Tanner Krebs, Gerardo Lopez, William Thornton
Math 314
9/21/17

COSC/MATH - 314

Assignment 3

Problem 1 We consider the alphabet A= $\{0, 1, 2, 3, 4\}$ and the space of messages consists of all 1-symbol words, so it is M = $\{0, 1, 2, 3, 4\}$. The encryption is done using the shift cipher, so it is given by the equation X = x+k (mod 5) applied to each letter of the plaintext (as discussed in class, x is the letter that we encrypt, k is the secret key, and X is the encrypted letter).

(a.) Suppose Eve knows that the symbols 0 and 1 have the same probability Prob(M=0)=Prob(M=1) = a, and the symbols 2,3, and 4 have the same probability Prob(M=2) = Prob(M=3) = Prob(M=4) = b, and she also knows that 0 is 2 times more likely than 2, so she knows that a = 2b. Find a and b. (Hint: use the fact that the sum of all probabilities is 1).

(b.) Calculate Prob (M= 2 — C = 4) (according to Eve?s distribution). Recall that C= $E_K(M)$, that is the ciphertext is obtained by encrypting the message M (which is drawn according to Eve?s distribution which you found at point a.), and the key is equally likely to be any number in the set 0,1,2,3,4. You?ll have to use the formula for conditional probability (see the notes, and the proof of Shannon?s theorem).

(c.) (extra credit) Show that the given encryption system is perfectly secure for M, by checking the definition given in class for perfect security ? version 1 (Note: As we did in the proof of the perfect security for one-time pad, you need to consider an arbitrary distribution on M, because the definition must hold for all possible distributions).

Solution:

Problem 2 The alphabet is the same as in Problem 1, but now the space of messages consists of all 2-symbol words, so it is M_1 =(0,0),(0,1), ...(4,3),(4,4). Eve knows that the individual symbols 0,1,2,3,4 have the same probabilities as in Problem 1, and that the two symbols in a word are independent. The encryption is again the shift cipher (recall that this means that the 2-symbol word (x_1, x_2) is encrypted as the 2-symbol word $(x_1 + k, x_2 + k)$, where k is the key and addition is modulo 5.)

(a.) Calculate Prob(M=(1,4)). (Hint: This is very simple, just use that the two symbols are independent).

(b.) Calculate Prob(M=(1, 4) — C = (2, 0)). (Hint: You?ll use of course the formula for conditional probability. For the numerator, take into account that the key has to be 1 (because if we shift (1,4) by 1 we get (1+1,4+1) = (2,0)). For the denominator, you need to look at all combinations (message, key) that can produce the ciphertext (2,0). Again use as a model, the proof of Shannon?s theorem given in the notes, but adapt to this situation).

(c.) a. Using the formal definition of perfect security (the one we discussed in class, and which you can find in the posted notes), explain what the results from (a) and (b) say about whether the shift cipher is perfectly secure for this M_1.

Solution: