Cryptology 2012
(Home work 3)

April 5, 2012

- Due on April 2, 10 am. Hard copies of solutions are to be submitted.
- 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. Given a pseudorandom function family $\mathcal{F} : \mathcal{K} \times \{0,1\}^n \to \{0,1\}^n$, construct a family $\mathcal{G} : \mathcal{K} \times \{0,1\}^n \to \{0,1\}^{2n}$ as $G_K(X) = F_K(X)||F_K(F_K(X))$. Is $\mathcal{G}$ pseudo-random, if so give a proof otherwise design an efficient adversary which breaks $\mathcal{G}$ in the prf sense.

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 $(\mathsf{msb}(C_1) \neq 0)$
   $C_1 = E_K(C_1)$
   $C_1 = \mathsf{drop}(C_1)$;
   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. Let F be a length preserving pseudorandom function. Define a keyed permutation $F^{(3)}$ as follows:

   - **Inputs:** A key $k \in \{0,1\}^{3n}$ parsed as $k = (k_1, k_2, k_3, k_4)$ with $|k_i| = n$, and an input $x \in \{0,1\}^{2n}$ parsed as (L_0, R_0) with $|L_0| = |L_1| = n$.

- **Computation:**
  (a) $L_1 \leftarrow R_0$; $R_1 \leftarrow L_0 \oplus F_{k_1}(R_0)$;
  (b) $L_2 \leftarrow R_1$; $R_2 \leftarrow L_1 \oplus F_{k_2}(R_1)$;
  (c) $L_3 \leftarrow R_2$; $R_3 \leftarrow L_2 \oplus F_{k_3}(R_2)$;
  (d) **Output** (L_3, R_3)

Show that $F^{(3)}$ as defined above is not a strong pseudorandom permutation.

4. 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.

5. 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:

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

6. Let R, S, and T be finite, non-empty sets. Suppose that for each $r \in R$, we have a function $h_r : S \to T$. In other words $\{h_r\}_{r\in R}$ is a family of keyed hash functions from S to T

   We say that the family of hash functions $\{h_r\}_{r\in R}$ is pairwise independent, if for all $s, s' \in S$, $s \neq s'$ and for all $t, t' \in T$

$$\Pr[r \xleftarrow{\$} R : h_r(s) = t \wedge h_r(s') = t'] = \frac{1}{|T|^2}.$$

   We say that the family of hash functions $\{h_r\}_{r\in R}$ is ϵ-almost universal, if for all $s, s' \in S$, $s \neq s'$,

$$\Pr[r \xleftarrow{\$} R : h_r(s) = h_r(s')] \leq \epsilon.$$

(a) Show that if a function family is pairwise independent then it is $\frac{1}{|T|}$-almost universal.

(b) Let p be an odd prime. For $a, b \in \mathbb{Z}_p$ define $h_{a,b} : \mathbb{Z}_p \to \mathbb{Z}_p$ by the rule

$$h_{a,b}(x) = (x + a)^2 + b \pmod{p}.$$

Prove that the family $\{h_{a,b}\}$ is $\frac{1}{p}$-almost universal.

7. Consider a simplified version of Merkle-Damgard construction. Let $\mathsf{comp} : \{0,1\}^{m+t} \to \{0,1\}^m$, where $t \geq 1$, and suppose that

$$x = x_1||x_2|| \cdots ||x_k,$$

where $|x_1| = |x_2| = \cdots = |x_k| = t$. Consider the following iterated hash function:

Algorithm Simplified Merkle-Damgard
$z_1 \leftarrow 0^m||x_1$
$g_1 \leftarrow \mathsf{compress}(z_1)$
for $i \leftarrow 1$ to $k-1$,
$z_{i+1} \leftarrow g_i||x_{i+1}$
$g_{i+1} \leftarrow \mathsf{compress}(z_{i+1})$
end for
$h(x) \leftarrow g_k$
return $(h(x))$

Suppose that compress is collision resistant, and further it is zero preimage resistant, i.e., it is hard to find $z \in \{0,1\}^{m+t}$, such that $\mathsf{compress}(z) = 0^m$. Under these assumptions prove that h is collision resistant.