Introduction to Cryptography

Homework 1

Due by November 15, 2009.

1. (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 *both* directions of the theorem.

2. An encryption scheme works in the following way. Let $1<m<n$ be positive integers whose greatest common divisor is 1. The key of the encryption scheme is the pair *(m,n)*. Partition the plaintext to segments of *n* letters each. Denote the letters of a plaintext segment as $p_0,p_1,\ldots,p_{n-1}$. The ciphertext is defined as the following word: $p_m,p_{2m \bmod n}, p_{3m \bmod n}, \ldots, p_{(n-1)m \bmod n}, p_{nm \bmod n}$. (Note that all letters of the plaintext appear in the ciphertext.)
   For example, if n = 12; m = 5 the plaintext "cryptography" will be encrypted as "ohpargytpurc".
   A more advanced encryption scheme (which we will denote as scheme B) works by first applying a monoalphabetic substitution cipher, followed by a applying the encryption scheme described above.
   Describe an effective method for breaking long enough ciphertexts, encrypted by this encryption scheme B. You can assume that the plaintext is a text in English. The overhead of your algorithm must be polynomial in the length of the ciphertext. Limit your answer to no more than 8 lines.

3. Let *G* be a function that maps strings of length *n* to strings of length *2n*. Define $\beta(n)$ = Prob(the $(n+1)^{th}$ bit of $G(x)$ is equal to '1')
   where the probability is taken over random choice of $x \in \{0,1\}^n$. Prove that if *G* is a pseudorandom generator, then there is a negligible function $\varepsilon()$ for which it holds that $\beta(n) < \frac{1}{2} + \varepsilon(n)$.
   You should give a formal proof, not just an intuitive argument.

   Hint: Prove first that it cannot be that $\beta(n) > 2/3$.
   Then show that for any constant $c>0$ it cannot be that $\beta(n) > \frac{1}{2} + c$.
   Finally show that for any polynomial $p(n)$ there must be an N such that for all $n>N$ it holds that $\beta(n) < \frac{1}{2} + 1/p(n)$. This solves the question.