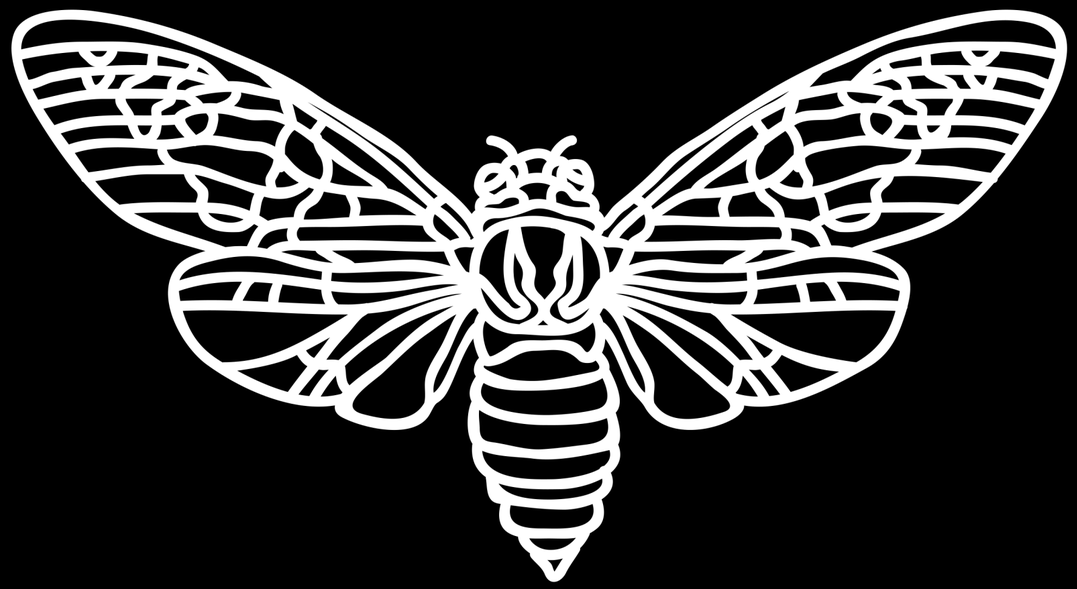
Cicada 3301

The Mystery

@iBotPeaches



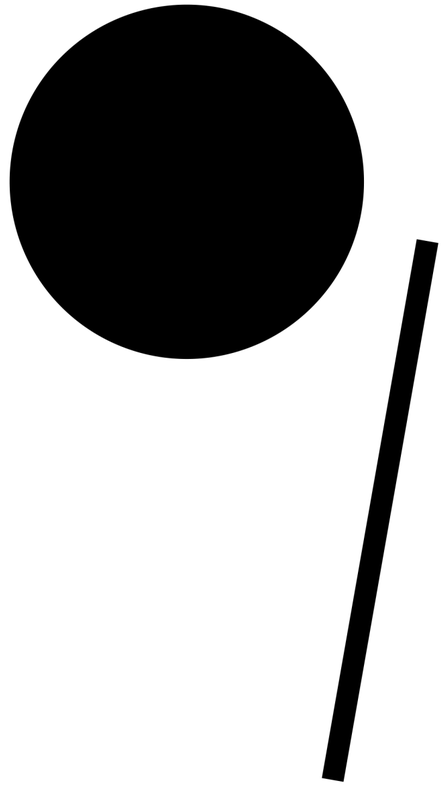
Story Time

- Cicada 3301
- 3 Puzzles
- Worldwide Hunt
- Largely Unknown
- Scary

Who

- Connor Tumbleson
- @iBotPeaches

Lets turn the clocks back



Jan 5, 2012

4chan.org

- Weird part of the Internet
- "*hidden in this image*"

Hello. We are looking for highly intelligent individuals. To find them, we have devised a test.

There is a message hidden in this image.

Find it, and it will lead you on the road to finding us. We look forward to meeting the few that will make it all the way through.

Good luck.

3301

Puzzle 1 - Hex Editor

```
51 45 14 00 51 45 14 00 | 51 45 14 00 51 45 14 00   QE..QE..QE..QE..
51 45 14 00 51 45 14 00 | 51 45 14 00 51 45 14 00   QE..QE..QE..QE..
51 45 14 00 51 45 14 00 | 51 45 14 00 51 45 14 00   QE..QE..QE..QE..
51 45 14 00 51 45 14 00 | 51 45 14 00 51 45 14 00   QE..QE..QE..QE..
51 45 14 00 51 45 14 00 | 51 45 14 00 51 45 14 00   QE..QE..QE..QE..
51 45 14 00 51 45 14 00 | 51 45 14 00 51 45 14 00   QE..QE..QE..QE..
51 45 14 00 51 45 14 00 | 51 45 14 00 51 45 14 00   QE..QE..QE..QE..
51 45 14 00 51 45 14 00 | 51 45 14 00 51 45 14 00   QE..QE..QE..QE..
51 45 14 00 51 45 14 00 | 51 45 14 01 51 45 14 01   QE..QE..QE..QE..
FF D9 54 49 42 45 52 49 | 56 53 20 43 4C 41 56 44    ┘TIBERIVS CLAVD
49 56 53 20 43 41 45 53 | 41 52 20 73 61 79 73 20   IVS CAESAR says 
22 6C 78 78 74 3E 33 33 | 6D 32 6D 71 6B 79 76 32   "lxxt>33m2mqkyv2
67 73 71 33 71 3D 77 5D | 4F 32 6E 74 6B 22 0A +    gsq3q=w]O2ntk".
```

