April 9, 2000

Authentication my way ...*

The **G**reenfield **A**uthentication **G**roup will authenticate documents and make me a multimillionaire. The foundation of my BUSINESS PLAN is an authenticating and compressing algorithm. The algorithm uses an easy technique to produce a number from a document. The public will not be able to reconstruct the information in the document, but the algorithm's output will be unique enough so that people will not be able to repudiate the document or forge another document in its place. I'll make a vast FORTUNE.

The GAG algorithm

Step 1 Discard any punctuation, any numbers, and any other characters which are not letters. Do, however, preserve spaces between words. Also, do *not* distinguish between lower and upper case (so "A" and "a" are considered the same letter).

Step 2 Count the number of vowels in the document (a vowel is one of the letters "a", "e", "i", "o" or "u"). Count the number of consonants in the document (a consonant here is any letter that's not a vowel). Count the number of spaces in the document. Note that a document *must* begin and end with a letter – spaces before the beginning and after the end don't count. Also, any succession of consecutive spaces will count as just one space.

Step 3 Multiply the number of vowels by 7, subtract 3 times the number of consonants, and add the *square* of the number of spaces. Find the mod 17 remainder of this number and output this number. This is the GAG number!

Example I'll apply the famous GAG algorithm to the following "document":

`I will pay Thomas $50 next Wednesday, or else $75 on the Friday following.`

Step 1 yields the following:

`i will pay thomas next wednesday or else on the friday following`

We count the vowels:

`i will pay thomas next wednesday or else on the friday following`

There seem to be 19 vowels.

`i_will_pay_thomas_next_wednesday_or_else_on_the_friday_following`

There are 11 spaces. Heroic further work enumerates 34 consonants. Now we compute

$$7(19) - 3(34) + (11)^2 = 133 - 102 + 121 = 152$$

but 152 mod 17 is 16: the GAG number of this document is **16**.

OVER

* Not recommended for the real world!

~~Homework~~ Some questions

Problem 1 Compute the GAG number of

`Good morning! I am here to help you. (He smiles and grabs the money.)`

Problem 2 Ted and I agree that

`We jointly and equally own the gravel pit at Loon Lake.`

but we've only published the GAG number of this document. It is known the document deals with the ownership of the Loon Lake gravel pit. First, compute the GAG number of this document. Then create a relevant document which will enable one of us to disavow the agreement published above. The document must have the same GAG number and deal with Loon Lake and its gravel pit, but it must assign ownership in some other manner. It should also be written in grammatical English! Show the details of your computations.

Some possible answers**

The algorithm creating the GAG number is not too good. It would assign the same GAG number to `frog jumping` and to `gorf jumping` and to `jumping frog`. There are lots of collisions using this algorithm! Also, the algorithm only has 17 possible outputs, so of *any* 18 "documents" at least 2 of them will have the same GAG number.

Here are a few answers I concocted to the problem above:

Example 1 `Ted owns the whole Loon Lake gravel pit and I own none of it.`

Example 2 `Ted has one third interest in the Loon Lake gravel pit.`

Example 3 `Ted has nineteen percent of the Loon Lake gravel pit.`

Example 4 `Ted owns none of the Loon Lake gravel pit. I own all the gravel pit.`

I recommend starting with some sentences and computing the GAG number of what you've written. Make small modifications until you get the "correct" GAG number, and until the sense of the document is what you want.

** with remarks on how I got them!