T-79.503 Foundations of Cryptology
Homework 4
October 8, 2003

1. 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.

2. (Stinson 2.12) Prove that, in any cryptosystem, $H(\mathbf{P}|\mathbf{C}) \leq H(\mathbf{K}|\mathbf{C})$. (Intuitively, this result says that, given a ciphertext, the opponent's uncertainty about the key is at least as great as his uncertainty about the plaintext)

3. (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 $H(\mathbf{P}|\mathbf{C})$,

4. The cryptosystem uses a 128-bit key. The language to be encrypted is a sequence of independent four-bit blocks with either exactly one 1-bit or exactly one 0-bit in each block. Every such block has equal probability.

   a) The language is encrypted as such. Determine the unicity distance.

   b) Design some coding for this language that completely removes the redundancy.

5. (Carbage in between) Consider a cryptosystem where $|\mathcal{P}| = |\mathcal{C}|$ and keys are chosen equiprobably. This cryptosystem is used to encrypt language L, which consists of strings of plaintext characters and has entropy H_L, redundancy R_L and unicity distance n_0. The language L is modified in such a way that after each block of d characters s plaintext letters are chosen uniformly random from $\mathcal{P}$ and inserted to the plaintext. What is the entropy, redundancy and the unicity distance of the modified language?