CSE 667, Assignment 3

Due: Friday, November 13, 2020, by 11:59 pm.

Note 1: The total mark for this assignment is 30.

Note 2: You should *NOT* directly copy anything from slides or other resources. You may get the ideas from slides but what you submit *must be in your own words*. Any help must be acknowledged.

1. Describe the Decrypting RSA using Obsolete and Weakened eNcryption (DROWN) attack. (6 points)

2. In order to reduce the decryption time of the RSA with a 4096-bits modulus for implementation in resource-constrained devices like IoT devices, smart cards, RFID tags, etc, it has been suggested to use a 1000-bit private exponent. Is the resulting scheme secure? Prove your claim. (6 points)

3. Describe Bleichenbacher's attack on RSA-PKCS1 v1.5 which applies to the SSL 3.0 protocol. (6 points)

4. Describe OAEP, OAEP+, and SAEP+. (6 points)

5. a) How the implementation of TLS 1.0 made it secure against Bleichenbacher's attack? Explain in detail. (3 points)

   b) How the decryption in OAEP does work? (3 points)