Puzzle 1 - Hex Editor

```
51 45 14 00 51 45 14 00 | 51 45 14 00 51 45 14 00   QE..QE..QE..QE..
51 45 14 00 51 45 14 00 | 51 45 14 00 51 45 14 00   QE..QE..QE..QE..
51 45 14 00 51 45 14 00 | 51 45 14 00 51 45 14 00   QE..QE..QE..QE..
51 45 14 00 51 45 14 00 | 51 45 14 00 51 45 14 00   QE..QE..QE..QE..
51 45 14 00 51 45 14 00 | 51 45 14 00 51 45 14 00   QE..QE..QE..QE..
51 45 14 00 51 45 14 00 | 51 45 14 00 51 45 14 00   QE..QE..QE..QE..
51 45 14 00 51 45 14 00 | 51 45 14 00 51 45 14 00   QE..QE..QE..QE..
51 45 14 00 51 45 14 00 | 51 45 14 00 51 45 14 00   QE..QE..QE..QE..
51 45 14 00 51 45 14 00 | 51 45 14 00 51 45 14 01   QE..QE..QE..QE..
FF D9 54 49 42 45 52 49 | 56 53 20 43 4C 41 56 44    ┘TIBERIVS CLAVD
49 56 53 20 43 41 45 53 | 41 52 20 73 61 79 73 20   IVS CAESAR says
22 6C 78 78 74 3E 33 33 | 6D 32 6D 71 6B 79 76 32   "lxxt>33m2mqkyv2
67 73 71 33 71 3D 77 5D | 4F 32 6E 74 6B 22 0A +    gsq3q=w]O2ntk".
```

Puzzle 1 - Caesar Cipher

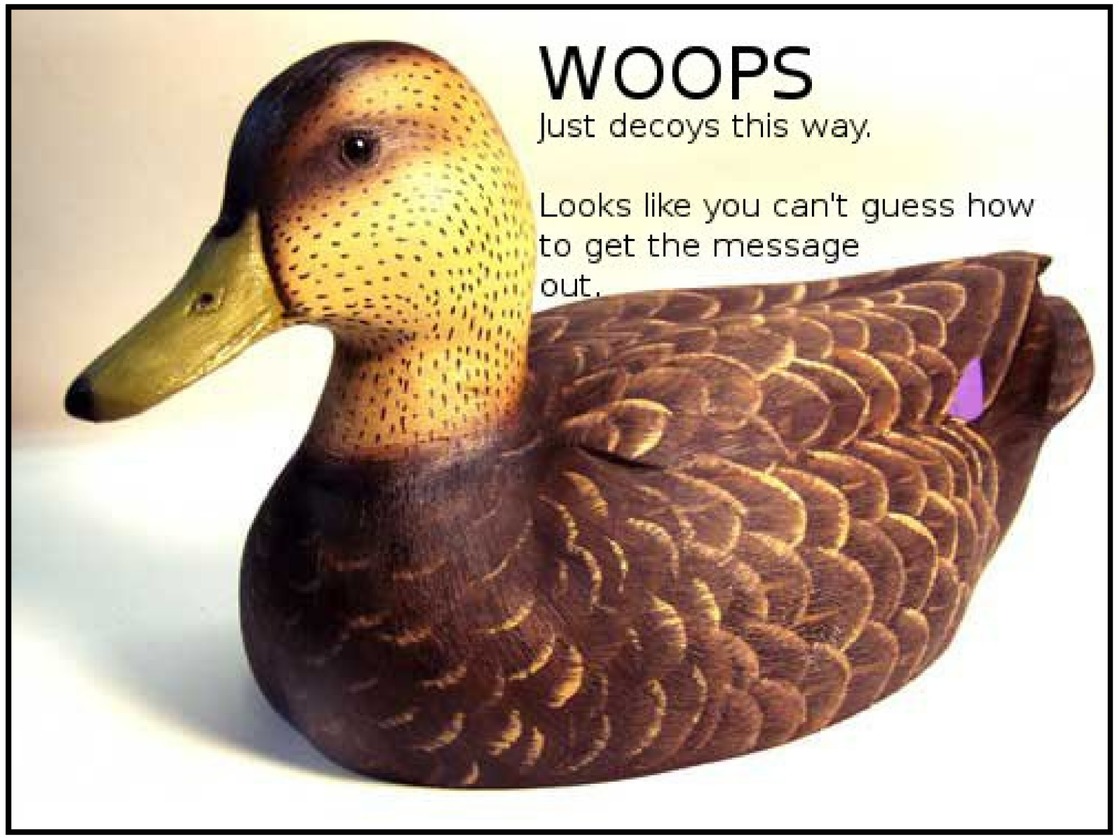
- *lxxt> 33m2mqkyv2gsq3q = w] O2ntk*
- ROT0 - ROT26 - “rotates” text

Puzzle 1 - Caesar Cipher

- *lxxt> 33m2mqkyv2gsq3q = w] O2ntk*
- ROT0 - ROT26 - “rotates” text
- **+4 - http:{//i.imgur.com/m{9{sY{K.jpg**

The Decoy

- Decoy Image
- *“can’t guess how”*
- *“to get image out”*



Niels Provos

OutGuess is a universal steganographic tool that allows the insertion of hidden information into the redundant bits of data sources.

Outguess

```
→ cicada outguess -r 3301orig2012cesarincluded.jpg out2.txt
Reading 3301orig2012cesarincluded.jpg....
Extracting usable bits:   29049 bits
Steg retrieve: seed: 228, len: 535
→ cicada cat out2.txt
Here is a book code.  To find the book, and more information, go to http://www.reddit.com/r/a2e7j6ic78h0j/

1:20
2:3
3:5
4:20
5:5
6:53
```

Outguess

```
→ cicada outguess -r 3301orig2012cesarincluded.jpg out2.txt
Reading 3301orig2012cesarincluded.jpg....
Extracting usable bits:   29049 bits
Steg retrieve: seed: 228, len: 535
→ cicada cat out2.txt
Here is a book code.  To find the book, and more information, go to http://www.reddit.com/r/a2e7j6ic78h0j/

1:20
2:3
3:5
4:20
5:5
6:53
```

1 10 Valēte! (i.imgur.com)
submitted 7 years ago by CageThrottleUs
1 comment share save hide report

2 2 djsl aoltlz? Nhta snwe uawg I nqbl mu ltlm, khta hzcn fhpwlnuh hvz (self.a2e7j6ic78h0j)
submitted 7 years ago by CageThrottleUs
comment share save hide report

3 2 djs ctrdqf, igpkvouvbag ng axf ghrofs, 'Vp, Bnbnvl, kant ics ltcbznl (self.a2e7j6ic78h0j)
submitted 7 years ago by CageThrottleUs
1 comment share save hide report

