T-79.5501 Cryptology
Homework 1
September 22 and 23, 2005

1. Plaintext is formed of independent bits arranged in blocks of four bits. The probability that a plaintext bit equals 0 is p. Each block x_1, x_2, x_3, x_4 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, y_3, y_4 where $y_i = x_i \oplus z$, $i = 1, 2, 3, 8$. It is assumed that every key bit is generated uniformly at random. Assume you see a ciphertext block with k zeroes and $4 - k$ ones, $k = 0, 1, 2, 3, 4$.

   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?

2. Consider a cryptosystem where $\mathcal{P} = \{A, B\}$ and $\mathcal{C} = \{a, b, c\}$, $\mathcal{K} = \{1, 2, 3, 4\}$, and the encryption mappings e_K are defined as follows:

K	$e_K(A)$	$e_K(B)$
1	a	b
2	b	c
3	b	a
4	c	a

   The keys are chosen with equal probability.

   a) Show that
   $$\mathbf{Pr}[\mathbf{x} = A|\mathbf{y} = a] = \frac{\mathbf{Pr}[\mathbf{x} = A]}{2 - \mathbf{Pr}[\mathbf{x} = A]}.$$
   b) Does this cryptosystem have perfect secrecy?

3. A PIN code for a smart card is a number of four decimal digits (p_1, p_2, p_3, p_4), where each p_i, $i = 1, 2, 3, 4$, is derived from a uniformly distributed random string of 16 bits $(r_1, r_2, ..., r_{16})$ by computing

   $$p_i = (r_{4i-3} + r_{4i-2} \cdot 2 + r_{4i-1} \cdot 2^2 + r_{4i} \cdot 2^3) \bmod 10.$$

   Determine the entropy of the PIN code. Compare it with the maximum entropy of a string of four decimal digits.

4. A positive real valued function h is defined in the interval [0,1] such that $h(p) = -p \log_2 p - (1 - p) \log_2(1 - p)$, for $0 < p < 1$, and $h(0) = h(1) = 0$. Then h is continuous at 0 and 1, and $h(p)$ is the entropy of a binary valued random variable with $\mathbf{Pr}[\mathbf{x} = 0] = p$ or $\mathbf{Pr}[\mathbf{x} = 1] = p$. Show that $h(p) > h(q)$ if and only if $|p - \frac{1}{2}| < |q - \frac{1}{2}|$.

5. The key of a cryptographic system is 128 bits. Key generation is performed using a pseudorandom number generator which generates the key in blocks of eight bits. The generator is flawed, due to which each octet it produces is of even parity, i.e. the number of ones is even. How many bits of entropy the produced keys have?

6. (Stinson 2.13) Let us consider a cryptosystem where $\mathcal{P} = \{a, b, c\}$ and $\mathcal{C} = \{1, 2, 3, 4\}$, $\mathcal{K} = \{K_1, K_2, K_3\}$, and the encryption mappings e_K are defined as follows:

K	$e_K(a)$	$e_K(b)$	$e_K(c)$
K_1	1	2	3
K_2	2	3	4
K_3	3	4	1

   Given that keys are chosen equiprobably, and the plaintext probability distribution is $\mathbf{Pr}[a] = 1/2$, $\mathbf{Pr}[b] = 1/3$, $\mathbf{Pr}[c] = 1/6$, compute $H(\mathbf{P})$, $H(\mathbf{C})$, $H(\mathbf{K})$, $H(\mathbf{K}|\mathbf{C})$ and $H(\mathbf{P}|\mathbf{C})$.