Selected Topics on Cryptology 2011
(Home work II)

July 7, 2011

- Due on July 22, 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. The CBC-Chain mode of operation is a CBC variant in which the IV that is used for the very first message to be encrypted is randomly selected, where as the IV used for each subsequent encrypted message is the last block of ciphertext that was generated. Show that CBC-Chain is insecure by constructing an efficient IND-CPA adversary.

2. Let E_K be a symmetric encryption scheme encrypting messages in $\{0,1\}^n$. We wish to construct a symmetric encryption scheme $\hat{E}_K$ (based on $E_K()$) for encrypting messages in $\{0,1\}^{n-1}$. For encrypting messages in $\{0,1\}^{n-1}$ we do the following

   Algorithm $\hat{E}_K(M)$
   $C_1 \leftarrow E_K(0||M)$;
   while $(\mathsf{msb}(C_1) \neq 0)$
   $C_1 \leftarrow E_K(C_1)$
   $C_1 \leftarrow \mathsf{drop}(C_1)$;
   return C_1

   Where $\mathsf{msb}(X)$ returns the most significant bit of X and $\mathsf{drop}(X)$ removes the most significant bit of X.

   (a) Show that the above encryption algorithm is well defined i.e., one can decrypt unambiguously if such an encryption procedure is followed

   (b) Assuming that E_K is a random permutation then $\hat{E}_K$ will also be so.

3. Consider a symmetric encryption scheme $\mathcal{SE} = (\mathcal{K}, \mathcal{E}, \mathcal{D})$. The oracle \$(.) responds to the query x of A by returning $|\mathcal{E}(x)|$ many uniform random bits. The IND\$ advantage of A is defined as

$$\mathbf{Adv}^{\text{ind\$}}_{\mathcal{SE}}(A) \;=\; \Pr\left[K \xleftarrow{\$} \mathcal{K} : A^{\mathcal{E}_K(.)} \Rightarrow 1\right] - \Pr\left[A^{\$(.)} \Rightarrow 1\right]$$

$\mathcal{SE}$ is considered secure in the IND\$ sense if for all efficient adversaries A the IND\$ advantage is small.

   (a) Show that security in the IND\$ sense implies security in the IND-CPA sense.

   (b) Show that the CTR\$ scheme is secure in the IND\$ sense.

4. 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:

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