4 2 gkho eokflvznz ac lvx oisfs, vq, o tnxegyqeg ovwus pns igabf hokumso (self.a2e7j6ic78h0j)
submitted 7 years ago by CageThrottleUs
1 comment share save hide report

5 2 osihe zg foik, ebavwf urfpte yt gpgiw. Mul nhxu W ool zotv crcftxj (self.a2e7j6ic78h0j)
submitted 7 years ago by CageThrottleUs
comment share save hide report

6 2 ercu mnw fymv, agk gsbz. Nne vrenm, Rto, A zldvr alojr tay nglyfm (self.a2e7j6ic78h0j)
submitted 7 years ago by CageThrottleUs
comment share save hide report

7 1 djsu mnw erg sevhaw qeras, cnn ywaa zzma, jvhhsr lvx oisfs vkuomkv (self.a2e7j6ic78h0j)
submitted 7 years ago by CageThrottleUs
comment share save hide report

8 1 Gjsu B rgarmu og avw hkre ujebg khl tgf h aznzss dsts uqqn sv, ouw (self.a2e7j6ic78h0j)
submitted 7 years ago by CageThrottleUs
comment share save hide report

9 1 erdlk vsda ww im vjwf fl oxp hocr. Hgj ltba Z wbavkhhbd uje cjcdxx. (self.a2e7j6ic78h0j)
submitted 7 years ago by CageThrottleUs
comment share save hide report

10 1 bgojakv fom sogl. W likaee oy rqfzx'y xxhvb thdojrl ghf uhyysy, ttv (self.a2e7j6ic78h0j)
submitted 7 years ago by CageThrottleUs
comment share save hide report

11 2 mcb lgjmdl byam zvgkxe aof lsxs. Mhx faa wee hm hzclr hbklcvcuxy (self.a2e7j6ic78h0j)
submitted 7 years ago by CageThrottleUs
comment share save hide report

a2e7j6ic78h0j

join 1,341 readers

6 users here now

a2e7j6ic78h0j7eiejd0120

Verify: 7A35090F

created by CageThrottleUs a community for 7 years

MODERATORS message the moderators

Pixelated_Fudge

about moderation team »

The Subreddit

- 2 images
- Many lines of gibberish

Rotation Cipher?

ROT-0: Ukbn Txltbz nal hh Uoxelmgox wdvg Akw; hvu ogl rsm ar sbv ix jwz
ROT-1: Vlco Uymuca obm ii Vpyfmnhpy xewh Blx; iwv phm stn bs tcw jy kxa
ROT-2: Wmdp Vznvdb pcn jj Wqzgnoiqz yfxi Cmy; jxw qin tuo ct udx kz lyb
ROT-3: Xneq Waowec qdo kk Xrahopjra zgyj Dnz; kyx rjo uvp du vey la mzc
ROT-4: Yofr Xbpxfd rep ll Ysbipqksb ahzk Eoa; lzy skp vwq ev wfz mb nad
ROT-5: Zpgs Ycqyge sfq mm Ztcjqrltc bial Fpb; maz tlq wxr fw xga nc obe
ROT-6: Aqht Zdrzhf tgr nn Audkrsmud cjbm Gqc; nba umr xys gx yhb od pcf
ROT-7: Briu Aesaig uhs oo Bvelstnve dkcn Hrd; ocb vns yzt hy zic pe qdg
ROT-8: Csjv Bftbjh vit pp Cwfmtuowf eldo Ise; pdc wot zau iz ajd qf reh
ROT-9: Dtkw Cgucki wju qq Dxgnuvpxg fmep Jtf; qed xpu abv ja bke rg sfi
ROT-10: Eulx Dhvdlj xkv rr Eyhovwqyh gnfq Kug; rfe yqv bcw kb clf sh tgj

Rotation Cipher?

