From: Alagic, Gorjan (Assoc)
To: Alagic, Gorjan (Assoc)
Subject: RE: last minute
Date: Tuesday, April 9, 2019 9:25:00 AM

Ok, LAC now does have a line saying they use SHA256 etc.

I see Ray put in that LEDA does not specify some stuff, including hash. I guess there is a line somewhere in the doc that they use SHA-3 for the FO transform, so I still checked that it seems complete.

Sorry about doing this last-minute.

From: Alagic, Gorjan (Assoc)
Sent: Tuesday, April 9, 2019 9:14 AM
To: Moody, Dustin (Fed) <dustin.moody@nist.gov>
Subject: RE: last minute

I'm just finishing going through LEDAcrypt now. I will have a look at the updated LAC too. Thanks.

From: Moody, Dustin (Fed)
Sent: Tuesday, April 9, 2019 9:12 AM
To: Alagic, Gorjan (Assoc) <gorjan.alagic@nist.gov>
Subject: last minute

Gorjan,

I didn't see a review for LEDAcrypt. Am I missing seeing it? Also, I asked LAC to update their spec with the hash function details. They already sent me the update – and it's uploaded on sharepoint. Can you check to make sure you're satisfied now? Thanks,

Dustin