on G. To encrypt a message m, the sender chooses $k \xleftarrow{\$} \{0,1\}^n$ and sends

$$(g^r, g^{rx}.k, \mathsf{Enc}_k(m)),$$

where $r \xleftarrow{\$} \mathbb{Z}_q$ is is chosen at random, and Enc represents a symmetric key encryption scheme. The above scheme needs to transmit two group elements along with the cipher produced by the symmetric encryption scheme.

(a) Suggest an improvement over this scheme, where the length of the cipher text would be shorter, i.e., suggest a scheme only one group element needs to be transmitted along with the cipher-text of the symmetric encryption.

(b) Can you suggest a way of adding a message authentication to this scheme.