Introduction to Cryptography

Homework 1

Due by March 18, 2008.

1. Let n be a positive integer, a *Latin square* of order n is an $n \times n$ square which contains the integers 1 to n, such that each of the n integers appears exactly once in every row and every column. For example, here is a 3×3 Latin square:

3	2	1
1	3	2
2	1	3

   Given a Latin square L of order n we can define an encryption system in which $[1,n]$ is the range of plaintexts, of ciphertexts, and of the keys. For a key k in $[1,n]$ and a plaintext m in $[1,n]$, the encryption is defined as $Enc_k(m)=L[k,m]$, namely the entry in row k and column m of the square L.

   Prove that if every key is chosen with equal probability, then this is a perfect cryptosystem. (Prove this statement for a general Latin square, not for the example given above.)

2. (Shannon's theorem)
   Consider an encryption scheme where the size of the plaintext space (P) is equal to the size of the ciphertext space (C), and is also equal to the size of the key space (K). (Namely $|P|=|C|=|K|$.) Then the encryption scheme provides perfect secrecy *if and only if* the following two conditions hold:
   - Every key is chosen with equal probability $(1/|K|)$.
   - For every message m in P and every possible ciphertext c in C, there exists a single key k in K, such that $E_k(m)=c$.

   Prove *one* of the two directions of the theorem (namely, either the "if" direction or the "only if" direction.).

3. Consider the following encryption system (similar to the one described in Lecture 2). The key is a (short) random key $k \in \{0,1\}^{|k|}$. The message is $m= m_1,\ldots,m_{|m|}$. The system uses a PRG $G : \{0,1\}^{|k|} \rightarrow \{0,1\}^{|2m|}$.
   A message is encrypted in the following way. Let $g=g_1 \ldots g_{2|m|}$ denote the output of $G(k)$. The ciphertext is $m_1 \oplus g_1 \oplus g_{|m|+1}$, $m_2 \oplus g_2 \oplus g_{|m|+2}, \ldots, m_{|m|} \oplus g_{|m|} \oplus g_{2|m|}$.

   Prove that if the PRG is strong then this encryption is secure. Do this by showing that if the encryption is not secure in the sense of indistinguishability, then the PRG is also not strong. In other words, show that if there are two message m,m' such that there is a polynomial time adversary D that can distinguish between the encryptions of m and of m', then there is a distinguisher that is given a 2|m| bit string and can tell whether this string was chosen from the set of outputs of the PRG, or was chosen uniformly at random).