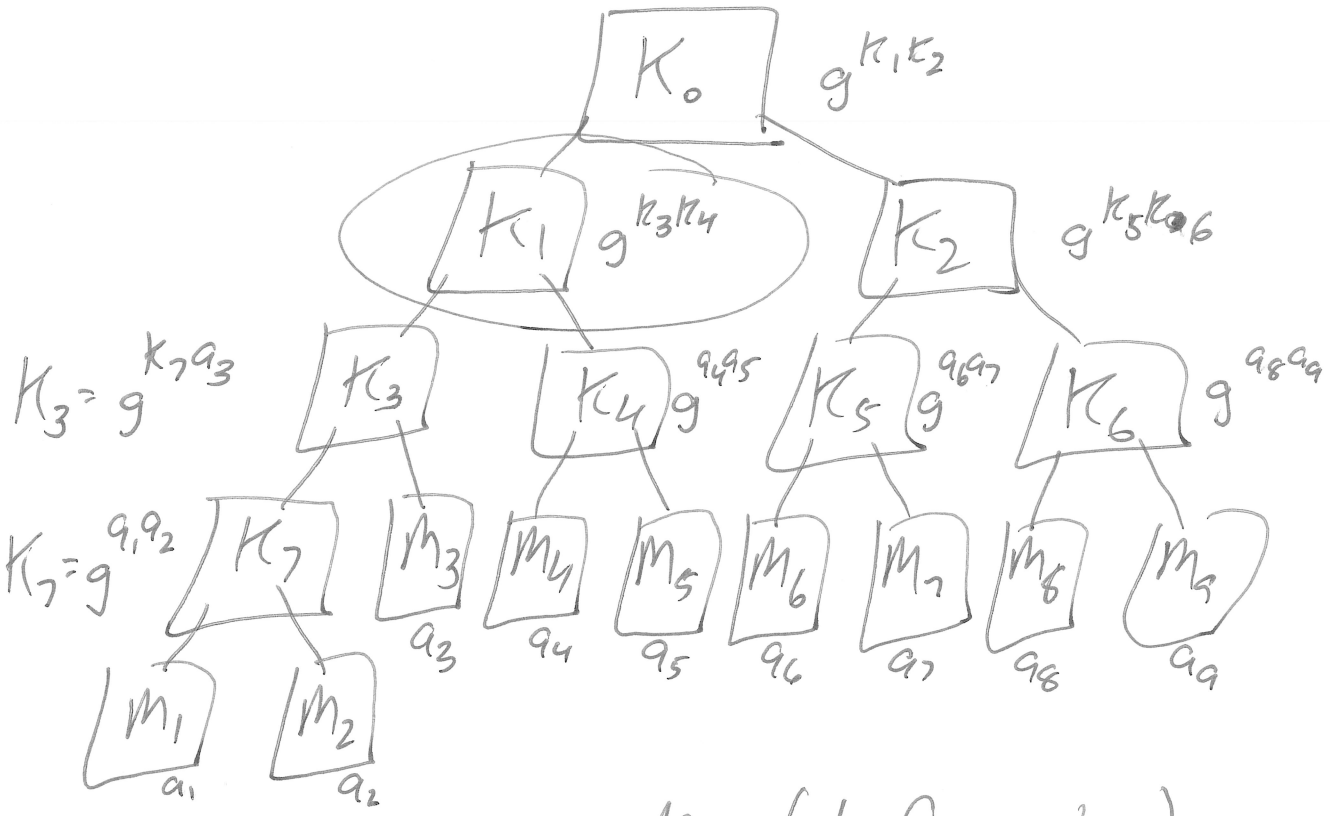
CIS 3362 11/17/21

Group Diffie-Hellman Key Exchange



Users: m_1 to m_9 (leaf nodes)

Blinded Keys: K_0 to K_7

Public: Prime p
generator g

Private keys for m_i are a_i

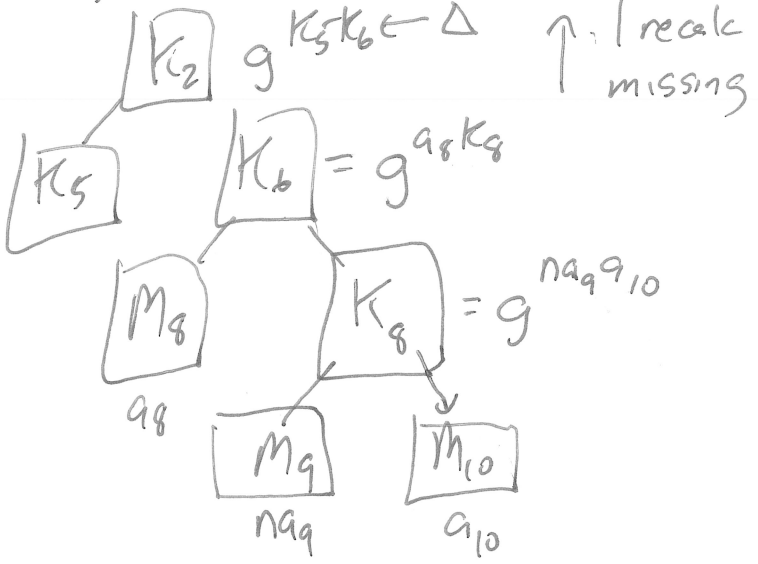
Questions: Adding User ?
Deleting User ?
} Run-Times?

Imagine adding M_{10}.

(1) Choose leaf node to "add to". (M_9)

(2) Add blind key to take place of location of M_9.
This will we the shared key between M_9, M_{10}.

(3) Go up ancestral path of tree and update each shared password.



Runtime = O(height)
= O(lg n).

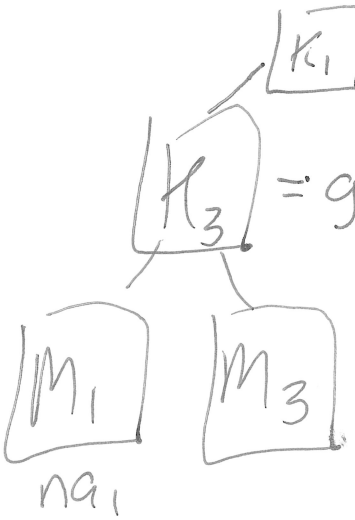
n = # people

Consider Deleting M_2

(1) We will replace its parent, K_7 with its sibling, M1.

(2) M1 chooses new private key, na_1.

(3) Bubble up new passwords as before.



Run-time is O(height)
= O(lg n)

n = # of users