

## Re: [XPOST] A unique number for every "person" – can it be done?

**Source:** <http://sci.tech–archive.net/Archive/sci.math/2005–02/9893.html>

---

**From:** Virgil (ITSnetNOTcom#virgil\_at\_COMCAST.com)

**Date:** 02/27/05

Date: Sun, 27 Feb 2005 12:38:51 -0700

In article <1109531453.50e0ba7c6d32846284ce75a5760458db@meganetnews2>, TGOS <tgos@invalid.invalid> wrote:

- > Hello,
- >
- > First please excuse the xpost, but the topic of this post does not fit
- > into any single NG and I didn't want to miss the right people by posting
- > to the wrong NG. Maybe we can find out where it really belongs to in the
- > discussion process and move the thread to the right group.
- >
- > For halve a year now I'm thinking about creating an algorithm, this
- > sounds like math, but without some form of hashing used in cryptography
- > it will most likely get nowhere, and the topic is program related. You
- > see, it's very hard to categorize the topic.
- >
- > The problem can be summarized in one sentence:
- >
- > Calculate a number for every human being, company and organization on
- > earth, that is guaranteed to be unique till the end of time.
- >
- > The rules in detail:
- >
- > 1) Every "person", real person or corporate body (like company or
- > organization), needs a number. Every means every one world wide.
- >
- > 2) Then number must be unique. Neither may there be two "persons" having
- > the same number at the same time, nor may there be two "persons" having
- > the same number at a different time. Even two billion years after my
- > death, nobody may have my number. For cryptographers, if it were a hash,
- > it must be guaranteed to be collision free, whereby the possibility of
- > collisions is allowed if the likeliness is close to zero (one in a
- > billion of cases) and if you can handle it (e.g. in case a collision
- > should one day be noticed, it is solved by ...) to still give both
- > involved parties a unique number.
- >
- > 3) The numbers may be earth bound. The system does not have to scale

sci.math: Re: [XPOST] A unique number for every "person" – can it be done?

- > *beyond earth, in case mankind can one day life on a planet other than*
- > *earth. But they may not be country bound. Countries come and go, they*
- > *join and separate and dissolve again.*
- >
- > 4) *The system must work without a central registry. Establishing a*
- > *registry and saying, every "person" gets a number when registering, that*
- > *is one higher than the last number, would work, but a central database*
- > *like system is required.*
- >
- > 5) *Once a person has a number, he can always recover it, in case it got*
- > *lost or forgotten, so the number creation is reproducible. An algorithm*
- > *working with the current time in ms since 1970 for example will*
- > *certainly add some randomness to the number and such making collisions*
- > *unlikely (in combination with other data), but you could not recover the*
- > *number again. This also means that all data for calculation must be*
- > *constant and can't change over the time.*
- >
- > 6) *The length of the number is not limited, but the shorter it is, the*
- > *better. However it may grow over the time; in thousand years having a*
- > *slightly bigger number would be acceptable.*
- >
- > 7) *You may use whatever data a "person" has available, but you may not*
- > *private data. If you tell someone your number, he should not be able to*
- > *gain any non-public knowledge about you through the number. If private*
- > *data is used, it must be one-way-hashed, so the original data is not*
- > *recoverable. On the other hand, the number should clearly show if it is*
- > *from an organization, from a company or from a real person.*
- >
- > 8) *Everyone must be able to calculate his/her number, without doing a*
- > *lot of research and it must be data everyone knows for sure (the exact*
- > *time of birth in ms does not qualify). On the other hand, people may be*
- > *forced to use a computer for doing that and have access to the Internet.*
- > *E.g. if you want to know the coordinates of their town of birth (using*
- > *whatever coordinate system you choice), this could be acceptable, as*
- > *there could be a search engine telling people the coordinates.*
- >
- >
- > *Be creative, try to find data useful for the purpose. Things you may*
- > *want to use:*
- >
- > *– Date of birth / Year of foundation*
- > *– Place of birth (consider not always known, names can change over time,*
- > *better go for coordinates)*
- > *– Name (First, Last / Name of company/organization)*
- > *– Name of parents (consider orphans / companies)*
- > *– Blood Type (consider companies have no blood type)*
- > *– Gender (consider companies)*
- > *– Eye color (should be constant, consider companies)*
- >
- > *and so on.*
- > *Just because some people may not know something or something may not*

Re: [XPOST] A unique number for every "person" – can it be done?

sci.math: Re: [XPOST] A unique number for every "person" – can it be done?

- > *apply to certain people doesn't mean you can not use it. But explain*
- > *what to do in the case it does not exist or is unknown.*
- >
- >
- > *I came up with plenty of ideas, but they were either too complicated or*
- > *creating collisions was too likely, that are not easily resolved.*
- >
- > *Simply writing down some data and hashing it creates a decent number,*
- > *but how long will this be collision free? How big must the hash be to be*
- > *secure for thousands of years and 6 billions of people and millions of*
- > *companies/organizations?*

Unless there is a limit on the number of objects to be numbered or no limit on the sizes of the numbers allowed, what you ask is impossible.

One method, using a finite number of characters, say  $n$ , greater than 1, as "digits" is to use one character as an end-of-number marker and the others to indicate an integer in base  $n-1$ . Or, if you use the space character as delimiter, just use ordinary integers base 10. The difficulty for computer use is that they will eventually get to have arbitrarily many digits, but that is inevitable unless there is some limit on the number of items to be tagged.