Pedro Avila
CSc 492
Senior Project Outline
Advisor Dr. T.J. Kearns
2004.04.10

<u>Subject</u>: Design and implement an RSA cryptosystem to learn about the underlying mathematics of the RSA algorithm.

<u>Object</u>: To encrypt and decrypt plaintext files using the RSA algorithm. Designing and implementing java programs efficiently and effectively will give me a first-hand look at the problems faced by implementers of an algorithm whose power and beauty lies in its terrifying simplicity.

<u>Equipment</u>:	- PC running Windows XP.	na

<u>Materials</u>:	- <u>The Code Book</u>	$14
	- <u>Números Inteiros e Criptografia RSA</u>	Borrowed
	- Various web sites	

<u>Outline of Procedures</u>:

Tasks to be completed before 2004.06.01:

1.	Read, understand and take notes on selected material.	50 hours
2.	Design system properties (equations to be used).	25 hours
3.	Design flow of information.	02 hours
4.	Design system interface.	03 hours
5.	Design system tests.	10 hours
6.	Code all necessary modules.	10 hours
7.	Debug coded material.	05 hours
8.	Quality and functionally test modules	02 hours
9.	Design Digital Signature option (time permitting)	03 hours
10.	Code Digital Signature option (time permitting)	02 hours
11.	Debug recoded material	02 hours
12.	Quality and functionally test modules	02 hours
13.	Check Documentation of Code.	02 hours
14.	Final Report outlining what was learned and functionality achieved.	20 hours
15.	Design and implement project web site	05 hours

Total Time   ~150 hours

Student: _____   Date: _____

Advisor: _____   Date: _____