T-79.5501 Cryptology
Homework 2
January 30, 2007

1. (HW 1/Problem 2, continued) 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

   The 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($\mathbf{P}|\mathbf{C}$).

2. Let us consider a secrecy system and the random variables related to it: plaintext $\mathbf{P}$, ciphertext $\mathbf{C}$ and key $\mathbf{K}$. As usual, $\mathbf{P}$ and $\mathbf{K}$ are assumed to be independent. Prove that 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. Let us consider a secrecy system and the random variables related to it: plaintext $\mathbf{P}$, ciphertext $\mathbf{C}$ and key $\mathbf{K}$. As usual, $\mathbf{P}$ and $\mathbf{K}$ are assumed to be independent. Prove that

   a) H($\mathbf{P}$) $\leq$ H($\mathbf{C}$).

   b) H($\mathbf{P}$) = H($\mathbf{C}$) if and only if $\mathbf{C}$ and $\mathbf{K}$ are independent.

4. 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 has even parity, i.e., the number of ones is even. How many bits of entropy the keys produced by this generator have?

5. A PIN code for Bluetooth Pairing consists of four independently and randomly selected alfanumeric characters (36 possible characters). The PIN is inserted through a key pad of a mobile device. Then each character is encoded into eight bits in the device system resulting in a 32-bit PIN code. Determine the entropy of the 32-bit PIN code. Compare it with the maximum entropy of a string of 32 bits.

6. (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 and redundancy R_L. The language L is modified in such a way that s plaintext letters are chosen uniformly random from $\mathcal{P}$ and inserted to the plaintext after each block of d characters. What is the entropy and redundancy of the modified language?