CO 485/685 Public-Key Cryptography

Instructor: Alfred Menezes

Prerequisties:

Background in PMATH 334 and PMTH 336 from the University of Waterloo

I would recommend reading the following from "A Course in Number Theory and Cryptography" by Neal Koblitz
(second edition, Springer, 1994).

* Chapter 1
* Chapter 2
* Section 3.1
* Sections 4.1, 4.2, 4.3
* Sections 6.1, 6.2