Enigma Nº 8 — Solución

La respuesta es QUEBRANTAHUESOS.

El texto se refiere al sistema de clave pública RSA. El artículo de una revista de ciencia donde se presentó un texto en clave usando este sistema poco después de que se creara es la columna "Mathematical Games" del número de agosto de 1977 de la revista *Scientific American*, por Martin Gardner. La clave usada se conoce como "RSA 129", y el texto en clave que no se encontró hasta 1993–94 es *"the magic words are squeamish ossifrage"*. Todas las referencias están en la página de la Wikipedia con este nombre.

Si buscamos información sobre RSA 129 podemos encontrar varias páginas que explican cómo decodificarlo, y por supuesto está explicado en el artículo original donde se decodificó. Se puede usar cualquier calculadora online para desencriptar usando RSA, o se puede programar en cualquier lenguaje de programación. El programa en Perl de la página siguiente es el que he usado para generar el enigma, y contiene también la forma de desencriptarlo. Usa el paquete `Math::BigInt`, que permite realizar operaciones con enteros grandes, necesaria para realizar las operaciones de exponenciación con exponentes grandes. Este programa da como salida *"la solucion a este enigma es quebrantahuesos"*, codificado asignando a cada letra dos dígitos, en orden con a=1, b=2,...

```
#!/usr/bin/perl

use v5.10;

use bigint;

# Usamos siempre las claves de RSA 129.

my $e = Math::BigInt->new("9007");

my $p = Math::BigInt->new('3490529510847650949147849619903898133417764638493387843990820577');
my $q = Math::BigInt->new('327691329932667095499619881908344613131776429679929425398798288533');
my $r = $p->copy()->bmul($q);

my $d = $e->copy()->bmodinv(($p-1)->bmul($q-1));


# "La solucion a este enigma es quebrantahuesos"
# ----------------------------------------------

my $texto = Math::BigInt->new('120100191512210309151400010005192'
.'005000514090713010005190017210502180114200108210519151 9');

my $cifrado = $texto->copy()->bmodpow($e, $r);

say "Cifrado:";
say $cifrado;

# Comprobacion
say "Descifrado:";
say $cifrado->copy()->bmodpow($d, $r);
```