

Re: Manual hashing

Source: <http://www.derkeiler.com/Newsgroups/sci.crypt/2004-06/2147.html>

From: AE (*hidden_at_nospam.com*)

Date: 06/29/04

Date: Tue, 29 Jun 2004 20:32:30 +0200

Here yet another suggestion I tried today: It's based on error correcting codes.

I'm using the string "mokkongshen" as an example.

1) convert characters and numbers to decimal numbers

For english text I'd use the following well known scheme to convert frequent characters to single digits and less frequent characters to pairs of digits.

```
1 2 3 4 5 6 7 8 9 0
a e i n o r s t
9 b c d f g h j k l m
0 p q u v w x y z # .
```

. is the stop symbol as used in a telegram

is necessary to switch between numbers and characters.

Every number is represented by itself, repeated once, so there's no collision between a number and this character.

The resulting number sequence is:

```
90 5 98 98 5 4 95 7 96 2 4
```

It's easier for me to do additions with numbers than with characters and numbers. Else I would have omitted this step.

2) Write this number sequence in the smallest square it fits.

Our example happens to fit exactly in a 4x4 square.

In other cases it might be necessary to fill the square with sequences of 09 (a combination that doesn't make sense at the end of a string and that doesn't make sense when being repeated so no danger a string could be replaced with a string where just 09 is appended.

Sum the rows and columns modulo 10.

9059 3
8985 0
4957 5
9624 1

0405

This is my compression step. Larger sequences should be split into several squares of at most 9x9 – this makes calculation less error-prone and preserves in the checksum of every square the entropy of typical english text.

- 3) Repeat this step with one or more squares that are filled in a different way. Don't simply change rows and columns – I'm filling them once diagonal and once in a spiral.

9098 6 9059 3
5859 7 7968 0
9476 6 5429 0
9524 0 9458 6

2737 0784

Generally it's simple to find a second square that produces the same checksum as the first one and that way to produce collisions. Adding these additional squares it should be more puzzling for the attacker to produce collisions.

- 4) Concatenate the resulting digits to numbers – and sum the rows of each square and the columns of each square.

$$3051 + 6760 + 3006 = 12817$$

$$0405 + 2737 + 0784 = 03926$$

The concatenation of row-sum and column-sum is the checksum:

0392612817

This is simply a different compression step that doesn't commute with addition modulo 10.

In this special example compression is not as good as requested, but for larger texts results will be better.