

Project notes

Weekly meetings Thurs morn until March.

Sha 256 & 512

Keccak

Nist finalist

- 1.) lightweight key implementation - Small size
- 2.) Benchmark against kyber

Outcomes

Demo Tues 12th Jan @ 11:00

Demo Powerpoint w/ code & slides - Live 1:00

Key gen Stage - compare benchmarks

Report still due Friday

Thursday weekly morning meetings - Ayesha to Plan