Cryptology 2012
(Home work 2)

February 14, 2012

- Due on March 5, 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. 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. Let $\pi \xleftarrow{\$} \mathrm{Perm}(64)$, and $P, C \in \{0,1\}^{64}$ be fixed. Find $\Pr[\pi(P) = C]$.

5. Show that DES has the property $\mathsf{DES}_k(x) = \overline{\mathsf{DES}_{\bar{k}}(\bar{x})}$, for every key k and input x. Here $\bar{z}$ denotes the bitwise complement of z. This property is called key complementarity property
   Hint: To prove this the high level description of DES is enough, the specific structure of the S-boxes would not be required to prove this property.

6. Using the key complementarity property deduce a brute force attack against DES with average complexity of 2^{54} DES encryptions.
   Hint: Assume that the adversary who is looking for K is given a plaintext block x and the two values corresponding to $\mathsf{DES}_K(x)$ and $\mathsf{DES}_K(\bar{x})$.

7. Let S be a finite set and let $f : S \to S$ be a bijection. The function f is an involution if $f(f(x)) = x$ for all $x \in S$. We say that a DES key k is weak if DES_k is an involution. Exhibit four weak keys for DES.

8. 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?
   Hint: You already have the value of $\Pr[\pi \xleftarrow{\$} \mathrm{Perm}(64) : \pi(P) = C]$ computed in problem 4. Use this value.

   (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 $1 \le i \le q$. 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.

9. Do a software implementation of AES-128 for both encryption and decryption using any programming language of your choice.