CS435/535 Algorithms
Spring 2016
Project #1 Evaluation Sheet

Name _____

Date and time received _____(Ö -- on time)

Late penalty (10% per day) _____

Score _____/_____

Program Correctness _____/14___

Part I (6pts):

1. Fermat's test is implemented____;
2. Probable prime numbers p and q are generated (each > 10^{40}) and saved in the file (p_q.txt)____;
3. e is co-prime of (p-1)(q-1), the public key-set file (e_n.txt) generated ____;
4. d is the mod inverse of e, the private key-set file (d_n.txt) generated ____;
5. e*d = (p-1)(q-1) ____;
6. n=p*q ____;

Part II (8pts):

1. test case 1 (bible_part1.txt)
   a. signed correctly____;
   b. verified correctly____; (with modified file)
2. test case 2 (bible_part1.docx)
   a. signed correctly____;
   b. verified correctly____; (with modified file)
3. test case 3 (monkey.jpg)
   a. signed correctly____;
   b. verified correctly____; (with modified file)
4. test case 3 (rsa435.exe)
   a. signed correctly____;
   b. verified correctly____; (with modified file)

Programming Practices (3)____/3

General code appearance___

Proper header___

Good general description of program___

Undergraduate student

Readme.txt (1)_____

Graduate student

Readme and report (4)_____/4

Readme.txt (1)_____

Report (3)___