# Selected Topics on Cryptology 2011
# (Home work )

June 27, 2011

- Due on July 7, 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. Consider a cryptosystem in which $\mathcal{P} = \{a, b, c\}$, $\mathcal{K} = \{K_1, K_2, K_3\}$ and $C = \{1, 2, 3, 4\}$. Suppose the encryption matrix is as follows:

| | $a$ | $b$ | $c$ |
|---|---|---|---|
| $K_1$ | 1 | 2 | 3 |
| $K_2$ | 2 | 3 | 4 |
| $K_3$ | 3 | 4 | 1 |

   Given that the keys are chosen with equal probability and the plaintext distribution is

$$\Pr[a] = \frac{1}{2}, \Pr[b] = \frac{1}{3}, \Pr[c] = \frac{1}{6}.$$

   Find the probability distribution on $\mathcal{C}$. Does this crypto-system provide perfect secrecy?

2. 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 $|\mathrm{Func}(n, \ell)|$.

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

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

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

4. Given a pseudorandom function family $\mathcal{F} : \mathcal{K} \times \{0,1\}^n \to \{0,1\}^\ell$, construct a family $\mathcal{G} : \mathcal{K} \times \{0,1\}^n \to \{0,1\}^{2\ell}$ 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.

5. 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.

6. Let $H : \mathcal{K} \times \{0,1\}^\ell \to \{0,1\}^{\ell_1}$ be a function family where $\ell > \ell_1$. Additionally the family $H$ has the property that for all $x, x' \in \{0,1\}^\ell$ with $x \neq x'$

$$\Pr[K \xleftarrow{\$} \mathcal{K} : H_K(x) = H_K(x')] \leq \epsilon.$$

   Such a function family is called an $\epsilon$-universal family. Also let $F : \mathcal{S} \times \{0,1\}^{\ell_1} \to \{0,1\}^{\ell_2}$, be a function family. Given $H$ and $F$ we define a new family of functions $G : \mathcal{K} \times \mathcal{S} \times \{0,1\}^\ell \to \{0,1\}^{\ell_2}$, such that for every $(K, S) \in \mathcal{K} \times \mathcal{S}$, $G_{K,S} : \{0,1\}^\ell \to \{0,1\}^{\ell_2}$, is defined as $G_{K,S}(x) = F_S(H_K(x))$, where $x \in \{0,1\}^\ell$. Show that if $H$ is $\epsilon$-universal and $F$ is pseudo-random then $G$ is also pseudo-random.