

From: [Kerman, Sara J. \(Fed\)](#)
To: [Moody, Dustin \(Fed\)](#)
Subject: RE: FAQ small revision
Date: Wednesday, April 26, 2017 3:10:00 PM
Attachments: [FAQs-Historical. v3.docx](#)

I may be over analyzing how to show the changes to Question 15 in the archive file. Attached is what I've done. Please feel free to offer another option. ☺

Sara

From: Moody, Dustin (Fed)
Sent: Wednesday, April 26, 2017 1:55 PM
To: Kerman, Sara J. (Fed) <sara.kerman@nist.gov>
Subject: RE: FAQ small revision

For complete transparency, we probably should. We also had an earlier version of this answer that could also be archived.

But yeah – it's not a big change, so it's not that critical.

From: Kerman, Sara J. (Fed)
Sent: Wednesday, April 26, 2017 1:53 PM
To: Moody, Dustin (Fed) <dustin.moody@nist.gov>
Subject: RE: FAQ small revision

So since the majority of the answer remains the same, do I need to do anything with moving the removed information to the "archive" section?

<http://csrc.nist.gov/groups/ST/post-quantum-crypto/archive.html>

From: Moody, Dustin (Fed)
Sent: Wednesday, April 26, 2017 1:48 PM
To: Kerman, Sara J. (Fed) <sara.kerman@nist.gov>
Subject: FAQ small revision

Sara,

Can you remove one sentence from our PQC FAQ #15? The answer currently says:

A15: The function `randombytes()` will be available to the submitters. This is a function from the SUPERCOP test environment and should be used to generate seed values for an algorithm. `Randombytes` should only be used to seed a NIST-approved DRBG.

The revision is to remove the last sentence:

Randombytes should only be used to seed a NIST-approved DRBG.

And the remaining paragraphs should stay the same. Thanks!

Dustin