

Re: Inverse Hash Function

Source: <http://www.derkeiler.com/Newsgroups/sci.crypt/2004-12/1918.html>

From: Valery Pryamikov (*Valery_at_nospam.harper.no*)

Date: 12/30/04

Date: Thu, 30 Dec 2004 12:18:10 +0100

"Henrick Hellström" <henrick.hellstrm@telia.com> wrote in message
news:ScRAd.12515\$d5.108371@newsb.telia.net...

> *Valery Pryamikov wrote:*

>

>> *If you are only interested in collision resistant, but not one way hash –*

>> *you can find such scheme.*

>>

>> *Preimage resistance is not possible due to your requirement $(h(h'(B)))=B$*

>>

>>

>>

>> *BTW: here is a simple scheme that satisfies your condition:*

> *[snip]*

>> *(classic RSA).*

>

> *Classic RSA is not collision resistant. $A, A+m$ is a collision.*

yep, that's right.

–Valery