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) [15] Do you see any synergy between Elgamal encryption scheme and DH key exchange protocol? Explain how one implicitly uses another to achieve its objective. Describe algorithmic and mathematical transformation to show the synergy (a simple verbal description is not enough).

2[10] PKI Concepts:
- (4) What are the core components of a PKI? Briefly describe each component.
- (3) Discuss the trustworthiness of root certificates provided by browsers.
- (3) What is the purpose of the X.509 standard and what is a certificate chain? How is an X.509 certificate revoked?

3) [10] Consider the following network configuration, in which Iolus is used.

Assume the GSC is distributing a new group key to the group members using Iolus. How many times will this new key be encrypted and decrypted before A learns the value of the new key? Also describe what entity performs each of the encryption and decryption.
4) [15] Tree-based Group Diffie-Hellman. Consider the following tree to answer the questions. (Multipliers are given in red and blue, to prevent misunderstandings.)

(a) [10] Members n2, n4, and n7 decide to leave the group and form a new one. Clearly describe all the steps for this partition and draw the new trees.

(b) [5] Member n9 decides to leave the group (original tree). Clearly describe all the steps.

5) [10] You need to read the following paper to answer this question: Chung Kei Wong, Mohamed Gouda, Simon S. Lam, "Secure group communications using key graphs" In Proceedings of SIGCOMM '98, Pages: 68 - 79. Consider the following key tree.

(a) [5] If U_A is removed from the group, what keys should be changed?
(b) [5] Assume key oriented rekeying is used. Describe the messages the group manager needs to send to the group members. Use the following convention to describe each message:

\[ \text{GM} \rightarrow \{\text{set of users}\} : \{K_x\}K_y, \{K_z\}K_w, \ldots \]

**Extra Credit:**

6 [20] How can Schnorr signatures can offer additional benefits over ECDSA for blockchains? Describe a signature variant that can be obtained from Schnorr for this purpose. Cite a relevant research paper and give the algorithmic description of such a Schnorr signature variant.

7) [20] Impact of the PRGN Quality over digital signatures

Security of DLP-based Primitives

During the class, we have discussed Meta-Elgamal signature families. DSS and Schnorr signatures are some of the most well-known examples of such digital signatures. In all these schemes, during the signature generation phase, the signer invokes a PRNG. For instance, in Schnorr signature scheme randomness \( R \) is generated and used together with the message as \( H(M||R) \). Despite its advantages for the formal proof process, this approach may also create vulnerabilities for such cryptosystems. Consider the following attack:

The server computes a Schnorr signature under private key \( y \) periodically such that for every message \( M \) to be signed, it adds current time stamp \( ts_i \) and involve randomness \( R_i \) as \( H(M||ts_i||R_i) \) and follows the Schnorr signature algorithm as required. Here, \( r_i \) is the output of a PRNG, which derives randomness from certain Operating System (OS) parameters.

Assume that an attacker managed infiltrating a virus into the OS of the server, which is capable of resetting OS parameters that PRNG relies on, meaning the seed of PRNG is set to its initial values.

Show that by observing small-constant number of signatures, the attacker can totally break the Schnorr signature scheme under these circumstances (remark that it does not mean the Schnorr signature scheme is flawed, it is about how it is used with certain PRNGs).

You must show how the attack works step by step, by illustrating algebraic recovery step, and explain how \( ts_i \) and \( r_i \) play a role in this attack. Moreover, there are special techniques and conditions for recover to be performed. Explicitly discuss these conditions.