Cryptology 2008
(Home work 1)

February 8, 2008

- Due on Friday, February 19, 4 p.m.
- Late submissions will not be accepted.
- Please give precise arguments for all statements that you write.
- Please do not hesitate to contact me if you do not understand the problems.
- Each problem in this homework bear 5 points.

1. Suppose we know that Karla (the sender) is encrypting using a hill cipher using a 2×2 matrix. Also we know that Karla is using a 29-letter alphabet, where A-Z have the usual numerical equivalents (i.e., A correspond to 0 and Z to 25), additionally blank=26, ?=27 and !=28. We receive the message
GFPYJP X?UYXSTLADPLW
We also know that the last five letters of the cipher correspond to KARLA the signature of the sender. Decrypt the whole ciphertext.

2. Show that the vigenere cipher is insecure in case of known plaintext attacks. How many plaintext ciphertext pairs would be necessary for complete key recovery of Vigenere cipher assuming a known plaintext attack.

3. Cryptanalyze the text in the file cipher.txt found in the website. You know that the cipher was generated from Vigenere cipher. (Credits would be given if you can partially decrypt it).

4. Let $x \xleftarrow{\$} X$ denote the event of choosing x from the set X uniformly at random. Give the values of the following probabilities:

   (a) $\Pr[x \xleftarrow{\$} \{0,1\}^4 : x = 0100]$

   (b) $\Pr[x \xleftarrow{\$} \{0,1\}^{10}, y \xleftarrow{\$} \{0,1\}^{10} : x = y]$

5. Consider a cryptosystem in which $\mathcal{P} = \{a, b, c\}$, $\mathcal{K} = \{K_1, K_2, K_3\}$ and $C = \{1, 2, 3, 4\}$. Suppose the encryption matrix is as follows:

	a	b	c
K_1	1	2	3
K_2	2	3	4
K_3	3	4	1

Given that the keys are chosen with equal probability and the plaintext distribution is

$$\Pr[a] = \frac{1}{2}, \Pr[b] = \frac{1}{3}, \Pr[c] = \frac{1}{6}.$$

Find the probability distribution on $\mathcal{C}$. Does this crypto-system provide perfect secrecy?