

CIS 3362 - 11/3/23

⑥ I'm here 11/10 - 11/18

Group Key Management

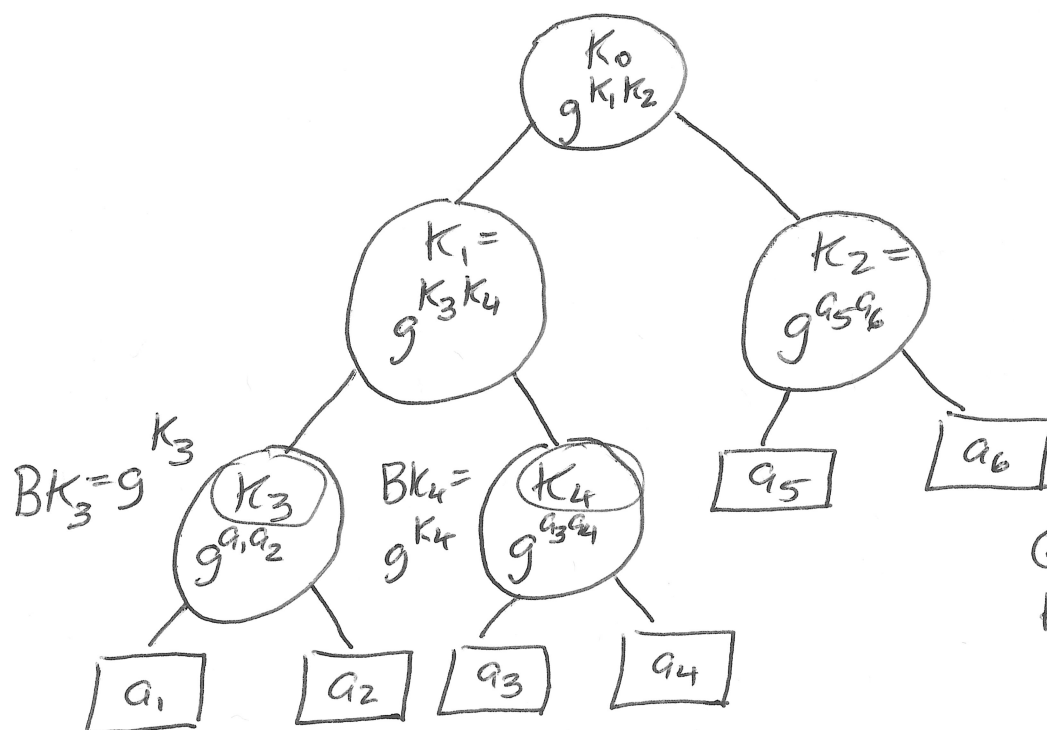
① Group Diffie-Hellman (Tree-Based)

p prime, g generator

Alice, Bob, Carol

a b c

$g^{abc} \bmod p$ shared group key



Users in leaf nodes in tree.

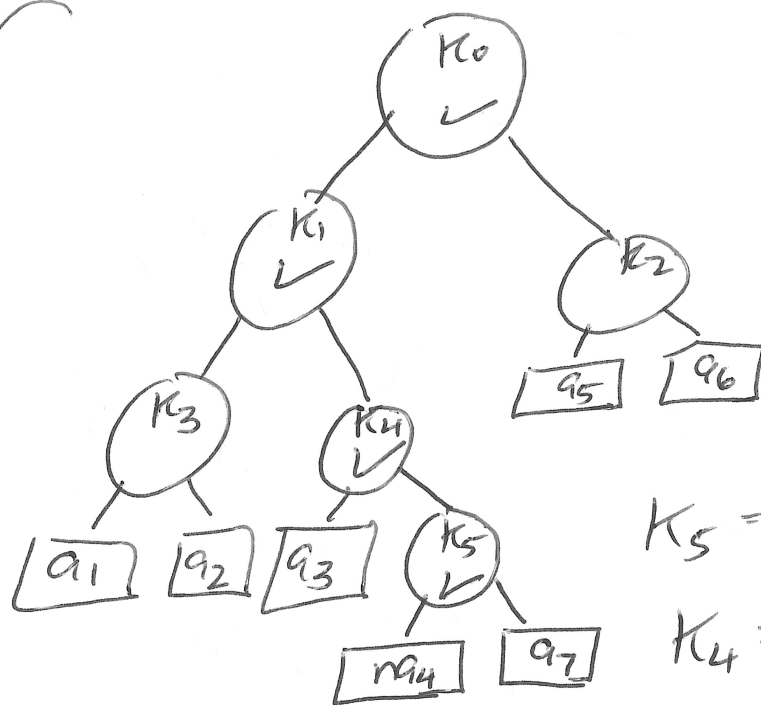
Internal nodes: own secret key this is what each group shares