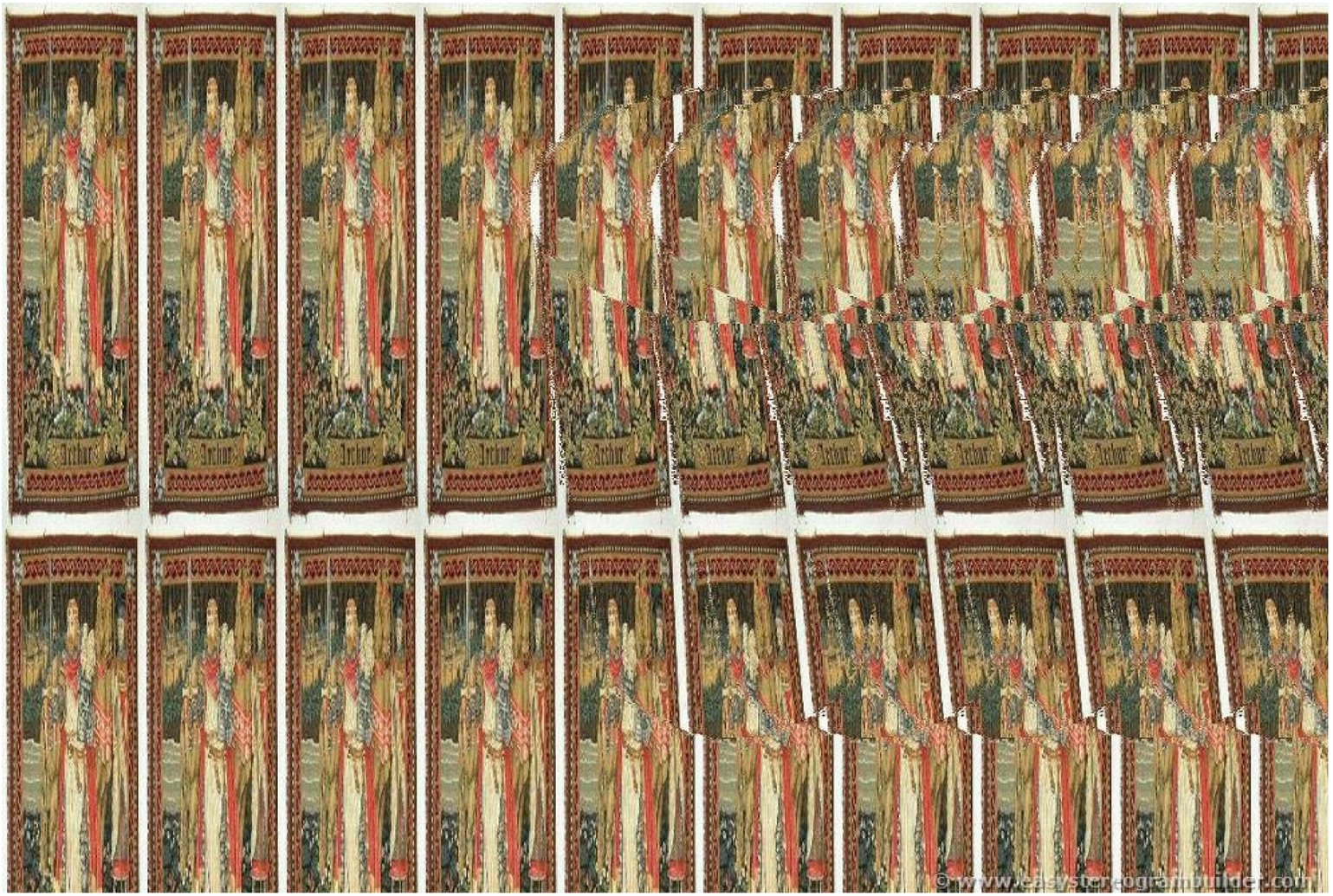
ROT-11: Fvmy Eiwemk ylw ss Fzipwxrzi hogr Lvh; sgf zrw cdx lc dmg ti uhk
ROT-12: Gwnz Fjxfnl zmx tt Gajqxysaj iphs Mwi; thg asx dey md enh uj vil
ROT-13: Hxoa Gkygom any uu Hbkryztbk jqit Nxj; uih bty efz ne foi vk wjm
ROT-14: Iypb Hlzhpn boz vv Iclszaucl krju Oyk; vji cuz fga of gpj wl xkn
ROT-15: Jzqc Imaiqo cpa ww Jdmtabvdm lskv Pzl; wkj dva ghb pg hqk xm ylo
ROT-16: Kard Jnbjrp dqb xx Kenubcwen mtlw Qam; xlk ewb hic qh irl yn zmp
ROT-17: Lbse Kocksq erc yy Lfovcdxfo numx Rbn; yml fxc ijd ri jsm zo anq
ROT-18: Mctf Lpdltr fsd zz Mgpwdeygp ovny Sco; znm gyd jke sj ktn ap bor
ROT-19: Ndug Mqemus gte aa Nhqxefzhq pwoz Tdp; aon hze klf tk luo bq cps
ROT-20: Oevh Nrfnvt huf bb Oiryfgair qxpa Ueq; bpo iaf lmg ul mvp cr dqt

Rotation Cipher?

ROT-21: Pfwi Osgowu ivg cc Pjszghbjs ryqb Vfr; cqp jbg mnh vm nwq ds eru
ROT-22: Qgxj Pthpxv jwh dd Qktahickt szrc Wgs; drq kch noi wn oxr et fsv
ROT-23: Rhyk Quiqyw kxi ee Rlubijdlu tasd Xht; esr ldi opj xo pys fu gtw
ROT-24: Sizl Rvjrzx lyj ff Smvcjkemv ubte Yiu; fts mej pqk yp qzt gv hux
ROT-25: Tjam Swksay mzk gg Tnwdklfnw vcuf Zjv; gut nfk qrl zq rau hw ivy

Image 1

Image 2



Outguess

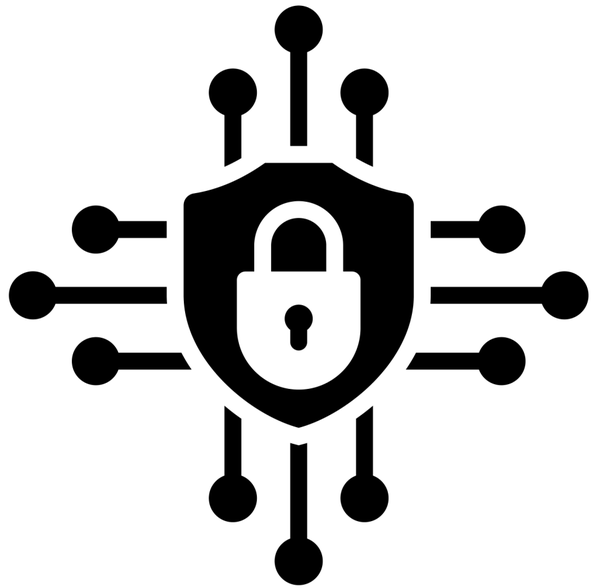
```
-----BEGIN PGP SIGNED MESSAGE-----
Hash: SHA1

- From here on out, we will cryptographically sign all messages with this key.

It is available on the mit keyservers.  Key ID 7A35090F, as posted in a2e7j6ic78h0j.

Patience is a virtue.

Good luck.

3301
-----BEGIN PGP SIGNATURE-----
Version: GnuPG v1.4.11 (GNU/Linux)

iQIcBAEBAgAGBQJPBRz7AAoJEBgfAeV6NQkP1UIQALFcO8DyZkecTK5pAIcGez7k
```

Outguess

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

- From here on out, we will cryptographically sign all messages with this key.

It is available on the mit keyservers.  Key ID 7A35090F, as posted in a2e7j6ic78h0j.

Patience is a virtue.

Good luck.

