

Cryptography Assignment 1 is compulsory, and contributes 5% towards your final assessment. It should be submitted by 14:50 (the end of the tutorial) on Tuesday 24th March 2009. You should hand in your assignment to Barbara either at the tutorial or earlier. In the absence of exceptional circumstances (such as documented illness), assignments submitted after 14:50 but within 1 hour of that time will receive at most half marks, and assignments more than 1 hour late will not be marked. Make sure your name and student number are written on your submission!

Note that many of the questions on this assignment differ from student to student. You will be given a single sheet of paper with a large quantity of text encrypted using the Vigenere cipher. This page includes a unique number; this number identifies your assignment. **Make sure you keep a record of this number, and write it clearly at the top of the first page of your assignment.** If you lose your copy of the Vigenere ciphertext, **do not** copy another student's sheet: see the lecturer for a new copy of your unique text.

1. **(8 marks)** We define two new types of cipher.

Let $k \in \mathbb{Z}_{26}$. Given a plaintext character x , we define an *inversion* cipher by $e_k(x) = k - x$ (thus k is the key in the form of a character in the english alphabet, and we encrypt x by calculating $k - x$).

Let $k = (a, b, c)$ where $a, b, c \in \mathbb{Z}_{26}$ and $\gcd(a, 26) = 1$. Given a plaintext character x , we define a *two-step* cipher by

$$e_k(x) = a(x + c) + b.$$

- (a) Show that an inversion cipher is an affine cipher.
- (b) Show that a two-step cipher is an affine cipher.
- (c) Sometimes, people try to improve security by applying more than one encryption to their plaintext. Use mathematical induction to prove that encrypting with a sequence of any number of affine ciphers is equivalent to encrypting with a single affine cipher.
2. **(17 marks)** You have been given a page of encrypted text, which was encrypted using the Vigenere cipher. There is also some information given about repeated substrings in the text and character frequencies in the text for potential keyword lengths from 1 to 4. Undertake cryptanalysis on this text. In your submission you should:
- Estimate the keyword length in 3 ways (using Kasiski's test, and Friedman's method 1 and 2). Comment on any differences and deduce the most likely keyword length.
 - Use the method of mutual index of coincidence to determine the keyword and decrypt the text.

In your submission, explain in detail what you did, what you tried, whether it worked and what the results are. I am more interested in your discussion of the process (worth 15 marks) than I am in you necessarily getting the plaintext (worth 2 marks). I would expect several pages submitted for this question. If you crack the cipher, you need only write a few lines of the plaintext. An electronic copy of your ciphertext is available upon request.

Please turn over.

3. (6 marks) Attached to this document is a collection of keys for the Hill cipher, in which each line commences with a unique number. For this question, you should only refer to the line with the same number as that at the top of your ciphertext for Question 2. Each line contains values for a , b , c and d , and some ciphertext.
- (a) Let your 2×2 matrix K for the Hill cipher be $K = \begin{bmatrix} a & b \\ c & d \end{bmatrix}$,
where the values of a , b , c and d are given on your line of the attached list of keys. Encrypt the plaintext *pigs* using K .
- (b) Using the same key K , find the plaintext which corresponds to the ciphertext given on your line of the attached list of keys.
4. (4 marks) Attached to this document is a collection of keys for the Autokey cipher, in which each line commences with a unique number. For this question, you should only refer to the line with the same number as that at the top of your ciphertext for Question 2. Each line contains values for the key, *plaintext1* and *ciphertext2*.
- (a) Use your key (from the list) to encrypt your *plaintext1* (from the list).
- (b) Assume that your *ciphertext2* (from the list) was encrypted using your key. Find the corresponding plaintext.

Make sure you write your unique number at the top of your assignment.