Group Keys K_0, K_1, K_2, K_3, K_4

① Add User - pick current user as a sponsor
Example a_4 sponsors a_7 .

② Delete User - a_1 wants to leave

Run-time
 $O(h)$
 $h =$
height of
tree



In sequence
calculate new
keys up the
tree.

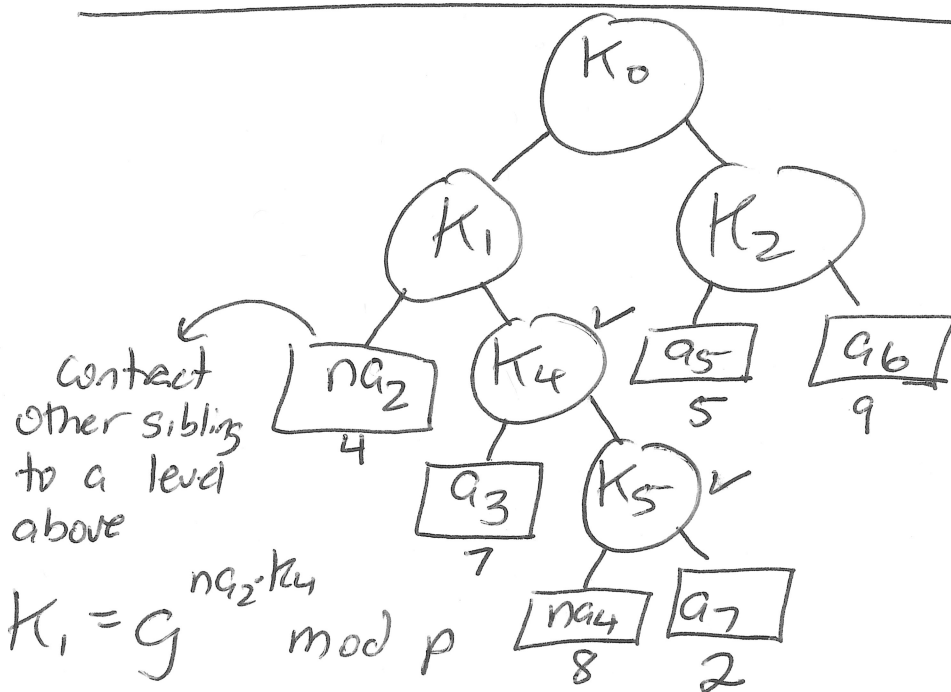
$$K_5 = g^{na_4 \cdot a_7} \mod p$$

$$K_4 = g^{a_3 K_5} \mod p$$

$$K_1 = g^{K_3 K_4} \mod p$$

$$K_0 = g^{K_1 K_2} \mod p$$

Delete a_1



$$K_1 = g^{na_2 \cdot K_4} \mod p$$

$$K_0 = g^{K_1 K_2} \mod p$$

$$p = 11 \quad \phi(11) = 10$$

$$g = 2$$

$$K_5 = 2^{2 \times 8} = 2^{16} \equiv 2^6 \equiv 64 \equiv 9 \mod 11$$

$$K_5 = 9$$

$$K_4 = 2^{7 \times 9} = 2^{63} \equiv 2^3 \equiv 8 \mod 11$$

$$K_4 = 8$$

$$K_2 = 2^{5 \times 9} = 2^{45} \equiv 2^5 \equiv 32 \equiv 10 \pmod{11}$$

$$\boxed{K_2 = 10}$$

$$K_1 = 2^{4 \cdot 8} = 2^{32} \equiv 2^2 \equiv 4 \pmod{11}$$

$$\boxed{K_1 = 4}$$

$$K_0 = 2^{4 \times 10} = 2^{40} \equiv 1 \pmod{11}$$