Homework #3

Due: February 19, 2021 **Points:** 100

Questions

1. (*25 points*) Devise an algorithm that generates an access control matrix *A* for any given history matrix *H* of the Chinese Wall model.
2. (*15 points*) A publisher wishes to implement a DRM scheme for its digital books. Please explain why enciphering the contents of the books, and then distributing the appropriate cryptographic keys, is insufficient to provide a digital rights management scheme.
3. (*10 points*) With the exception of the break-the-glass policy model, the hybrid modes we have studied do not discuss availability. What unstated assumptions about that service are they making?
4. (*25 points*) The system *plugh* has users Skyler, Matt, and David. Skyler cannot access David's files, and neither Skyler nor David can access Matt's files. The system *xyzzy* has users Holly, Sage, and Heidi. Sage cannot access either Holly's or Heidi's files. The composition policy says that Matt and Holly can access one another's files, and Skyler can access Sage?s files. Apply the Principles of Autonomy and Security to determine who can read whose files in the composition of *xyzzy* and *plugh*.
5. (*25 points*) Modify the two-bit system in the first example in Section 9.3 as follows. Whenever a HIGH operation is performed, the HIGH state bit is output. Whenever a LOW operation is performed, the LOW state bit is output. The initial state is not output (in contrast to the example). Is this version of the two-bit system noninterference secure with respect to Lucy? Why or why not?