

## newbie Q's about RSA, OAEP

**Source:** <http://www.derkeiler.com/Newsgroups/sci.crypt/2003-11/1996.html>

---

**From:** Dominic (*dominicsmith501\_at\_hotmail.com*)

**Date:** 11/28/03

Date: 28 Nov 2003 07:20:43 -0800

I've found articles covering the maths behind these algorithms, but is there anything which gives a good introduction to their practical use?

Are there recommended minimum/maximum lengths for RSA keys?

Is it safe (not necessarily efficient) to code long messages in RSA by splitting it into blocks and coding each separately (as you would with Rijndael). Are ECB, CBC modes applicable in that case?

Should you generally use OAEP rather than coding the message uncooked? I know this is a good idea when encoding short messages to avoid dictionary attacks, but is it useful with longer messages?

Is there an accepted scheme for indicating the length of the message?

Dom