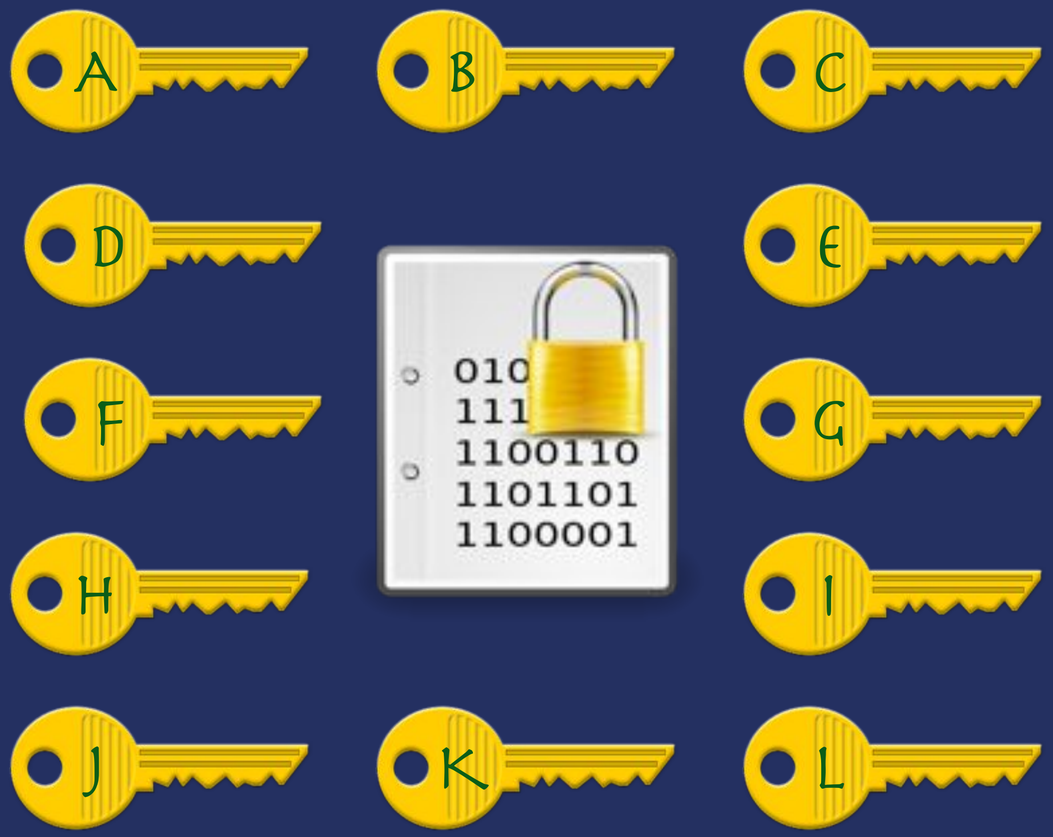
Keeping Secrets

Keeping Secrets

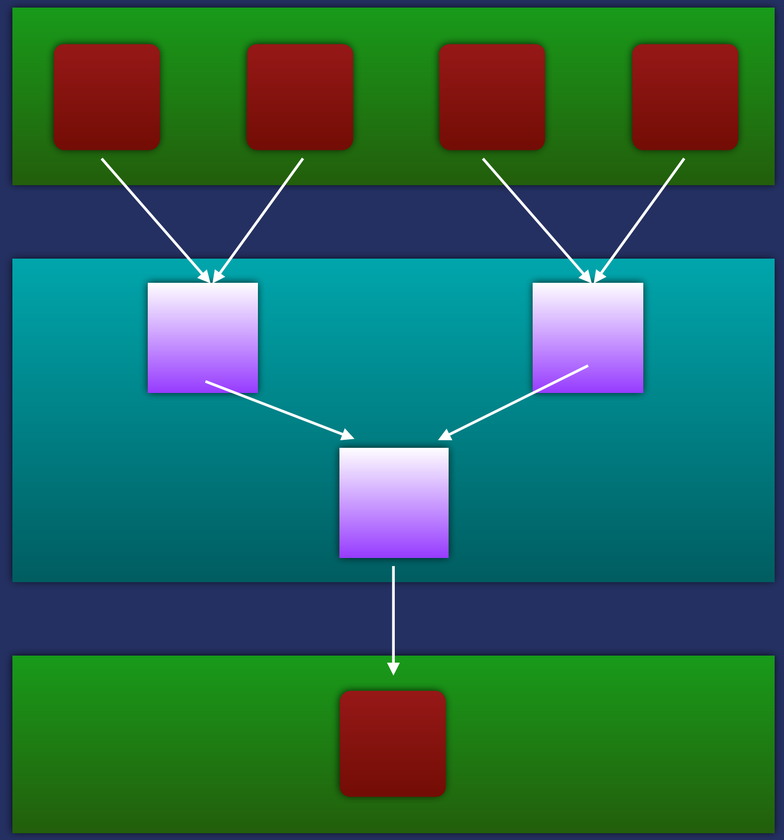
O-SNAP has some data that is too sensitive for a single individual to be able to access alone.

Our security consultants have suggested that we use an xor encryption scheme where need to know parties each have keys of different lengths which are merged together to form a one time pad.



Collective Reduce Pattern

- N atomic data units to one output
- N-ary operation (often binary) applied to all data units
- Order of application does not change the result



Next Steps

Go to the shell and pull from the repository.

Make a parallel implementation in OpenMP, Cilk, and TBB

Solution Sketch

- Have each user load their key
- Wrap the key with a generator function to get the i-th byte
- xor the i-th byte of all keys and the message to produce the output byte