Illegal Hashes

By @edent on 2022-11-28 · #cryptography #hashing #NaBloPoMo · 7 comments · 450 words

To understand this blog post, you need to know two things.

01. There exists a class of numbers which are illegal in some jurisdictions. For example, a number may be copyrighted content, a decryption key, or other text considered illegal.
02. There exists a class of algorithms which will take any arbitrary data and produce a fixed length text from it. This process is known as "hashing". These algorithms are deterministic - that is, entering the same data will always produce the same hash.

Let's take the MD5 hashing algorithm. Feed it *any* data and it will produce hash with a fixed length of 128 bits. Using an 8 bit alphabet, that's 16 human-readable characters.

Suppose you live in a country with *Lèse-majesté* - laws which make it treasonous to insult or threaten the monarch.

There exists a seemingly innocent piece of data - an image, an MP3, a text file - which when fed to MD5 produces these 128 bits:

```
01001001 00100000 01101000 01100001
01110100 01100101 00100000 01110100
01101000 01100101 00100000 01110001
01110101 01100101 01100101 01101110
```

Decoded into ASCII, that spells `I hate the queen .`

128 bits is *probably* too short to be illegal in all but the most repressive of regimes. It would be hard, if not impossible, to squeeze terrorist plans into that little space.

But it is just enough space to store an encryption key for copyrighted material.

Therefore, it is possible that there exists a file which - by pure coincidence - happens to have an MD5 hash which is illegal.

Because MD5 is a relatively weak algorithm, it is possible to create *deliberate* hash "collisions". That is, take some data and manipulate it until it has the *same* MD5 as a different piece of data.

Someone could, theoretically, deliberately create a file which looks unremarkable when viewed, but is illegal when hashed.

The SHA-1 hashing algorithm produces 160 bits - 20 ASCII characters. It is *somewhat* cheap and easy to produce a file with a specific SHA-1 hash.

The SHA-512 hashing algorithm, as its name suggests, produces a 512 bit hash. That's enough space for 64 ASCII characters. Is that long enough to contain text which is blatantly illegal? Almost certainly. But modern hashing algorithms are designed to be resistant to collision attacks. So much so that it seems like theoretical quantum computers will be needed to crack them. The chances of any file having an illegal hash is infinitesimally small.

Nevertheless, it intrigues me that there may be a form of hash-steganography. How would you detect whether the hash of a file was problematic?

7 thoughts on “Illegal Hashes”

Christian Lawson-Perfect says: 2022-11-28 12:42

@Edent oh, that's a brilliant idea! A person could even put out an album of a dozen or so innocuous MP3 files whose MD5 hashes would concatenate to a long illegal string.I'm not sure this would be as much of a technicality to avoid prosecution as you'd like it to be - as easy as collisions are to deliberately find, they're still very hard to stumble across, so you'd have to go a long way to make it look accidental

Reply

iucounu says: 2022-11-28 13:05

@Edent I seem to remember this was likely the case with criminal.jpg: an innocuous doodle that would get your account instantly locked if you posted it on Twitter.

The hypothesis was, it had the same hash as a banned image, and I guess Twitter checks image hashes?

Reply

Lawrence Akka KC says: 2022-11-28 13:33

@christianp @Edent Not sure I follow. I guess the hypothetical law might say that stating "I hate the Queen" would be illegal. Publishing the hash would not be "stating" IHTQ. So there would be no offence. Much would turn on the wording of the actual law.

Reply

Lawrence Akka KC says: 2022-11-28 13:33

@christianp @Edent If everyone started publishing the hash, and it became sufficiently known that it represented the forbidden text, then a judge would have to decide whether publishing the hash was sufficiently equivalent to 'stating' IHTQ, such that an offence had been committed.

Reply

Christian Lawson-Perfect says: 2022-11-28 13:36

@law @Edent that's what I was thinking of: if it was well-known that the hash could be computed to produce the illegal string, then distributing the original file would be considered equivalent to distributing the illegal string.But I know nothing about the law, so it'd be the height of arrogance not to defer to you!

Reply

raymii says: 2022-11-28 16:15

raymii reposted this Article on lobste.rs.

Reply

Alan says: 2022-11-28 17:23

Not a lawyer and this is for entertainment only, but in the US I believe for it to be a crime it would require evidence of intent to use those bits for said illegal purposes. Simply having the bits is not enough to constitute a crime, since there are valid legal reasons to have those bits. More philosophically, information requires a context of interpretation and without an implied context of usage it has no meaning. The word "Beans" may have a specific precise meaning in one context, and an entirely different meaning in a different context.

Reply

Leave a Reply

Your email address will not be published. Required fields are marked *

Comment *

Name *

Email *

Website

Notify me of follow-up comments by email.

Notify me of new posts by email.

