Group Diffie-Hellman Key Exchange

Users: M₁ to M₉ (leaf nodes)
Blank keys: K₀ to K₃
Public: Prime p
generator g

Private keys for Mᵢ are aᵢ, aᵢ

Questions: Adding User? Run-Times?
Deleting User?
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 use the shared key between \(M_9, M_{10}\).
3. Go up ancestry path of tree and update each shared password.

\[
\text{Runtime} = O(\text{height}) \\
= O(\log n).
\]

\(n = \# \text{ people}\)

---

Consider Deleting \(M_2\)

1. We will replace its parent, \(K_7\) with its sibling, \(M_1\).
2. \(M_1\) chooses new private key, \(na_1\).
3. Bubble up new passwords as before.

\[
K_{11} = g^{K_{13}K_4} \uparrow \text{recall missing}
\]

\[
K_{13} = g^{na_1g_3}
\]

\[
M_1, M_3
\]

\(\text{Runtime is } O(\text{height}) \\
= O(\log n)\)

\(n = \# \text{ of users}\)