3301
-----BEGIN PGP SIGNATURE-----
Version: GnuPG v1.4.11 (GNU/Linux)

iQIcBAEBAgAGBQJPBRz7AAoJEBgfAeV6NQkP1UIQALFcO8DyZkecTK5pAIcGez7k
```

GPG / PGP

- Integrity
- Confidentiality
- Signing



```
gpgv: Signature made Thu Jan  5 03:46:03 2012 UTC
gpgv: using RSA key 181F01E57A35090F
gpgv: Good signature from "Cicada 3301 (845145127)"
```

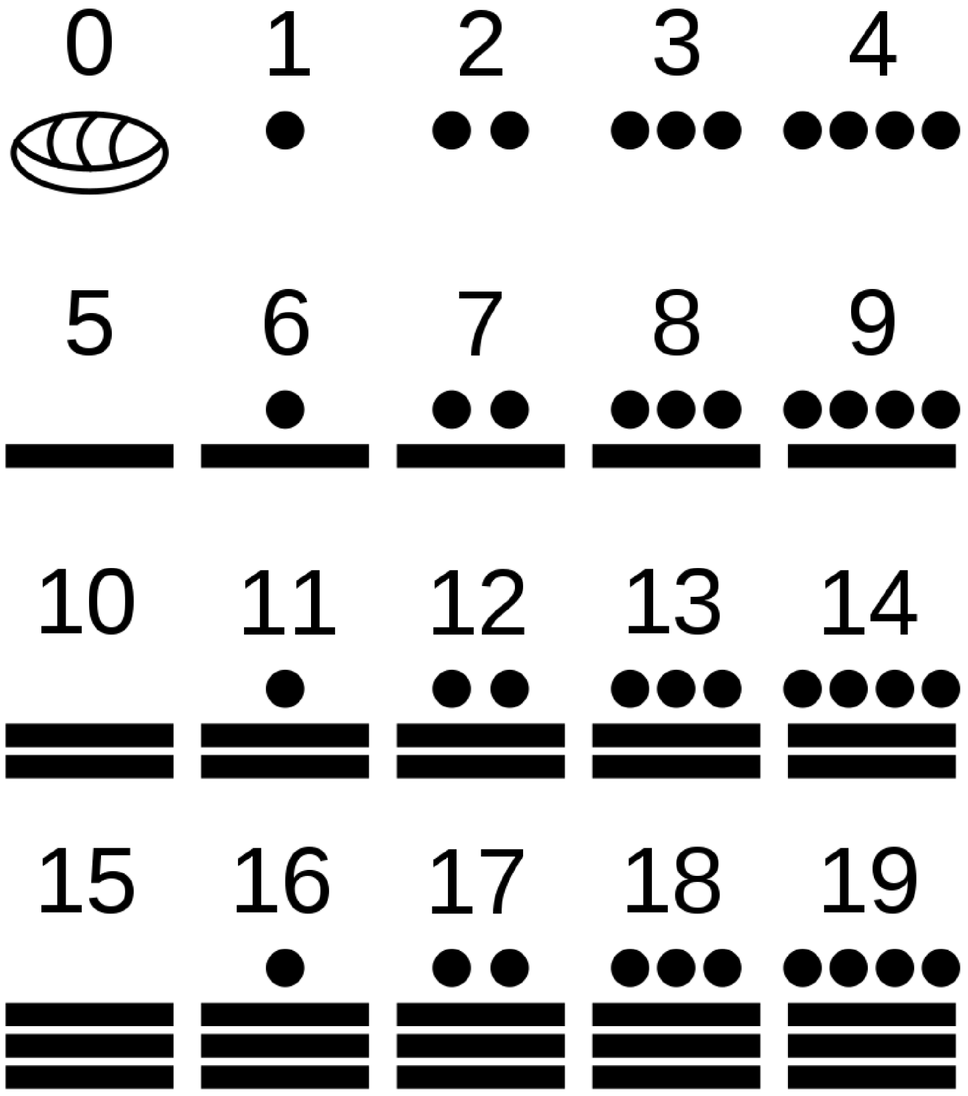
Outguess

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

The key has always been right in front of your eyes.

This isn't the quest for the Holy Grail.  Stop making
it more difficult than it is.

Good luck.

3301
-----BEGIN PGP SIGNATURE-----
Version: GnuPG v1.4.11 (GNU/Linux)
```

Reddit Header

Mayan Numerals

- Base 20
- Zero (shell)
- One (dot)
- Five (bar)



