Selected Topics on Cryptology 2009
(Home work 1)

May 28, 2009

- Due on June 11, 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 $\mathrm{Perm}(n)$ denote the set of all permutations from $\{0,1\}^n$ to $\{0,1\}^n$ and $\mathrm{Func}(n,\ell)$ be the set of all functions from $\{0,1\}^n$ to $\{0,1\}^\ell$. Find $|\mathrm{Perm}(n)|$ and $|\mathrm{Func}(n,\ell)|$.

2. Let $x \overset{\$}{\leftarrow} X$ denote the event of choosing x from the set X uniformly at random. Give the values of the following probabilities:

   (a) $\Pr[x \overset{\$}{\leftarrow} \{0,1\}^4 : x = 0100]$

   (b) $\Pr[x \overset{\$}{\leftarrow} \{0,1\}^{10}, y \overset{\$}{\leftarrow} \{0,1\}^{10} : x = y]$

3. 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.

4. Given a pseudorandom function family $\mathcal{F} : \mathcal{K} \times \{0,1\}^n \rightarrow \{0,1\}^\ell$, construct a family $\mathcal{G} : \mathcal{K} \times \{0,1\}^n \rightarrow \{0,1\}^{2\ell}$ as $G_K(X) = F_K(X)||F_K(F_K(X))$. Is $\mathcal{G}$ pseudorandom, if so give a proof otherwise design an efficient adversary which breaks $\mathcal{G}$ in the prf sense.

5. Given a pseudorandom function family $\mathcal{F} : \mathcal{K} \times \{0,1\}^n \rightarrow \{0,1\}^\ell$, construct a family $\mathcal{G} : \mathcal{K} \times \{0,1\}^{2n} \rightarrow \{0,1\}^{2\ell}$ as follows: given $X \in \{0,1\}^{2n}$ let $X = X_1||X_2$ such that $X_1, X_2 \in \{0,1\}^n$, construct $G_K(X) = F_K(F_K(X_1) \oplus X_2)$. Is $\mathcal{G}$ pseudorandom, if so give a proof otherwise design an efficient adversary which breaks $\mathcal{G}$ in the prf sense.

6. 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

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

$\mathcal{SE}$ 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.