TELE 3119: Trusted Networks
Session 2, 2016: Quiz 1

Question 1. [5 points]

Increasing the key length is one way to increase security of an encryption algorithm against the brute-force type of attack. DES uses 56-bit key, which is not secure, given the modern computing power. Assume that 56-bit key was just sufficient in 1979 when DES was standardized, and assume that the hardware performance improves about 40% per year, then how many bits of a DES key would just suffice next year (i.e. 2017)? Until what year would a 112-bit DES key be sufficient?

[**Hint:** How much approximately does the hardware performance improve in two years?]

Question 2. [15 points]

Alice and Bob have agreed on the following protocol for sending a message securely from Alice to Bob. The protocol is based on the ideas of the one-time pad, but without a common, shared secret. Instead, for each message, both Alice and Bob choose a random number and execute the following protocol to send message M from Alice to Bob:

(i) Alice ➔ Bob : $M_1 = M \oplus R_A$
(ii) Bob ➔ Alice : $M_2 = M1 \oplus R_B$
(iii) Alice ➔ Bob : $M_3 = M_2 \oplus R_A$

Here, in 3 rounds only the messages M_1, M_2 and M_3 in the right hand side are sent. Assume that an eavesdropper (i.e. Eve), is passively observing the above communication between Alice and Bob. Note that Eve does not actively interfere in any stages above (i.e. she does not change or generate any messages).

a) [5 points] Show that Bob can recover the message M after three rounds of exchange.

b) [10 points] Is this scheme secure? Why or why not?