CSI4108 / SEC5101
(Fundamentals of) Cryptography

Assignment #4
Due: Friday, December 2, 2022 (before 16:00, to be submitted via Brightspace)

All questions in this assignment are to be done individually (i.e., not working with anyone else).

1. **[2.5 marks]** Implement HMAC-SHA-512. You may use any library or toolkit to call SHA-512, but implement the rest of HMAC yourself. Compute the HMAC of the following string: "I am using this input string to test my own implementation of HMAC-SHA-512." Use any library or toolkit to call HMAC-SHA-512 on this string to confirm that your implementation is correct.

2. **[2.5 marks]** Implement DSA. Using a 1024-bit prime p and an appropriate 160-bit prime q with generator g of the q-order subgroup of Z_p^*, choose a signature key pair (x, y), an appropriate value k, and the hash function SHA-1. You may use any library or toolkit to find p and q and to call SHA-1, but implement the rest of DSA yourself. Sign the message m = 522346828557612 using the privacy key x. Verify the signature using the public key y.

3. **[1.5 marks]** With your implementation from question #2, sign the message m = 8161474912883 using the same value of k. Show that an observer of the two signatures will be able to completely compromise security.

4. **[1 mark]** It is possible to use a hash function to construct a block cipher with a structure similar to DES. Since a hash function is one-way and a block cipher must be reversible (in order to decrypt), how is it possible? Explain in your own words.