Homework 3 in Cryptography I

Prof. Dr. Rudolf Mathar, Paul de Kerret, Georg Boecherer

20.05.2010

Exercise 7. The text contained in the file "ciphertext.txt" has been encoded using a Vigenère cipher with an unknown key of length k. Due to the length of the ciphertext, the following questions have to be answered by implementing short programs.

a) Calculate the index of coincidence of the ciphertext. What is the value of k estimated by using the "Kasiski-Babbage" approach?

b) Calculate and compare the frequencies of the letters obtained with different choices for k. Why is it more meaningful to use $k = 5$ instead of $k = 6$ or $k = 7$?

c) Using $k = 5$, how can we obtain the key? What is then the key obtained?

d) Use the key to decode the ciphertext, and write the decoded text in a text file.

Hint: In Matlab, the functions used to read and write in a text file are "fread" and "fwrite".

Exercise 8. Let $\mathcal{M} = \{a, b\}$ be the message space, $\mathcal{K} = \{K_1, K_2, K_3\}$ be the key space and $\mathcal{C} = \{1, 2, 3, 4\}$ be the ciphertext space. Let $\hat{M}$, $\hat{K}$ be stochastically independent random variables with support $\mathcal{M}$ and $\mathcal{K}$, respectively, and with probability distribution

$$P(\hat{M} = a) = \frac{1}{4}, P(\hat{M} = b) = \frac{3}{4}, P(\hat{K} = K_1) = \frac{1}{2}, P(\hat{K} = K_2) = \frac{1}{4}, P(\hat{K} = K_3) = \frac{1}{4}.$$

The following table explains the encryption rules:

	K_1	K_2	K_3
a	1	2	3
b	2	3	4

, e.g. $e(a, K_1) = 1$.

Compute the entropies $H(\hat{M}), H(\hat{K}), H(\hat{C})$ and $H(\hat{K} \mid \hat{C})$. Does the cryptosystem have perfect secrecy? If not, propose a modified system which has perfect secrecy.

Exercise 9. Let $(\mathcal{M}, \mathcal{K}, \mathcal{C}, e, d)$ be a cryptosystem. Suppose that $P(\hat{M} = M) > 0$ for all $M \in \mathcal{M}$, $P(\hat{K} = K) > 0$ for all $K \in \mathcal{K}$ and $|\mathcal{M}| = |\mathcal{K}| = |\mathcal{C}|$. Show that if $(\mathcal{M}, \mathcal{K}, \mathcal{C}, e, d)$ has perfect secrecy, then

(i) For all $K \in \mathcal{K}, P(\hat{K} = K) = \frac{1}{|\mathcal{K}|}$ and

(ii) For all $M \in \mathcal{M}, C \in \mathcal{C}$, there is a unique $K \in \mathcal{K}$ such that $e(M, K) = C$.