Homework 4

(Return your solution to the class on May 23 Wednesday)

HW will be completed by each student **individually (no collaboration).** Directly borrowing (e.g., copy-paste) from any material and putting in solutions (e.g, from online solutions, Wikipedia, or research papers) is **plagiarism** (see Syllabus for its corresponding actions). Please cite very carefully each resource you use, but citing a solution does not give a license to directly put it as an answer. **All of your answers must be in your in own words and interpretations.** HW should be prepared by a text editor (e.g., Microsoft Word or Latex). Handwritten submissions are **not** accepted.

Each question is 10 pt. Answers for attack questions could be around 2-3 paragraph explanations, preferably supported with figures, if possible. Please give citations for your resources.

1. What is “The Heartbleed Bug”, describe in detail how it works against SSL, and how it can be prevented?

2. What is POODLE attack, describe how it works and how it can be prevented?

3. Is it possible to attack TLS and DTLS Record Protocols based on timing measurements (i.e., delicate timing analysis of decryption processing)? Find out at least one research paper (hint around 2013) that achieves this attack, and describe how the attack works and it could be prevented?

4. What is “Venom Vulnerability” targeting Virtual Machines?

5. What are “Spectre and Meldown” vulnerabilities?

**Extra Credit:**

6) [20 pt] We have covered ETA scheme in the class.
   - [5 pt] What is the main design contribution of ETA, compared to its base scheme Schnorr?
   - [5 pt] How did the signer ensure O(1) private key storage?
   - [5 pt] Which properties of Schnorr signature permitted ephemeral public keys to be stored at the verifier side?
• [5 pt] We have covered a Message Recover version of ETA (MRETA) in the class (over the board). How does MRETA eliminate $x_j$ component from the signature?

7) [15 pt] We have covered HAA scheme in the class.
• [5 pt] What is the main observation that permit the design of HAA scheme?
• [5 pt] How does multiplicative homomorphism play a role in HAA design?
• [5 pt] Why is HAA an offline-online signature variant?