T-79.503 Foundations of Cryptology
Homework 4
October 14, 2004

1. (Stinson 2.11) Based on the definition of perfect secrecy and theorems and corollaries given in the text book, prove that a cryptosystem has perfect secrecy if and only if H($\mathbf{P}|\mathbf{C}$)= H($\mathbf{P}$).

2. Prove that, in any cryptosystem

   a) H($\mathbf{C}|\ \mathbf{K}$) = H($\mathbf{P}$)

   b) (Stinson 2.12) H($\mathbf{P}|\mathbf{C}$) $\leq$ H($\mathbf{K}|\mathbf{C}$)

   c) (Shannon's pessimistic inequality) If cryptosystem has perfect secrecy then H($\mathbf{P}$) $\leq$ H($\mathbf{K}$).

3. Plaintext is formed by independent bits arranged in blocks of eight bits. The probability that a plaintext bit equals 0 is p. Each block $x_1, x_2, \ldots, x_8$ is encrypted using one key bit z by adding it modulo 2 to each plaintext bit. Hence the ciphertext block is $y_1, y_2, \ldots, y_8$ where $y_i = x_i \oplus z$, $i = 1, 2, \ldots, 8$. It is assumed that every key bit is generated uniformly at random. Assume you see a ciphertext block with k zeroes and $8-k$ ones, $k = 0, 1, 2, \ldots, 8$.

   a) Determine the probability that the encryption key was $z = 0$.

   b) What kind of ciphertext maximizes this probability?

   c) Which ciphertext does not give any information at all about the used key bit?

4. Consider a language where messages are strings of letters chosen independently from the set $\{a, b, c, d\}$ with the following probability distribution:

   $$p(a) = \frac{1}{2},\ p(b) = \frac{1}{4},\ \text{ and } p(c) = p(d) = \frac{1}{8}.$$

   a) Compute the redundancy of this language.

   b) Prior to encryption the messages are coded into strings of bits using the following coding rule:

   $$a \mapsto 00,\ \ b \mapsto 01,\ \ c \mapsto 10,\ \ \ d \mapsto 11,$$

   Compute the redundancy of this plaintext language.

5. The keystream z_i, $i = 1, 2, \ldots$ of a binary stream cipher is generated by repeating a finite random sequence k_j, $j = 1, 2, \ldots, m$, of length m. Hence $z_i = k_i$, for $i = 1, 2, \ldots, m$, and $z_{i+m} = z_i$, for all $i = 1, 2, \ldots$. This stream cipher is used to encrypt plaintext with redundancy R_L. Give an estimate for the unicity distance.

6. The DES keys are 64 bits long, where each eighth bit is a parity bit computed as a modulo 2 sum of the preceding seven bits. A key management center uses DES encryption algorithm and a "master" DES key to encrypt DES keys to end users. Each ciphertext block consists of one encrypted DES key. Estimate the unicity distance of this cryptosystem, that is, estimate the number of encrypted end users' DES keys that an attacker needs to uniquely compute the master key given enough computing time.