Practical 1

This practical is worth 45% of the continuous assessment portion of this module and is due 21:00 on Thursday October 6th. Submit a report in PDF with answers to the questions, and where applicable include any programs.

Code breaking

Q1 (30%) Break the monoalphabetic substitution cipher in `ciphertext.txt` in this directory, that is, give a plausible plaintext for this ciphertext. The plaintext is English, in which all punctuation was removed and all upper-case letters were converted to lower-case. The only non-printing character is the space character.

You are free to do the cryptanalysis fully by hand, but you may benefit from writing a little code, in particular to do statistical analysis on the frequencies of letters. You may need to collect an arbitrary sample of English text, and perform the same conversion as was done on the plaintext (remove punctuation and convert upper-case to lower-case).

There are many advanced approaches in the literature to do cryptanalysis of monoalphabetic substitution ciphers, but do not get carried away, and do not waste time on extraneous concerns such as fancy user interfaces. Do not panic if you do not manage to decipher the text in the end. Credit is not given for finding the plaintext per se, but for evidence of a sound approach to trying to solve the problem, demonstrating awareness of the redundancy that exists in natural language text. Explain what worked and what didn't. Include any code that you wrote.

Mini ChaCha20

Consider a miniature version of the ChaCha20 cipher, in which the state consists of just 64 bits, written as a 4×4 block of 4-bit values, instead of a 4×4 block of 32-bit values.

Note that a rotation by 16, 12, or 8 positions now leaves the bitstring unchanged. A left rotation by 7 positions is the same as a right rotation by 1 position.

Q2 (15%) Perform one double round of this cipher starting with state (given here in hexadecimal):

F	E	D	C
B	A	9	8
7	6	5	4
3	2	1	0

It is well possible to do this purely by pen and paper, but it may be easier to write a few lines of code to do this. (As before, do not waste time on extraneous concerns such as fancy user interfaces.) Show a few intermediate results, including at least:

- Show in detail the four basic steps in the quarter round applied on the first column.
- Indicate the diagonals involved in the diagonal round, giving the values in each diagonal before and after the round.
- Give the complete state at the end of the double round.

Extended Euclidean algorithm

The numbers 89 and 55 are coprime, i.e. their greatest common divisor is 1, which implies $s \cdot 89 + t \cdot 55 = 1$, for some integers s and t.

Q3 (10%) Find s and t using the extended Euclidean algorithm. Show all intermediate steps.

Modular arithmetic

Q4 (15%) Write out the multiplication table for integers modulo 10. Which numbers have multiplicative inverses modulo 10? Justify your answer.

In general, for the integers modulo N, y has a multiplicative inverse if and only if y and N are coprime. Explain why this is.

Hint: you should be able to solve this exercise with the mathematics already discussed in this module, and very basic facts about integer division. You are generally free and encouraged to do additional reading, but it won't necessarily make solving the present exercise any easier. If you rely on theorems from maths textbooks, you would still need to explain why those theorems hold.

Finite fields

Q5 (30%) Write out the addition and multiplication tables of $\mathbb{F}_{3^2}$, formed by polynomials of degree strictly less than 2, with coefficients that are integers mod 3, with irreducible polynomial x^2+1. For a couple of entries in the multiplication table, show your working, to demonstrate that you know how to do multiplication and long division for polynomials.

Next, write out the multiplication table of $\mathbb{F}_{3^2}$ as above, but now with irreducible polynomial x^2+x+2. Show that the two choices of the irreducible polynomial result in the same field, the difference being merely the naming of the elements. In other words, if you consistently substitute polynomials by other polynomials in the two tables that you constructed with x^2+1, then you will get the tables that you constructed with x^2+x+2, apart from the order of rows and columns. Describe the consistent substitution(s) in one sentence. Justify your answer.

Hint: the only mathematics that you need for this exercise was discussed in the lectures. You are generally free and encouraged to do additional reading, but it won't necessarily make solving the present exercise any easier. What may help is to look for common patterns in the two multiplication tables.

Rubric

There are 5 questions/assignments in this practical. The percentages approximately indicate the proportion of time you could be expected to spend on each of the parts. Your submission will be marked as a whole however,

and an exceptional achievement in one or more of the five parts could make up for small mistakes in other parts. Marking is according to the standard mark descriptors published in the Student Handbook at:

> `https://info.cs.st-andrews.ac.uk/student-handbook/learning-teaching/feedback.html#General_Mark_Descriptors`

You should submit your work on MMS by the deadline. The standard lateness penalties apply to coursework submitted late, as indicated at:

> `https://info.cs.st-andrews.ac.uk/student-handbook/learning-teaching/assessment.html#lateness-penalties`

I would remind you to ensure you are following the relevant guidelines on good academic practice as outlined at:

> `http://www.st-andrews.ac.uk/students/rules/academicpractice`