Reddit Sidebar

a2e7j6ic78h0j

join 1,352 readers

4 users here now

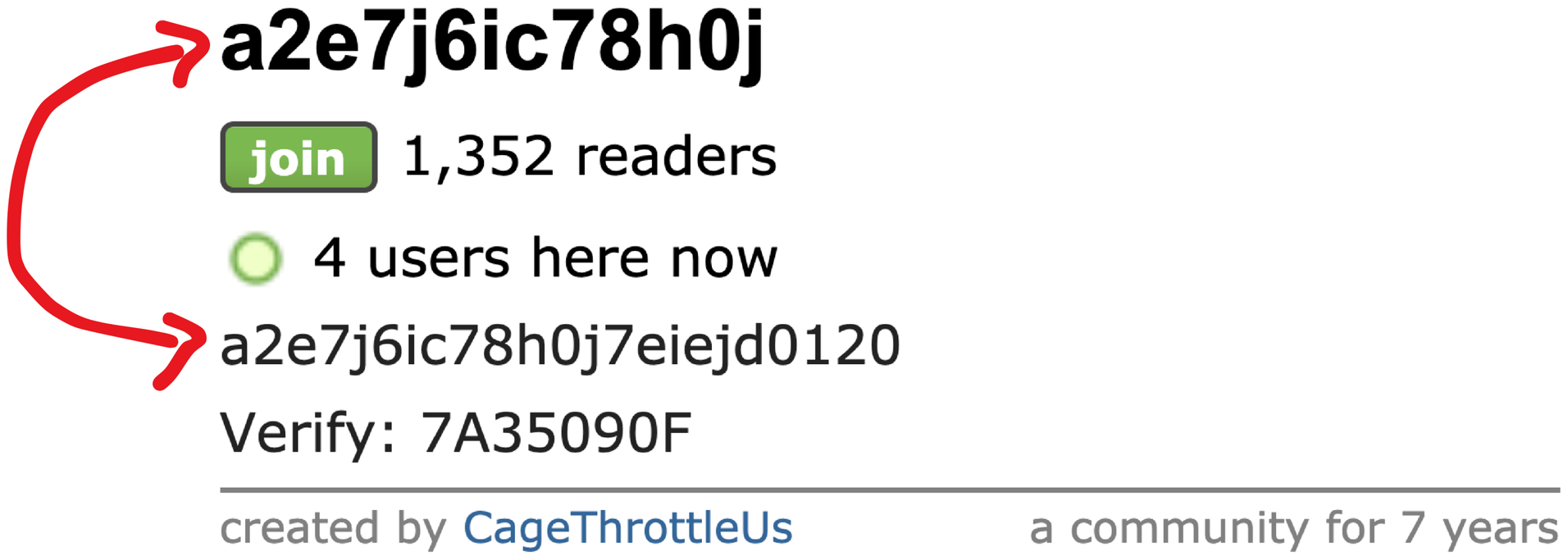
a2e7j6ic78h0j7eiejd0120

Verify: 7A35090F

---

created by CageThrottleUs a community for 7 years

Reddit Sidebar



Letters to Numbers

a

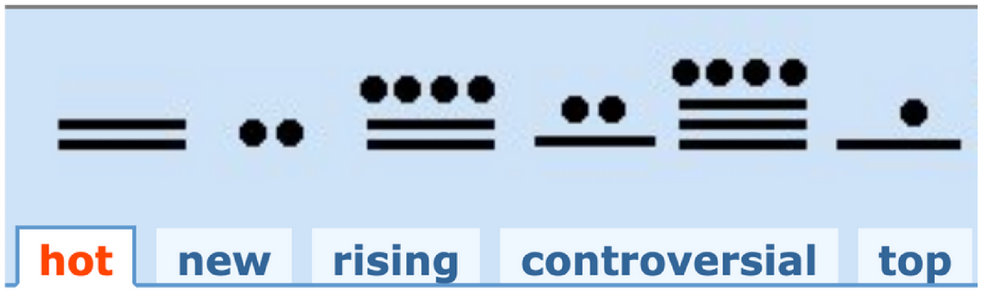
2

e

7

j

6



Letters to Numbers

a

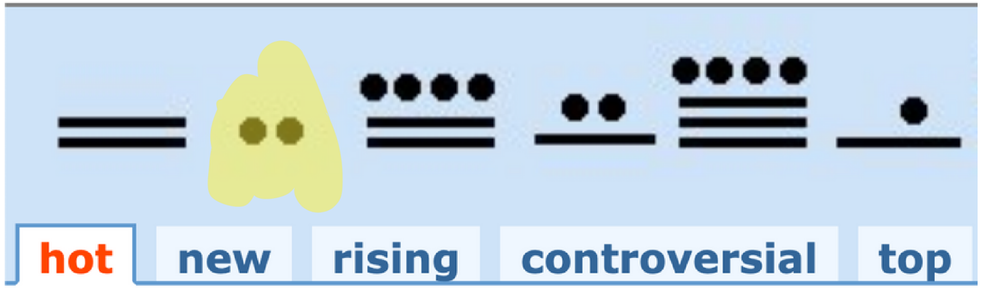
2

e

7

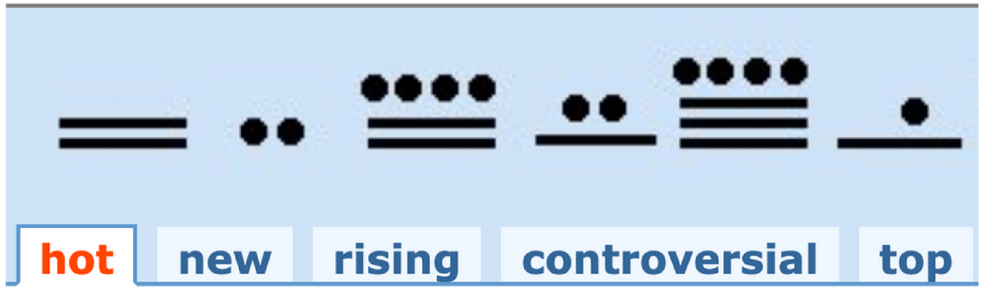
j

6



Letters to Numbers

a 2 e 7 j 6



10 2 14 7 19 6

The Number

10 2 14 7 19 6 18 12 7 8 17 0 19

7 14 18 14 19 13 0 1 2 0

The book?

djsl aoltlz? Nhta snwe uawg I nqbl mu ltlm, khta hzcn fhpwlnuh hvz

10 2 14 7 19 6 18 12 7 8 17 0 19

7 14 18 14 19 13 0 1 2 0

The book?

djsl aoltlz?

10 2 14 7 19 6 18 12 7 8

Vigenere Cipher

- d shift 10
- j shift 2
- s shift 14
- l shift 7

- a shift 19
- o shift 6
- l shift 18
- t shift 12
- l shift 7
- z shift 8

Vigenere Cipher

- d shift 10 t
- j shift 2 h
- s shift 14 e
- l shift 7 e
- a shift 19 h
- o shift 6 i
- l shift 18 t
- t shift 12 h
- l shift 7 e
- z shift 8 r

