CS 419 / ECE 478: Introduction to Network Security (Spring 2016)

Instructor: Dr. Attila A Yavuz

Homework 2
(Assigned 4/28/16, Due 5/10/16 in class)

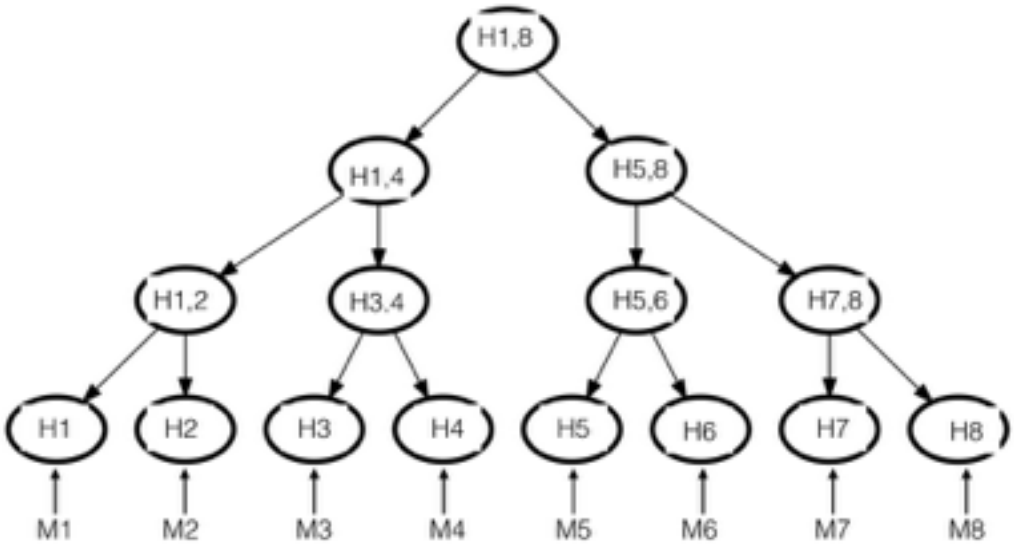
Requirements: HW will be completed by each student **individually (no collaboration)**.

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 LaTeX or Word. Handwritten submissions **are *not* accepted.**

---

1) **[24] Merkle Hash Tree**



Suppose a sender S uses this Merkle hash tree to authenticate these messages to a receiver R. What should be done before this tree can be used?

[8] How would one authenticate message 4?

[8] Merkle hash trees have an additional level of hash in the leaves. Is this necessary? Why?

[8] What are the necessary conditions for a set of data to be authenticated by Merkle-tree? Please provide at least two example application where Merkle-tree with proper data type can be used.

2) [24] Cryptographic hash functions and their use in one-time/multiple time signatures

[12] Let L be the number of messages, t is the number of bits to be signed in a message, and |f| is the bit-length of one-way function. Describe Lamport One time signature variant I, II, III, IV, VI, and VII (excluding V) . For each variant, describe the its algorithm, its performance in terms of security and efficiency, and what are the key sizes and what is its storage complexity. For example, for one variant, you might want to mention what is the computational complexity for the efficiency of the algorithm and what is the security trade-off you must pay in order to achieve that efficiency. You must also mention what is the storage complexity of the public and private key in Big O.

[12] One-time/multiple signatures, after many years, started gain a new traction in the research community. What is the main reason behind this? Compared traditional cryptographic methods (e.g., RSA, ECDSA), what is the main security advantage of multiple-time signatures and why they are more secure?

3) [48] RSA encryption and digital signatures

[8] What is the role of Euler-Function, Extended Euclid Algorithm and Fermat Little Theorem in RSA encryption? Explain the role of each by showing the specific step in RSA encryption and decryption process.

[8] Using Euclid's algorithm (Not extended, but just Euclid), calculate the g gcd(16261, 85652). Using Fermat's little theorem, compute 3^31 (mod 7) (Hint: Decompose the exponent)

[8] In RSA, public key *e* can be smaller than the private key *d*. What are the performance and security implications of this? What should be considered for selecting public exponent e as a security metric?

[8] In RSA encryption and signatures, the use of private/public key pair between sender and verifier is swapped. Why this is the case? (Hint: Think about the purpose of signatures and encryption. Also, think about the purpose of authentication and its difference from encryption)

[8] In RSA signatures, randomness was introduced during the signing process using Coron's Full Domain Hash Function. What is the objective of this randomness? Please again use Google Scholar to look up JS Coron's paper on full domain hash function. You may want to look Bellare's paper on full domain hash function. Please note that full domain hash function **IS NOT** an RSA-based signature scheme.

[8] Textbook implementation of RSA is subjected to timing-based side-channel attacks. Explain why (Hint: see how square and multiply algorithm works and tie this to a side-channel attack). Describe a simple blinding technique that can prevent this basic side-channel attack. This technique is also called masking.

4) [24] ORAM

[6] What is the basic formal security definition of ORAM? Please go on Google Scholar and find the Path-ORAM paper by Emil Stefanov et al.

[4] What is IND-CPA encryption? Give its formal definition based on symmetric encryption.

[4] Why IND-CPA encryption is required in order for ORAM to work?

[10] Give a basic Path ORAM tree with 8 items, where b1,…,b8 represent blocks to be accessed (assume stash size = 4). Denote each intermediate node with a number (see ORAM slides for an example). On this Path ORAM tree, why is accessing the same block arbitrary number of times yield indistinguishable access patterns? How is this achieved?

- Why IND-CPA encryption plays a role on this?
- Which step of Path-ORAM ORAM algorithm (in addition to IND-CPA aspect) is vital to achieve indistinguishable access patterns?