MTH6115 Cryptography Exercises 4

Hand in to BLUE BOX on SECOND FLOOR of math sci building before 4:30pm on Friday 27/2/09.
Remember: *The work you hand in should be your OWN work. If you work in groups make sure you YOURSELF understand the answers that have been obtained, and write up your answers YOURSELF. I take a dim view of copied answers, and will penalise them severely when I detect them.*

Q1 Let p be a plaintext message using symbols from an alphabet A. Describe how a substitution cipher for encrypting p can be viewed as a stream cipher by defining a suitable keyword and substitution table. [10]

Q2 (a) Alice encrypts a plaintext message over the alphabet $\{0, 1, 2, 3\}$ by using a stream cipher with keyword k and the following substitution table S_1.

	0	1	2	3
0	1	2	0	3
1	2	1	3	0
2	0	3	1	1
3	3	0	2	2

Construct a substitution table S_2 which Bob can use, with the the same keyword k, to decrypt the ciphertext. [20]
(b) (i) Explain in general how you would construct a decryption substitution table S_2 from an encryption substitution table S_1 over an arbitrary alphabet A.
(ii) What properties would the encryption substitution table S_1 need to ensure that it is the same as the decryption substitution table S_2? [20]
(c) Give an example of a 3×3 Latin square L with entries from $\{0, 1, 2\}$ which can be used for both encrypting and decrypting the same stream cipher. [10]

Q3 Let C_1, C_2 be two stream ciphers over the same alphabet A with respective keywords k_1, k_2 and substitution tables S_1, S_2. Let C be the combined cipher obtained by first encrypting the plaintext using C_1, then encrypting the resulting ciphertext with C_2.
(a) Prove that if $A = \{a, b, c, \ldots, z\}$ and S_1, S_2 are both equal to the Vigenère square then C is a Vigenère cipher. Explain how to construct a keyword for C. [10]
(b) Prove that if $k_1 = k = k_2$ then C is a stream cipher with keyword k. Explain how to construct a substitution table for C. [10]
(c) Prove that if $A = \{0, 1, 2\}$, $k_1 = 0001\ldots$, $k_2 = 0120\ldots$, and S_1, S_2 are both equal to the table below

	0	1	2
0	0	1	1
1	2	0	2
2	1	2	0

then C is not a stream cipher. [20]