

Nat McHugh

An important site on a minor internet.

Home	About	PGP Key	
------	-------	---------	--

Tuesday, November 11, 2014

Three way MD5 collision

Previously I explained how I created two images one of James Brown the other of Barry White with the same MD5 hash. At the end of the post I said I was going to try and create a three way collision where three images have the same MD5 hash. Neil K made a suggestion about the image



Neil
@kneil_

Follow

@natmchugh Image suggestion for the third hash collision:
White, Brown, ...and Black -- day19.com/images/pics/20...
7:07 AM - 4 Nov 2014

1

So I set to work.

After a couple of false starts where I started with the wrong image file I managed to achieve a three way collision. Here are the images.



Twitter

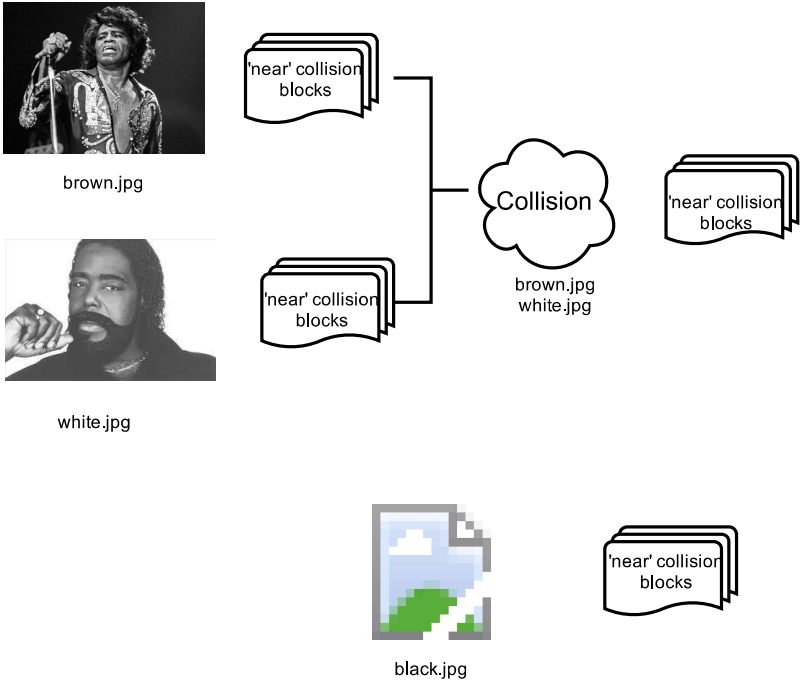


If you want to check

```
1 $ curl -s http://www.fishtrap.co.uk/black.jpg.coll | md5
2 b69dd1fd1254868b6e0bb8ed9fe7ecad
3 $ curl -s http://www.fishtrap.co.uk/brown.jpg.coll | md5
4 b69dd1fd1254868b6e0bb8ed9fe7ecad
5 $ curl -s http://www.fishtrap.co.uk/white.jpg.coll | md5
6 b69dd1fd1254868b6e0bb8ed9fe7ecad
```

A new hash value

This isn't the same hash as before instead the 3 images now collide with a new hash value b69dd1fd1254868b6e0bb8ed9fe7ecad . This is because I had to add near collision blocks to all three images. In the case of the first two the blocks added are the same. This is probably best illustrated with a diagram.



Again I created the files with HashClash. As inputs I used white.jpg and black.jpg images. To

Tweets by @natmchugh

natmchugh

@natmchugh

@katie_fenn ok 🔥🔥🔥

17 May

natmchugh

@natmchugh

@katie_fenn I have one if you need to borrow one.

17 May

natmchugh

@natmchugh

Ah yes short Weierstrass form versus Edwards form, very amusing.

12 May

natmchugh

@natmchugh

@katie_fenn Sadly not available beta.companieshouse.gov.uk/search/c ompani...+

Embed View on Twitter

Popular Posts

Create your own MD5 collisions
A while ago a lot of people visited my site (~ 90,000) with a post about how easy it is to make two images with same MD5 by using a chos...

How I created two images with the same MD5 hash
I posted the following images the other day which although looking totally different have exactly the same MD5 hash (e06723d4961a0a3f950e...

How I made two PHP files with the same MD5 hash
I recently posted a link on twitter to two PHP scripts which have different behaviours but the same MD5 hash. To verify this download the fi...

How to make two binaries with the same MD5 hash
One question I was asked when I demo'd creating two PHP files with the same hash is; does it work on compiled binaries? Well the ans...

Three way MD5 collision
Previously I explained how I created two images one of James Brown the other of Barry White with the same MD5 hash. At the end of the post I...

The Magic Words are Squeamish Ossifrage - factoring RSA-129 using CADO-NFS
This thing got long and can basically be summarised as: I factored smaller RSA numbers on free cloud computing using excellent open sour...

Hash Collisions Reading List


make brown.jpg.coll I just had to append the extra collision blocks to brown.jpg which was already a collision with white.jpg.

I could go on adding more and more files in a tree structure to get many documents to collide. The number of collisions needed is n-1 where n is the number of files. It was this tree of collisions that allowed Marc Stevens to [predict the 2008 US presidential election](#).

A word about file sizes

The files started out different sizes to each other, however, before each collision was generated between two files padding had to be added to one of the files to make it the same as the other. Without this step it would be impossible to extend a collision in the unpadded version to the full MD5 algorithm. This is because the padding includes the size of data processed.


Posted by [Nathaniel McHugh](#) at [10:20 PM](#)

 +1 Recommend this on Google

Labels: [Hash functions](#)

Location: [Sheffield, South Yorkshire, UK](#)

1 comment:

 **Blake Bond** Monday, March 06, 2017

<http://md5online.co.uk/>

[Reply](#)

Enter your comment...

Comment as:

Select profile... ▼

Publish

Preview



Lately in an effort to code up and properly understand the Wang attack on the MD4 family of hash functions I've been reading a lot of pa...



Images with colliding MD5 hash

These images of James Brown and Barry White have the same MD5 hash e06723d4961a0a3f950e7786f3766338. Don't believe me. You can...



Bug Bounty - Remote Code Execution in Magento 1.x

Magento is a popular ecommerce solution written in PHP. It is widely used for web shops both large and small. The most current product is Ma...



MD5 collisions in ssh keys

You can insert MD5 collision blocks in many data formats and if you do it right the result will be 2 objects that differ but which when pass...

Labels

- [Cloud](#)
- [Hash functions](#)
- [Maths](#)
- [MD5](#)
- [PHP](#)
- [RSA](#)

Blog Archive

- [2017](#) (1)
- [2015](#) (8)
- ▼ [2014](#) (5)
 - ▼ [November](#) (2)
 - [Three way MD5 collision](#)
 - [Colliding MD5 Images go crazy](#)
 - [October](#) (3)

Links

- [Inviqa](#)
- [Sheffield PHP User Group](#)
- [Fishtrap](#)