Selected Topics on Cryptology 2010
(Home work)

August 5, 2010

- Due on August 20, 10 am.
- Problems 1-8 are compulsory, and you can choose one among problems 9 and 10.
- 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 $x \xleftarrow{\$} X$ denote the event of choosing x from the set X uniformly at random. Give the values of the following probabilities:

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

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

4. 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.

5. Assume that a sender encrypts a message of m blocks using the CBC mode. During transmission, block number $m/2$ gets corrupted. After the receiver decrypts the cipher, how many blocks of the decrypted message would be corrupted?

6. 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.

7. 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.

8. 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:

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

9. 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.

10. 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 ϵ-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 ϵ-universal and F is pseudo-random then G is also pseudo-random.