The University of Newcastle
School of Electrical Engineering and Computer Science

COMP3260/6360 Data Security

Assignment 1

*Due on **Wednesday, 18th April 2018, 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" the ciphers). Each cipher is one of the following types: transposition, monoalphabetic substitution or polyalphabetic substitution.

For each ciphertext describe the steps you went through, what assumptions you made and why (e.g., IC indicates period of around 3, single- letter frequency distribution indicates transposition cipher, etc.).

For each cipher, *7 marks* will be given if the cipher is broken (and both the key and the plaintext provided) and *18 marks* will be given for the detailed description of the performed cryptanalysis. That means that up to 18 marks per cipher may be given 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 as low as *7 marks* per cipher.

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 may write your own program or you may use somebody else's program, as long as you properly acknowledge the program source.

We recommend that you 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/a8fa/src/jkrypto/index.html. This program provides the option of either GUI or command line control.