Homework Assignment Due October 21, 2021:

1. Imagine that Fred sees your RSA signature on m_1 and m_2, (i.e., he sees (m_1^d mod n) and (m_2^d mod n)).
How does he compute the signature on each of m_1^j mod n (for positive integer j), m_1^{-1} mod n, $m_1 \times m_2$ mod n, and in general $m_1^j m_2^k$ mod n (for arbitrary j and k)?

2. Choose one of your favorite operating systems (e.g. Windows 98/2000/XP or UNIX) and compare its security policy with the Clark-Wilson model. Does its security mechanism satisfy Clark-Wilson axioms? You may take a look at http://www.giac.org/practical/gsec/Sonya_Blake_GSEC.pdf, though I am sure you will have your own opinion.

How to Submit Your Assignment:

Please send your completed assignment to talia.q@ufv.ca :
The Subject Field must read: CIS221 Assignment 1. Please copy and paste this into the Subject Field of you submission. Failure to do this exactly will result in a grade of zero for the assignment with no exceptions.