Post Comment

To respond on your own website, enter the URL of your response which should contain a link to this post's permalink URL. Your response will then appear (possibly after moderation) on this page. Want to update or remove your response? Update or delete your post and re-enter your post's URL again. (Learn More)

URL/Permalink of your article

Ping me!

Found this post useful? Click the icons to support this blog

More ways to support my blog

Get new posts by email

Enter your email address to subscribe to this blog and receive brand new posts by email.
(Or subscribe to this  Atom Feed.)

Email Address

Free Sign Up

Join 13,468 other subscribers.

🔎 Search Blog Posts

Search

Explore The Archives

2022		
January 30 posts	February 23 posts	March 15 posts
April 19 posts	May 19 posts	June 19 posts
July 19 posts	August 18 posts	September 12 posts
October 8 posts	November 28 posts	December

2021		
January 31 posts	February 28 posts	March 31 posts
April 30 posts	May 31 posts	June 30 posts
July 31 posts	August 31 posts	September 30 posts
October 31 posts	November 30 posts	December 31 posts

2020		
January 31 posts	February 29 posts	March 31 posts
April 30 posts	May 31 posts	June 30 posts
July 31 posts	August 31 posts	September 30 posts
October 31 posts	November 30 posts	December 31 posts

2019		
January 31 posts	February 12 posts	March 17 posts
April 12 posts	May 12 posts	June 10 posts
July 7 posts	August 5 posts	September 6 posts
October 14 posts	November 30 posts	December 17 posts

2018		
January 8 posts	February 4 posts	March 6 posts
April 14 posts	May 5 posts	June 6 posts
July 6 posts	August 13 posts	September 14 posts
October 8 posts	November 30 posts	December 4 posts

2017		
January 12 posts	February 9 posts	March 8 posts
April 4 posts	May 10 posts	June 5 posts
July 5 posts	August 6 posts	September 3 posts
October 4 posts	November 30 posts	December

2016		
January 10 posts	February 10 posts	March 11 posts
April 9 posts	May 8 posts	June 9 posts
July 6 posts	August 9 posts	September 4 posts
October 2 posts	November 30 posts	December 14 posts

2015		
January 8 posts	February 11 posts	March 10 posts
April 4 posts	May 9 posts	June 3 posts
July 7 posts	August 9 posts	September 10 posts
October 2 posts	November 30 posts	December 4 posts

2014		
January 13 posts	February 13 posts	March 14 posts
April 14 posts	May 8 posts	June 7 posts
July 9 posts	August 5 posts	September 5 posts
October 1 post	November 30 posts	December 20 posts

2013		
January 25 posts	February 17 posts	March 15 posts
April 18 posts	May 11 posts	June 14 posts
July 6 posts	August 14 posts	September 6 posts
October 4 posts	November 30 posts	December 14 posts

2012		
January 14 posts	February 8 posts	March 13 posts
April 15 posts	May 10 posts	June 16 posts
July 8 posts	August 8 posts	September 6 posts
October 6 posts	November 30 posts	December 31 posts

2011		
January 13 posts	February 11 posts	March 11 posts
April 12 posts	May 8 posts	June 8 posts
July 6 posts	August 5 posts	September 11 posts
October 7 posts	November 30 posts	December 17 posts

2010		
January 6 posts	February 15 posts	March 12 posts
April 13 posts	May 4 posts	June 3 posts
July 15 posts	August 8 posts	September 11 posts
October 9 posts	November 30 posts	December 9 posts

2009		
January 1 post	February 5 posts	March 3 posts
April 7 posts	May 12 posts	June 8 posts
July 10 posts	August 10 posts	September 12 posts
October 22 posts	November 31 posts	December 15 posts

2008		
January 2 posts	February	March 2 posts
April 3 posts	May 2 posts	June
July 1 post	August 3 posts	September 1 post
October 3 posts	November 2 posts	December 1 post

2007		
January	February	March
April	May	June
July	August	September
October	November 4 posts	December 5 posts

2006		
January	February	March
April 1 post	May	June
July	August	September
October	November 1 post	December

2005		
January	February	March 1 post
April	May	June
July	August	September 1 post
October	November	December

2004		
January	February	March
April	May 5 posts	June 3 posts
July 1 post	August	September
October	November	December

2003		
January	February	March 2 posts
April	May	June
July	August	September
October	November	December

2002		
January	February 1 post	March
April 3 posts	May	June
July	August	September
October	November	December

2001		
January	February	March
April	May	June
July 1 post	August	September
October 1 post	November	December

2000		
January	February	March 1 post
April	May	June
July	August	September
October	November 1 post	December

1999		
January	February	March
April	May	June
July	August	September 1 post
October	November	December 1 post

1997		
January 1 post	February	March
April	May	June
July	August	September
October	November	December

1995		
January	February	March 1 post
April	May	June
July	August	September
October	November	December

1987		
January	February	March
April	May	June
July	August	September
October	November	December 1 post

ISSN 2753-1570