CS 5594
Homework Assignment 1

Given: Feb 09, 2024 **Due:** Feb 22, 2024

General directions. The point value of each problem is shown in [ ]. Each solution must include all details and an explanation of why the given solution is correct. **In particular, write complete sentences. A correct answer without an explanation is worth no credit.** The completed assignment must be submitted on Canvas as a PDF by 11:59 PM on Feb 22, 2024. **No late homework will be accepted.**

Digital preparation of your solutions is mandatory. Use of LaTeX is optional, but encouraged. No matter how you prepare your homework, **please include your name.**

---

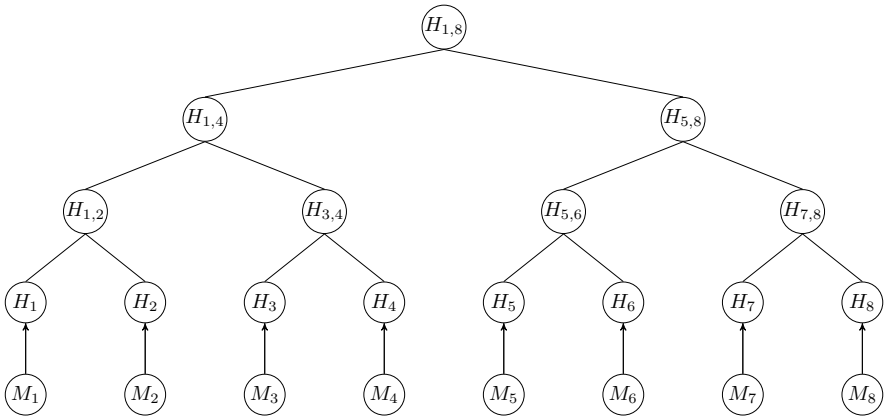
[20] 1. Consider the three attributes including Consistency, Availability, and Partition Tolerance in a distributed system:

A. Prove that a distributed system cannot achieve these three attributes simultaneously.

B. Show how public blockchain manages to achieve these attributes. Specifically, which attribute is scarified in favor of the other two attributes? Describe the core technique that the public blockchain used to fully achieve those two attributes, while managing to (eventually) offer the remaining one.

---

[50] 2. Suppose a sender S uses the following Merkle-hash tree T to authenticate messages $(M_1, \ldots, M_8)$ to a receiver R.



A. How would one authenticate message M_4? What elements of T must be transmitted from S to R, and write the correct verification equation.

B. Why the Merkle-hash tree T has an additional level of hash in the leaves?

C. What are two necessary conditions for a set of data to be authenticated by the Merkle-hash tree?

D. Show how to find a collision in a Merkle-hash tree T' with a *flexible* structure (i.e., the number of the inputs is not fixed). Specifically show how to find two sets of messages $\mathcal{A} = \{A_1, \ldots, A_t\}$ and $\mathcal{B} = \{B_1, \ldots, B_{2t}\}$ such that $\mathsf{MerkleRoot}(\mathcal{A}) = \mathsf{MerkleRoot}(\mathcal{B})$.

E. Describe how Merkle-hash trees are used to achieve integrity in public blockchain (e.g., bitcoin).

---

[30] 3. In class, we have covered a Digital Signature Algorithm (DSA), in which the signature (r, s) for the message m can be computed as

$$\begin{cases} r = (g^k \mod p) \mod q \\ s = k^{-1}(H(m) + x \cdot r) \mod q \end{cases}$$

where k is a random private key per signing, x is long-term private key and H is a cryptographic hash function.

A. Consider a variant of DSA algorithm, in which the second component of the signature generation is computed as

$$s = k^{-1}(m + x \cdot r) \mod q$$

Show that this variant is not secure, in which the attacker can forge valid signature for any arbitrary message of it choice without querying any signatures from the signer.

B. Sony PS3 was hacked by the hacker group "fail0Overflow" via a key recovery attack on the ECDSA digital signatures computed in Sony PS3 platform. Explain what caused the attack and show the steps of the attack in details.

---

[25] 4. Consider the following ECC curve E:

$$Y^2 = X^3 + 231X + 473, p = 17389, q = 1321, G = (11259, 11278) \in E(\mathbb{F}_p).$$

A. Assume the signing key of Alice is $sk = 542$. What is her corresponding public key pk? What is her signature on the hash of a message $H(m) = 644$ with the ephemeral key $k = 847$?

B. Assume the public key of Bob is $pk = (14594, 308)$. What is his private key sk? (you can use any method to find it, but describe it in details). Use his private key sk that you found to forge his signature on the hash of a message $H(m) = 516$ using the ephemeral key $k = 365$.
