COSC312: Assignment 1

Due: 21/8/2023

Instructions

- All work is to be submitted by email to michael.albert@otago.ac.nz by midnight on the due date.
- PDF format for text documents is preferred.
- Note that this assignment has two pages—there are a total of ten marks available.

Problems

1. The inhabitants of *Cryptologia* use a ten character alphabet where the characters are the digits 0, 1, 2, . . . , 9. This makes implementing Vigenère ciphers rather simple—you just take a sequence of digits, repeat it as often as necessary and add it to the text, discarding any carries. The only statistical non-uniformities that have been observed in (unencrypted) Cryptologian texts are that successive letters are never the same. That is, the pairs 00, 11, 22, . . . , 88, and 99 never occur as consecutive letters. In fact, any sequence of digits that does not contain a repeated pair like this is a valid Cryptologian text.

   (a) How would you propose determining the likely key length for a Vigenère cipher based on Cryptologian from a ciphertext? [2 points]

   (b) If you know the key length, can you ever be certain about what the key is? Why, or why not? [1 point]

   (c) You will receive by email a message encoded from Cryptologian using a Vigenère cipher. Try to determine the key length and as much information as possible about the key. Explain your methods and submit any program you used. [3 points]

2. Neither of the following pseudo-random generators are secure (for fairly trivial reasons). In each case, demonstrate this fact by giving an efficient statistical test with a significant advantage over the generator.

   (a) $G : \{0, 1\}^{24} \to \{0, 1\}^{48}$ where $G(k)$ is just two copies of k concatenated together. [1 point]

   (b) $G : \{0, 1\}^{63} \to \{0, 1\}^{70}$ where $G(k)$ is k concatenated with the seven-bit binary representation (including leading zeros) of the number of 1's in k. [1 point]

3. Suppose that $G : \{0,1\}^s \to \{0,1\}^n$ *is* a secure pseudo-random generator. Which, if any, of the following modifications of G is also secure? Explain your answer in each case. A sentence or two will suffice.

   (a) $H(k)$ which is defined from $G(k)$ by taking the exclusive-or of $G(k)$ and the sequence 010101... of alternating 0's and 1's. [1 point]

   (b) $H(k)$ which is defined from $G(k)$ by appending the exclusive-or of the bits in $G(k)$ (that is, $H(k) = G(k)0$ if the number of 1-bits in $G(k)$ is even, and $H(k) = G(k)1$ if the number of 1-bits in $G(k)$ is odd). [1 point]