

Problem Set 6
Due 12/10/2005

Send to tmorgan@ccs.neu.edu, with CC to noubir@ccs.neu.edu

Problem 1 (20 points):

Textbook 5.7, page 219.

Problem 2 (10 points):

Textbook 5.8, page 219.

Problem 3 (20 points):

Textbook 5.10, page 219.

Problem 4 (10 points):

Textbook 5.12, page 220.

Problem 5 (10 points):

Textbook 5.14, page 221.

Problem 6 (10 points):

Textbook 6.9, page 269. Decrypt only the first pair (3781, 14409).

Note: there is a typo, exercise 6.9 refers to exercise 5.12 instead of 5.6.

Problem 7 (20 points):

Textbook 5.13, page 220.

Note: there is a typo, in line 3 of this exercise, replace " y^a " by " y^d ". In parts (b) and (c), a value of d needs to be specified. You should use the value $d = 1234577$.