2016 Puzzle

Cicada 3301 2016 Puzzle

Cicada's Twitter Account: https://twitter.com/1231507051321

Cicada twitter posted https://twitter.com/1231507051321/status/684596461628223488 which leads to

Important note: *What was believed to be a "dendrite" is actually an oak tree, as revealed by a Google search for "dead oak tree clipart".*
(http://www.clipartbest.com/cliparts/abc/y97/abcy97qTL.jpeg)

- Please note, the blocks in the background are noise from the image compression, not a QR code.
- The image size is 563 x 569 (both primes).

Run outguess:

```
-----BEGIN PGP SIGNED MESSAGE-----
Hash: SHA1

Hello.

The path lies empty; epiphany seeks the devoted.

Liber Primus is the way.  Its words are the map, their
meaning is the road, and their numbers are the direction.

Seek and you will be found.


Good luck.

3301


Beware false paths.  Verify OpenPGP 7A35090F.


-----BEGIN PGP SIGNATURE-----
Version: GnuPG v1

iQIcBAEBAgAGBQJWhcHDAAoJEBgfAeV6NQkP8GUP/iDXI/9lqvu/HTCujpPcIgYJ
H0Z8FdHDjz86A9yeyXYEUwPu1cLjSNUyGLBlu5dXuGpakuVeHtHnocuwrY24E2o4
Bnaqd1U8hUVU4Y68Va+jRIKS2NrPwg+HFFHr44DHKLHBM4CRqhLBFin36CeUIWmi
jykPMWwrLgxLy8FNXHvN/Fxqt0dbZ6/g1pxM2XOVEvy8bW/Xj7rj3VJGFOL7YVmM
Lae2PuCbmLZD/gaIhbGcPG7NEyUpFBbKEZ6Ul5i5LMeaRgS6KJHwLykeYdGWn65v
j8uY8+5zLBYus/OdbAZiiY6FnOgU/ESRQChQZILxiUIVT/OtFjz5IHrcVg3otoHl
tVfnSvqEk/AJ+w/MscTIBdxLPuvHmYD1B1XK/uZCRP/Dby6x8NFAR/zKAsqzkTY7
E4m34JzcPdsTnla0zmnz/O90jijfH+QAogyZSuEpdJIJlyFSzvDwhDme55gIAC0x
E1W7mxiOdss+Ebbmyyv4ul+l0UCB3qzfLw2Vijxmw/nWoDRqKk6kJf9vWL05BRu9
RoAap3rh0AC7SCV3fHjQj5VOUEJzHoz4YzrK15sa7SOZfeiP6XpfdzZfesiAWI8x
MUiyTFIqCeWZWJoSIe/1yFtumTkXO8/Dn0SCx9D4R6DVSiM9PRSdYgzT/+oRlIEl
Y8f7hrgdyn31uqGUgV4q
=sKXT
-----END PGP SIGNATURE-----
```

Likely only clue in message = 'numbers are the direction.' but this is still possible just 3301 way of speaking and not a clue.

If you verify the PGP key using GPG you get:

```
gpg: Signature made Thu 31 Dec 2015 07:01:07 PM EST using RSA key ID
7A35090F

gpg: Good signature from "Cicada 3301 (845145127)"

gpg: WARNING: This key is not certified with a trusted signature!

gpg:          There is no indication that the signature belongs to
the owner.
```

```
Primary key fingerprint: 6D85 4CD7 9333 22A6 01C3  286D 181F 01E5
7A35 090F
```

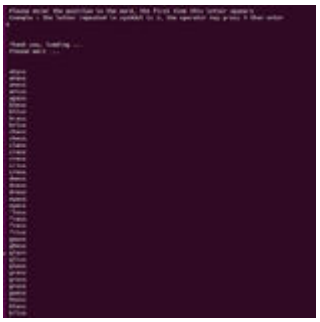
Bruteforce Software & Programs Section

Cicada_Breaker

This is a tool I programmed to find words with a repeated letter in a specific position, or even a sequence with different letters. **Note : You need Linux to run it. Setting up a bootable USB with Linux takes 10 minutes. Check this for instructions :**

☀http://www.ubuntu.com/download/desktop/create-a-usb-stick-on-windows

Tuto for Linux/Ubuntu/Backtrack ...



Launch a terminal from the same folder containing the program, write ./Prog then press enter if you want to use the 1-sequence mode, or ./Prog2 for the 2-sequence mode.

