COSC412: Assignment 1

Due: 21/8/2020

Instructions

- All work is to be submitted by email to michael.albert@otago.ac.nz.
- PDF format for documents is preferred—work can be done by hand and scanned into digital form.
- There are 12 points indicated—the maximum possible score is 10. You are free to choose your strategy. That could include submitting perfect work for the whole assignment, getting a feeling of quiet satisfaction from having done so, achieving insurance against having made a silly error, and obtaining a score of 10.

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 a consecutive increasing pair (including a 'wrap-around' of 90). That is, the pairs 01, 12, 23, ..., 89, and 90 never occur as consecutive letters.

   (a) How would you propose determining the likely key length for a Cryptologian Vigenère cipher 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 by a Cryptologian 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) $G : \{0,1\}^{64} \to \{0,1\}^{70}$ where $G(k)$ is the concatenation of k and the six bit representation of the number of blocks (maximal runs of equal digits) in k. [1 point]

   (b) $G : \{0,1\}^{64} \to \{0,1\}^{128}$ where $G(k)$ is the concatenation of k with its negation. [1 point]

3. Suppose that $G : \{0,1\}^s \to \{0,1\}^n$ *is* a secure pseudo-random generator (assuming that such a thing exists). Which of the following are also secure? Give arguments for or against, not just answers.

   (a) $H(k)$, the string of $n-1$ bits, obtained from $G(k)$ by deleting its first character. [1 point]

   (b) $H(k)$ defined as $G(k)c$, the string of $n+1$ bits where c is the exclusive or of the bits of $G(k)$. [1 point]

4. Consider the two primes:

$$p = 220836086241007,$$
$$q = 436460983609873.$$

   Let $N = (p-1)(q-1)$ and consider the basic form of RSA encoding modulo pq with public encoding key

$$e = 425641.$$

   (a) Compute the private decoding key d i.e., find d so that $de = 1 \mod N$. [1 point]

   (b) The encoding of a "message", m i.e., the value of m^e modulo pq where m is a positive integer less than pq, is

$$45250314786351235469212809932.$$

   What was m? [1 point]

   The `sympy` module in Python may be of use here (other suitable software products are also available).