

# Hash collisions

---

*Source:* <http://sci.tech-archive.net/Archive/sci.math/2007-12/msg00203.html>

---

- *From:* [marksmith@xxxxxxxxxxxxxxxxxxxxx](mailto:marksmith@xxxxxxxxxxxxxxxxxxxxx)
  - *Date:* Sat, 1 Dec 2007 12:13:27 -0800 (PST)
- 

Hi all,

I am working through some past questions for a mid term exam:

"Assuming that it is computationally infeasible to launch attacks that require  $2^{128}$  computations of hash values, how long should the hash values be to achieve weak and strong collision resistance respectively?" – 5 marks.

I've done some research on the internet, and can't find any hard definitions for "strong" or "weak" collision resistance. Obviously collisions are impossible to avoid completely (unless of course the hash is larger than the messages themselves!).

But do you have any idea how to arrive at hard and fast numbers for these terms?

Thanks,

Mike

.