The more people on it the better results we get.

http://paf.im/H0rBI

```
 Update 1.0 :
This tool will allow you to find for example words like :
xxxSS, xxBBxxxx, xxxOUxxxx, xABxxxxx ...

You have to enter the length of the word,
the sequence you're looking for,
and its position in the word.

The tool will give you all the words with this combination.

For this beta version you can use only 360 000 words,
I will work on it in order to use the whole dictionnary.

Notice that it is very optimised, it will take no time.

Update 1.1 :
- Some bugs now are corrected
- Optimization ++
- 3 new modes
   1 : Fixed length / Fixed position
   2 : Free length / Fixed position
   3 : Fixed length / Free position
   4 : Free length / Free position

Update 1.2 :
- 2 new modes :
   5 : One character / Fixed position / Fixed length
   6 : One character / Fixed position / Free length

Update 1.3 :
- 8 new modes for 2 sequences

- You have many combines for the searched sequences based on
```

```
the length of the word containing the sequences (fixed and free),
the order of sequences (fixed = one before the other, free =
all possibilities for them) and their
position (Fixed seq_1 at position X and seq_2 at position Y).
PS : A Bruteforce code may come in the next updates
PPS : Next step the Bruteforce program
```

Infos :

The code starts being heavy, I have included the 2-sequence search option (with many modes like for the one sequence program) in a new program.

PS : You don't have to pay the guy for his program "DECPRYPTIONIST", since this one does the same thing, whatever ... (EDIT: decryptionist is much more powerful... anyway this is a quite ok free alternative)

Cicada_solver

EDIT : Instructions on how to help us with runes guessing and what we are looking for based on my conversation with Cicada_Solver and XDDD dude

For example : ᚳ ᛁ ᚱ ᚳ ᚢ ᛗ ᚠ ᛖ ᚱ ᛖ ᛏ ᚳ ᛖ - C I R C U M F E R E N C E - this 13 letter word was not encrypted at all (all it took is to look at the gematria and replace runes with letters) . There are only 4 words that long in the entire book :

ᛇᛈᛋᚢᛚ ᚠᛈᚢᚳᛖᚠᚹᛉ - (EO) P (S/Z) U L A P U (C/K) E F D X

ᛖᛞᚠᚹᛏᚠᛏᛖᛏᛉᚳᛏᛏ - E D A (AE) T O (EA)E (EA) X (C/K) (EA) T

ᛈᚳᛇᚢᛏᚳᚷᛇᛟᛏᚢᚺᚦ - P (C/K) (EO) U T (C/K) (IA/IO) (EO) (NG/ING) N U H (TH)

ᛒᛏᚠᛉᛁ ᛗᚢᚳᛈᚺᛟᛚᛇ - B (EA) F X I M U (C/K) P H (NG/ING) L (EO)

or

ᚳ ᛁ ᚱ ᚳ ᚢ ᛗ ᚠ ᛖ ᚱ ᛖ ᛏ ᚳ ᛖ ᛋ - C I R C U M F E R E N C E S - this 14 letter word was also not encrypted . There are 3 more words that long in the book :

ᛒᚷᛞᛉᛗᛒᛉᚳᛟᚦᚣᛞᚠᛏ - B G D X M B X (C/K) (NG/ING) (TH) Y D (AE) (EA)

ᛉᛁ ᛝᚦᛟᚾᛖᛏᚠᚹᛗᛖᚣᚠ - (EA) I (IA/IO) (TH) (NG/ING) N E N F O M E Y A

ᛏᚠᚾ ᚱᚹᚠᛋᛏᚹᚾ ᛖᛒᚢᚦ - T F J R W F S N W J E B U (TH)

The explanation from Cicada_Solver : Let's take the word "CIRCUMFERENCES". If we assume the word repeats itself in the book and you think that after encryption it gives ᛏᚠᚾ ᚱᚹᚠᛋᛏᚹᚾ ᛖᛒᚢᚦ - T F J R W F S N W J E B U (TH) then you have to guess which

opetations have been applied on the word ᚴ ᛁ ᚱ ᚴ ᚢ ᛗ ᚠ ᛖ ᚱ ᛖ ᚾ ᚴ ᛖ ᛋ (CIRCUMFERENCES) with the gematria to have the result ᛏ ᚠ ᚱ ᚠ ᛋ ᚾ ᚹ ᚾ ᚠ ᛊ ᚾ ᚹ ᛇ ᛒ ᚢ ᚦ (T F J R W F S N W J E B U (TH))

When you have an idea try it on other words and correct your guess since you can verify the other possibilities (if you detect a rune, then use cicada_breaker to guess the others one by one and remember each rune reduce the possibilities from n! to (n-1)!).

If everyone try this, by the end we would have lots of runes guessed (wrong and maybe right) but it is the same operation so we all think about the results and a dozen of minds are much better than one for this task. By comparing the results we can be sure about some runes.

Don't forget that an operation should be bijective and should be able to be reversed otherwise the operation of encryption/decryption could not be executed, so Cicada has necessarily used bijections to encrypt Liber Primus.

And when we have some runes guessed we can launch the bruteforce program.

