The University of Newcastle
School of Electrical Engineering and Computer Science

COMP3260/6360 Data Security

Assignment 1

This assignment is to be done in pairs

*Due on **Friday, 2nd April 2021, 11:59pm**, electronically via the 'Assignment1' link in Blackboard.*

Total 100 marks

Your task is to decrypt four ciphertext files called *c1*, *c2*, *c3 and c4* without the knowledge of the keys (i.e., to "break" these ciphers). Each cipher is one of the following types: transposition, monoalphabetic substitution or polyalphabetic substitution.

For each ciphertext provide a detailed description of the steps you go through, what assumptions you make and why (e.g., IC indicates period of around 3, single-letter frequency distribution indicates transposition cipher, etc.).

For each ciphertext, *most marks* will be given for the detailed description of the performed cryptanalysis. That means that may be given a high mark even if the cipher has not been broken. Conversely, if you break the cipher but don't provide a detailed description of your steps, you may score a low mark. Please refer to the marking scheme for details.

You will need to use a program to help you break the ciphers, that is, to perform statistical analysis of the ciphertext, as well as to decrypt the ciphertext with a chosen cipher and key. You can only use JKrypto, whose current version was written by Lawrie Brown and based on the original code by Daryl Bossert, both at ADFA, Canberra Australia. This program has been used to encrypt all 4 assignment files.

jkrypto is available for download as a Java .jar file from http://lpb.canb.auug.org.au/adfa/src/jkrypto/index.html
This program provides an option of either GUI or command line control.