From:	Miller, Carl A. (Fed)
To:	Moody, Dustin (Fed)
Subject:	Re: Background reading on crypto
Date:	Tuesday, November 29, 2016 5:21:45 PM

Ok, I'll take a look at Koblitz's books too. Thanks.
-Carl

—————

Carl A. Miller
Mathematician, Computer Security Division
National Institute of Standards and Technology
Gaithersburg, MD

From: "Moody, Dustin (Fed)" <dustin.moody@nist.gov>
Date: Tuesday, November 29, 2016 at 1:46 PM
To: "Miller, Carl A. (Fed)" <carl.miller@nist.gov>
Subject: RE: Background reading on crypto

Carl,

I'm probably not the best person to ask for symmetric crypto. Even for public key, I'm not sure which books are really good. I used Koblitz's books, which are all pretty good. I never took a course on "crypto" really. I have heard of the Katz & Lindell book, so it's probably pretty good. Sorry I'm not more help!

Dustin

From: Miller, Carl A. (Fed)
Sent: Tuesday, November 29, 2016 1:42 PM
To: Moody, Dustin (Fed) <dustin.moody@nist.gov>
Subject: Background reading on crypto

Hi Dustin –

I'm planning to do some studying of classical crypto, and I'm curious if you have any recommendations for good surveys or textbooks? Where I'm coming from is that I have a strong math background, and I've also dealt with the quantum versions of some classical crypto concepts, but I've not studied classical crypto formally. Thus something fairly broad/basic may be good to start. So far I've found this book: http://www.nowpublishers.com/article/Details/TCS-001 , which looks short and easily digestible. There's also "Introduction to Modern Cryptography" by Katz & Lindell, but that seems to be very popular and it's hard to track down a library copy. Talk to you later!

-Carl

—————

Carl A. Miller
Mathematician, Computer Security Division
National Institute of Standards and Technology
Gaithersburg, MD