Anybody that wishes to help - please download the software and try this method . The more people on it the more info for bruteforcing.

I have 29! possibilities which is about 8.841762*10^30 permutations, if we suppose that there is no other operations added on the other pages, this is just not possible to calculate even with super calculators I've got in labs (in which case it would take years before having the solution). It is a factorial-complexity so it is O(n!) for 2X variables we need 1000 years to find. (For n = 20 it takes about 800 years)

In mechanical engineering, we deal with problems like this one since the inversion of a matrix needs the calculation of determinants and the law looks like this one O(n!), we transform the system to another form having a polynomial-complexity O(n^p) then we have our solution in no time.

The Liber Primus problem is easier cuz we have words and sequences (this is its Achilles' hell), which can be guessed cuz they are comprehensible not like numbers and results of a calculation for determinant (In CFD and FEM the dimensions of the problem give us n = 10^9 easily ... so it is 10^9! operations).

I maybe repeate what I've said, but it is important to guess runes with the cicada_breaker V1 I gave you, it would reduce the possibilities to 2.092279*10^13 possibilities and this is rational to bruteforce in labs.

When I said statistical studies and probabilities, you have to take the decrypted pages, take the words reapeated and look for them in the other pages since lenght is known. What you should do is to take long words, write them in runes and copare them with long words from Liber Primus, if you figure out about the permutations applicated on the word, each time you reduce the possibilities from n! to (n-1)! and so on, and this is why I said that is ok if the runes are wrong, the

calculation doesn't take time and the worst thing that could happen is having a wrong text. By the end we eliminate the "lenght-of-the-word" possibilities, and since the word is a finite space we can try all the other possibilities by hand.

The only solution to bruteforce is to cut the gematria table to 1X - 1Y permutations, 1X to guess and 1Y to bruteforce.

Guys this is a mathematical problem, we should deal with it with maths if you don't find the key fixed by cicada.

I cannot be more clear than this time.

PS : Do not forget, I assumed that there is only one opperation applied on every rune.

Dr B 67

****

what if they knew that whoever would decode this would have dyslexia, and so Liber Primus would automatically be decoded in their head as Libra Primary (as in the constellation Libra) libra is the scales so "liber primus is the way" would only mean [balances is the way] as for "beware false paths" Scorpions are a symbol of treachery, but libra is the symbol of justice idk... but some key words would be (balance,scorpion,claw) and key numbers would be 2.6/ 2.7/ 3.9/ 4.5/ 4.9/ 5.2/ 5.7/ 5.9/ 6.1/ 6.5/ 9.4 only got this much out of 30min OCD but you might be able to do something with it, but beware i got no clue so...yeh

if balance is the key, and this Libra is the way then during the equinox where day and night are equal follow where the Libra constellation is pointing.

~Punqi

****

Python Program for Solving Runes:

A collaborative effort to get as many different cyphers put into the program: https://github.com/Be5haram/CICADA2K16/blob/master/RuneSolver.py

---

Important notice for Primus solvers

UPDATE: Two members of our community are currently working on decryption tools (one - a dictionary word search, the other - a Vigenere solver)

Pages 28 to 32 Discoveries and Decryptions

Page 28

Characters have been translated from Runic to Latin on page 28:

(Lines here correspond to lines on the page)

[http://pastebin.com/NqF7M1Xn]

Anyone who has ideas about these words, please leave your thoughts in the comment section. Please understand, that after #, the coding system changes (# = 13 red dots).

EDIT: If you would like to use a word-searching software, please, help yourself

[http://www.thewordfinder.com/classicscrabble.php]

-4CID.

Actually this software is way better imho so I'm putting this one up as well :

http://www.bestwordlist.com/indexbeginning.htm

-Dr B 67

- -

EDIT: Thank you, <jacquerie> for pointing that pages were already transliterated. Please follow this link:
[https://titanpad.com/vFCy7T5p0O]

Some interesting facts about the number 15:

- The number of chapters in the book (whereas for "chapter" I mean a paragraph with a big red starting rune) is exactly 15.
- From page 41 to page 56 you can see some kind of "plants" at the left and right edges of the page. The right side plant, near the center, has 5 dots. The left side one, however, has only 3 (two of them being removed. It's easy to see if you zoom in). 3 and 5 are the prime factors of 15.

Pages 8-14 straws/saplings meanings & Discoveries

Fibonacci Tree reference

The saplings from page 8 and on represent the Fibonacci tree. The top of the sapling has exactly 13 branches, which is the number you'd expect from a Fibonacci tree like the one on the right. To find more: http://oeis.org/A000045/a000045.html

So the highlighted branches are: 2-3-5-6-8-10-11-13. Anything up with this? Branch 2 and branch 5 make me think of runes somehow.