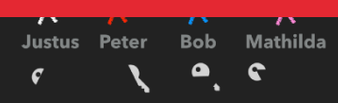
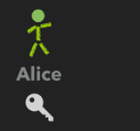
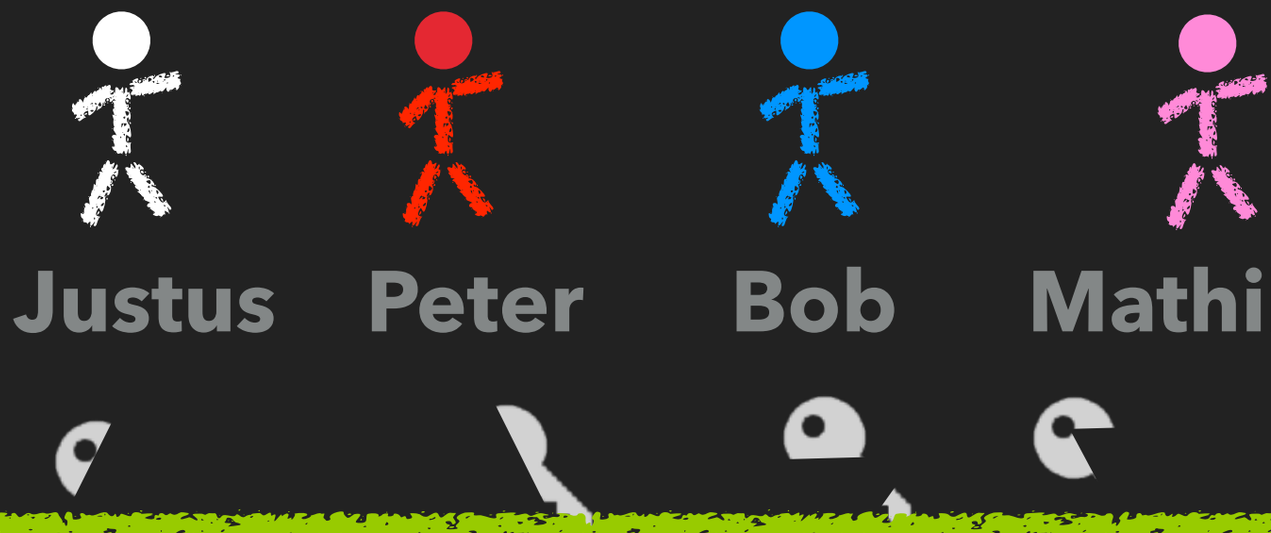
DO NOT TRY THIS WITHOUT A CRYPTOGRAPHER

SECRET SHARING







Secret sharing (“t out of n”) shares a secret such, that the secret can be restored with any t (here 3) of the n (here 4) parts.

This can be used for secret recovery without a single point of trust (failure).

DO NOT TRY THIS WITHOUT A CRYPTOGRAPHER

PATTERNS

KEY DERIVATION 1: PASSWORD TO KEY