

Re: XOR passphrase with a constant

Source: <http://www.derkeiler.com/Newsgroups/sci.crypt/2005-05/1210.html>

From: Andrew (anelless_at_gmail.com)

Date: 05/30/05

Date: 30 May 2005 11:49:50 -0700

Furthermore given two different passphrases P1 and P2, a single known constant C, $H(C + P1)$ and $H(C + P2)$, is finding a collision for either made any easier than finding a collision for $H(P1)$ or $H(P2)$ if an attacker knows these instead?

My guess would be that if $\text{Length}(C + P1) > \text{Length}(H(C + P1))$ but $\text{Length}(P1) \leq \text{Length}(H(P1))$ then the task would be made easier. But to be honest it's all a bit much for me to visualise.