

Date: Wednesday, April 3, 2002
Lecturer: Dr Jean-Yves Chouinard
Office: Colonel-By Hall, room A-610

ELG-5373 Secure Communications and Data Encryption

Assignment #3 (due on Monday, April 15, 2002 at the beginning of the lecture.)

Question 1:

(RSA public key encryption)

Problem 4.5 from the course notes.

Question 2:

(Diffie-Hellman key exchange protocole)

Problem 4.12 from the course notes.

Question 3:

(Factorization and primality)

a) Use trial division to factor or demonstrate the primality for:

- i) $n_1 = 307, 821$
- ii) $n_2 = 16, 803, 654$
- iii) $n_3 = 194, 685, 276, 691$

b) Use the Pollard-Rho algorithm to factor:

- i) $n_4 = 785, 994, 771, 137$
 - ii) $n_5 = 2, 506, 741, 191, 739$
 - iii) $n_6 = 265, 870, 264, 098, 379$
-

Question 4:

(Chinese remainder theorem)

Problem 7.2 from the course notes.
