CS 4390/5390 Fall 2013
Shirley Moore, Instructor
Homework 6
Due Tuesday, November 26

1. **Symmetric encryption with a deck of cards**. Alice randomly shuffles a deck of cards and deals it all out to herself and to Bob (each of them gets half of the 52 cards). Alice now wishes to send a secret message *m* to Bob by saying something aloud. Eavesdropper Eve is listening in: she hears everything Alice says (but Eve can't see the cards).
(a) Suppose Alice's message *m* is a string of 48 bits. Describe how Alice can use the cards to communicate *m* to Bob in such a way that Eve will have no information about *m*.
(b) Now suppose Alice's message *m* is 49 bits. Prove that no protocol (using the cards) can exist that allows Alice to communicate *m* to Bob in such a way that Eve will have no information about *m*.

2. (a) Show that for all $k \in \{0,1\}^{56}$ and all $m \in \{0,1\}^{64}$, $DES_k(m) = \overline{DES_{\bar{k}}(\bar{m})}$. This is called the key-complementation property of DES.
(b) Explain how to use the key-complementation property of DES to speed up exhaustive key search by about a factor of two. Explain any assumptions you make.

3. Find a key *k* such that $DES_k(x) = DES_k^{-1}(x)$ for all $x \in \{0,1\}^{64}$. Such a key is called a "weak" kdy.

4. (a) Let $F : \{0,1\}^n \rightarrow \{0,1\}^n$ be a random function. Randomly pick $x_1, x_2, \ldots, x_r \in \{0,1\}^n$ and compute $y_i = F(x_i),\ i = 1, \ldots, r$. What is the probability that all the y_i are distinct?
(b) How many different permutations are there from 128 bits to 128 buts?
(c) How many different functions are there from 128 bits to 128 bits?
(d) Find the tightest upper and lower bounds you can for the probability that a random function from 128 bits to 128 bits is actually a permutation.

5. Read IEFT RFC 4772 Security Implications of Using DES at http://www.ietf.org/rfc/rfc4772.txt .
(a) Summarize the security vulnerabilities of DES.
(b) How is the recommendation that DES keys be refreshed after encoding 2^{32} blocks related to the Birthday Paradox?