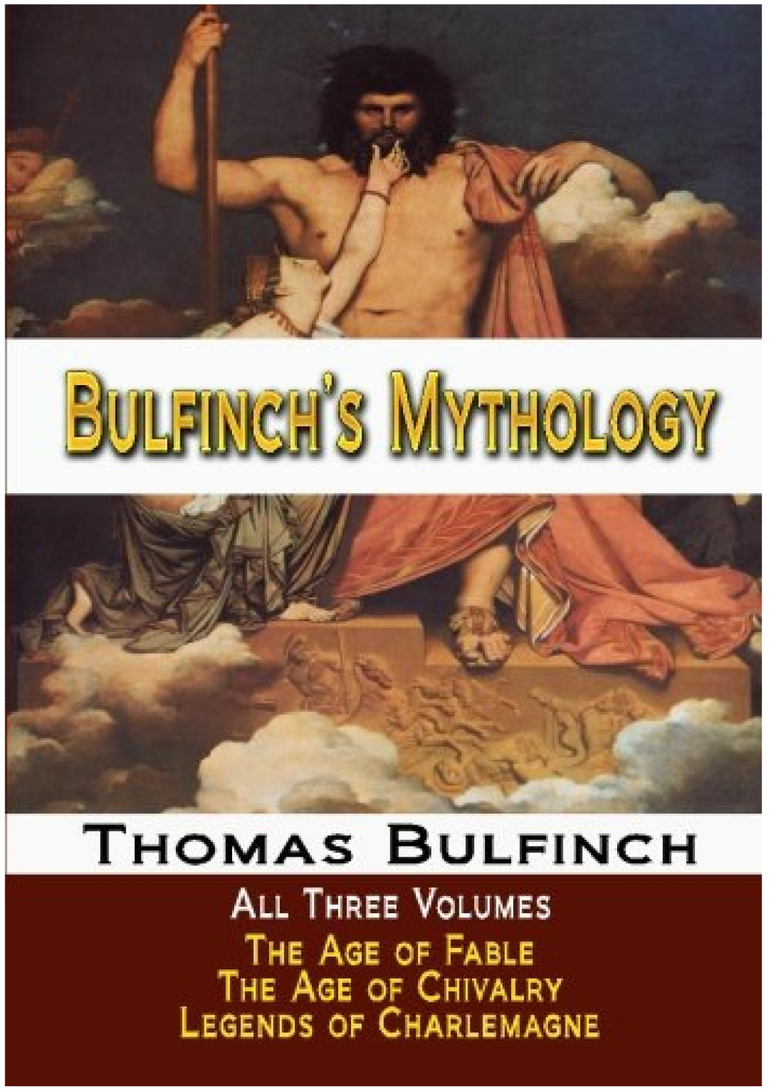
The book

thee hither? What evil have I done to thee, that thou shouldst act

the valley, approaching me and saying, 'Oh, Knight, what has brought

The book

- Story about King Arthur
- Book code!



The message

Call us at us tele phone numBer

two one four three nine oh nine six oh eight

The Call - (214) 390-9608

The Call Transcript

*Very good. You have done well. There are **three** prime numbers associated with the original final.jpg image.*
***3301** is one of them.*
*You will have to **find** the other two. Multiply all three of these numbers together and add a .com to find the next step.*
Good luck. Goodbye.

Find the Primes

- Original image

Find the Primes

- Original image
- **509**px by **503**px
- **3301** x **509** x **503**

845145127.com

Find our symbol at the location nearest you:

52.216802,	21.018334
48.85057059876962,	2.406892329454422
48.85030144151387,	2.407538741827011
47.664196,	-122.313301
47.637520,	-122.346277
47.622993,	-122.312576
37.577070,	126.813122

Locations


Greenland
Iceland
Finland
Sweden
Norway
Russia
United Kingdom
Poland
Germany
Ukraine
France
Spain
Italy
Kazakhstan
Mongolia
Türkiye
China
South Korea
Japan
Iraq
Iran
Afghanistan
Pakistan
Algeria
Libya
Egypt
Saudi Arabia
India
Thailand
Mali
Niger
Sudan
Chad
Nigeria
Ethiopia
DRC
Kenya
Tanzania
Angola
Namibia
Botswana
Madagascar
South Africa
Indonesia
Papua New Guinea
Australia
New Zealand
North Atlantic Ocean
South Atlantic Ocean
Indian Ocean
Southern Ocean
North Pacific Ocean
South Pacific Ocean
Canada
United States
Mexico
Venezuela
Colombia
Peru
Brazil
Bolivia
Chile
Argentina

Locations

- Australia
- France
- South Korea
- Poland
- California
- Arkansas
- Hawaii
- Florida
- Louisiana
- Washington

Warsaw, Poland

- Cicada Symbol
- QR code

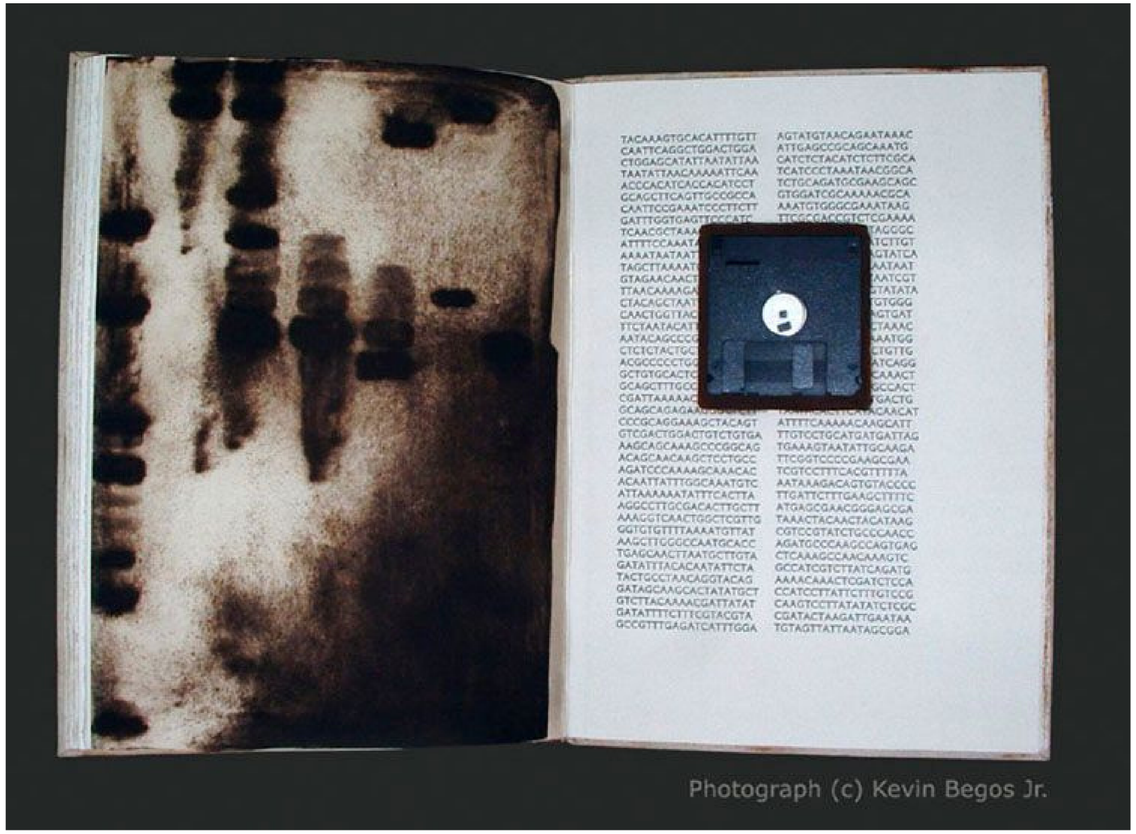
The Posters

Outguess

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

A poem of fading death, named for a king
Meant to be read only once and vanish
Alas, it could not remain unseen.

