Cryptology 2014
(Home work 2)

March 3, 2014

- Due on March 20, 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. 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. For $k = (k_1, k_2, k_3)$ define $\mathsf{3DES}_k(X) = \mathsf{DES}_{k_3}\left(\mathsf{DES}_{k_2}^{-1}(\mathsf{DES}_{k_1}(X))\right)$. Let $P, C \in \{0,1\}^{64}$ be such that $C = \mathsf{3DES}_k(P)$. We apply the following algorithm for an exhaustive key search on 3DES

   Algorithm Exhaustive(P, C)
   for each possible key $K = (K_1, K_2, K_3)$
   if $\mathsf{3DES}_K(P) == C$,
   output $K = (K_1, K_2, K_3)$
   end if
   end for

(a) How many calls to DES is performed by the above algorithm?

(b) If we assume that DES behaves like a random permutation, i.e, for any fixed $P, C \in \{0,1\}^{64}$

$$\Pr[k \xleftarrow{\$} \{0,1\}^{56} : \mathsf{DES}_k(P) = C] = \Pr[\pi \xleftarrow{\$} \mathrm{Perm}(64) : \pi(P) = C].$$

Then, how many wrong keys would be output by the algorithm Exhaustive in average?

(c) Now, suppose you have at your disposal q plaintext/ciphertext pairs (P_i, C_i), such that $C_i = \mathsf{3DES}_k(P_i)$, for $1 \leq i \leq q$. Write an algorithm similar to the algorithm Exhaustive to perform an exhaustive search in this scenario such that the number of wrong keys displayed by the algorithm is reduced. How many DES encryption/decryption is performed by your algorithm.

(d) How many wrong keys are now displayed by the modified algorithm on average (give an estimate as a function of q). What would be the value of q such that we can be almost sure that no wrong key would be displayed by the algorithm.

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 $\mathcal{F} : \mathcal{K} \times \{0,1\}^n \to \{0,1\}^n$, 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.

5. 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.

6. 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 $k = (k_1, k_2, k_3)$ 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.

7. For a function $g : \{0,1\}^n \to \{0,1\}^n$, define an oracle $g^{\$}(.)$ as follows. On an input $x \in \{0,1\}^n$, the oracle selects r uniformly at random from $\{0,1\}^n$ and outputs $(r, g(r))$. Given a function family $F : \{0,1\}^k \times \{0,1\}^n \to \{0,1\}^n$, define the WPRF advantage of an adversary $\mathcal{A}$ as

$$\mathbf{Adv}_F^{\text{wprf}}(\mathcal{A}) = \Pr\left[K \xleftarrow{\$} \{0,1\}^k : \mathcal{A}^{F_K^{\$}(.)} \Rightarrow 1\right] - \Pr\left[\rho \xleftarrow{\$} \mathsf{Func}(n,n) : \mathcal{A}^{\rho^{\$}(.)} \Rightarrow 1\right].$$

   The family F is called a weak *pseudo-random function* if for every adversary $\mathcal{A}$ with reasonable resources $\mathbf{Adv}_F^{\text{wprf}}(\mathcal{A})$ is small.

   (a) Prove that if a function family is pseudo-random then it is also weak pseudo-random.

   (b) Let $G : \{0,1\}^k \times \{0,1\}^n \to \{0,1\}^n$ is a pseudorandom family. Define a new family $F : \{0,1\}^k \times \{0,1\}^n \to \{0,1\}^n$ as

$$F_K(x) = \begin{cases} G_K(x) & \text{if } x \text{ is even} \\ G_K(x+1) & \text{if } x \text{ is odd.} \end{cases}$$

   Show that F is weakly pseudo-random but not pseudo-random.

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:

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

9. 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.

10. [**Implementation**] Do a software implementation of AES-128 for both encryption and decryption using any programming language of your choice.