MATH 3024 Assignment 01

After completing `MATH3024` *you have been hired by a government agency in Canberra, which believes that members of the American Literature Department at Melbourne University are using enciphered messages to hide terrorist activities against the Australian government. Due to educational cutbacks, they were only able to hire a student who completed the first two weeks of* `MATH3024` *at Sydney Uni, and who is unaware of the weaknesses of classical ciphers. Your supervisor presents you with the following problems before promoting you to more challenging tasks within the agency.*

1. (2 pts) [Vigènere cipher] You suspect that the first ciphertext uses a Vigenère cipher. Find the deciphering key and plaintext.

2. (2 pts) [Substitution cipher] The second ciphertext has a standard coincidence index for English, and you suspect a simple substitution cipher. Find the deciphering key and plaintext.

3. (2 pts) [Product cipher] After recognizing the weaknesses of previous ciphers, the cryptosystem suddenly changes, and your supervisor believes that the Melbourne University Junta is now using product cipher, composing substitution and transposition ciphers. Find the substitution key, the transposition key, and the plaintext message.

4. (2 pts) [N-time pad cipher] The American Literature group suddenly gets wise to the insecurity of classical cryptosystems, and tries to implement the use of one-time pads. However they make the implementation mistake of reusing the key for multiple ciphertexts, of which you intercept three. Find the key and plaintext messages.

5. (2 pts) [Information theory] Your supervisor presents you with a model cryptosystem, giving the probabilities of each the plaintexts and a specification of the enciphering algorithm. Find the entropy of the plaintext, keyspace, and ciphertext languages, and the conditional entropy of the cryptosystem.

Individual data for this assignment can be accessed from the course home page. Answers to the assignment should be submitted by Tuesday 27 April 2004, following the directions on the course home page.