CM30173: Example sheet 2

30th January

Questions 1-3 relate to lecture 2. Question 4 relates to lecture 3.

1. Show that the Vernam cipher is vulnerable to a known-plaintext attack.

2. Alice and Bob don't have a shared key but want to communicate in secret. They try to accomplish this using the one-time pad. Alice uses a keystream $k \in (\mathbb{Z}_2)^n$, Bob uses a keystream $l \in (\mathbb{Z}_2)^n$. Alice encrypts the plaintext $x = x_1 x_2 \dots x_n$ with k and sends this to Bob. Bob encrypts the ciphertext with l and sends this back to Alice. Alice then decrypts with her keystream k and sends the result to Bob who decrypts with l and hence has the plaintext. Explain why an attacker is able to recover both keystreams and the plaintext.

3. Assume that (despite advice against it!) Alice and Bob reuse a keystream k in the one-time pad. Oscar has collected two ciphertexts $y = y_1 y_2 \dots y_n$ and $y' = y'_1 y'_2 \dots y'_n$ encrypted with the same key. What information might Oscar be able to glean from these? What might make his job easier or harder?

4. There are two possible decryption algorithms for the SPN given in lectures. We could reverse the order of operations and the key schedule, using the inverse substitution and permutation operations. Why might we wish to avoid this?

   Since we do not apply a permutation in the last round it is also possible to use the encryption algorithm for decryption if we replace the S-box by its inverse and make changes to the key schedule.

   (a) Calculate the inverse of the S-box

   (b) Find the changes to the key schedule

   (c) Check your algorithm by decrypting the ciphertext produced in class

   For this exercise and for future use, you should produce an implementation of this SPN (encryption and decryption) in the programming language of your choice, or using a system such as Maple. You should be able to change the S-box used but you need not generalise it further.