1:5
152:24
the product of the first two primes
14:13
7:36
12:10
7:16
24:3
```

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

In twenty-nine volumes, knowledge was once contained.
How many lines of the code remained when the Mabinogion paused?
Go that far in from the beginning and find my first name.

1:29
6:46
the product of the first two primes
2:37
14:41
17:3
27:40
the first prime
2:33
1:1
```

The books

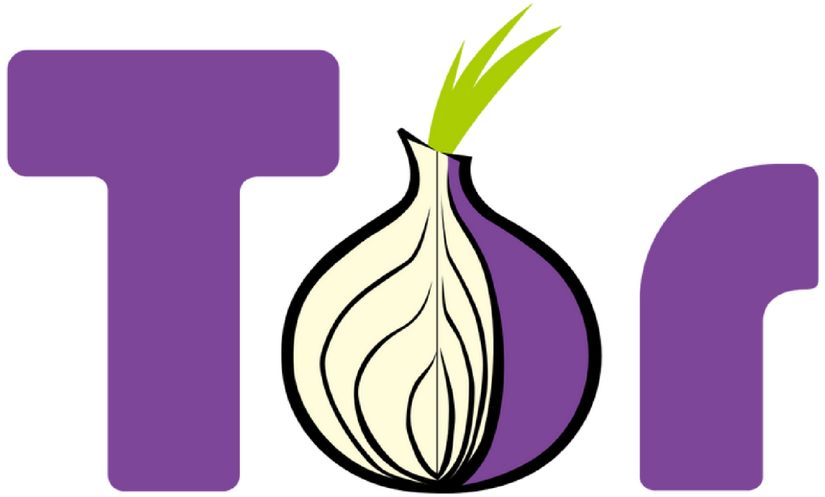


Agrippa

Encyclopaedia Britannica

An Onion

sq6wmgv2zcsrix6t.onion



The Onion

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

Congratulations!

Please create a new email address with a public, free, web-based service.
Once you've never used before, and enter it below.  We recommend you do
this while still using Tor, for anonymity.

We will email you a number in the next few days (in the order in which
you've arrived to this page).  Once you've received it, come back to this
site and append a slash and then the number you received to this url.
(For example, if you received "3894894230934209", then you would go to
"http://sq6wmgv2zcsrix6t.onion/3894894230934209")

3301
-----BEGIN PGP SIGNATURE-----
```

The Onion

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

Congratulations!

Please create a new email address with a public, free, web-based service. Once you've never used before, and enter it below. We recommend you do this while still using Tor, for anonymity.

We will email you a number in the next few days (in the order in which you've arrived to this page). Once you've received it, come back to this site and append a slash and then the number you received to this url. (For example, if you received "3894894230934209", then you would go to "http://sq6wmgv2zcsrix6t.onion/3894894230934209")

3301
-----BEGIN PGP SIGNATURE-----

The Number/Email

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


This message will only be displayed once.

Here is a message that has been encrypted with RSA (the Crypt::RSA Perl module available in CPAN) :

- -----BEGIN COMPRESSED RSA ENCRYPTED MESSAGE-----
Version: 1.99
Scheme: Crypt::RSA::ES::OAEP

eJwBzQAy/zEwADE4OABDeXBoZXJ0ZXh0Ca4y//uzl/HvFoP9Klf53nEFH0T4c+ui5de8+vqGOnZc
9DlrsWQe+xxVaPaYgKAD9Wn9VWQ6A5o254r5pa4hkDIY5RRmVfqOm88HJpGdbGGTckyEwJapCLDT
tHzZWAZ0FIVj6fH2whErHoVmZ82zQJ64OLtzr1gYk+2kIZuqtLclV9RDhs6j7meTaod2BDrF26tY
d33awv0txxrgXRhd/FDFVtKb0K84cQs2xtO/9A0yLs5GEK2xpG2yM4AeWWft
=I1r6Wtzf/29vTggAK+ELEA==
- -----END COMPRESSED RSA ENCRYPTED MESSAGE-----


Here is the public key used to encrypt it. Note that it has a low bit modulus and is therefore breakable:

$VAR1 = bless( {
                 'e' => 65537,
                 'n' => '78808916397911537795302584646496939287334116815815771036902928223331980368647390659163440305126971
                 'Version' => '1.99',
                 'Identity' => '<quaetrix0@gmail.com>'
               }, 'Crypt::RSA::Key::Public' );
```

The Number/Email

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


This message will only be displayed once.

Here is a message that has been encrypted with RSA (the Crypt::RSA Perl module available in CPAN) :

- -----BEGIN COMPRESSED RSA ENCRYPTED MESSAGE-----
Version: 1.99
Scheme: Crypt::RSA::ES::OAEP

eJwBzQAy/zEwADE4OABDeXBoZXJ0ZXh0Ca4y//uzl/HvFoP9Klf53nEFH0T4c+ui5de8+vqGOnZc
9DlrsWQe+xxVaPaYgKAD9Wn9VWQ6A5o254r5pa4hkDIY5RRmVfqOm88HJpGdbGGTckyEwJapCLDT
tHzZWAZ0FIVj6fH2whErHoVmZ82zQJ64OLtzr1gYk+2kIZuqtLclV9RDhs6j7meTaod2BDrF26tY
d33awv0txxrgXRhd/FDFVtKb0K84cQs2xtO/9A0yLs5GEK2xpG2yM4AeWWft
=I1r6Wtzf/29vTggAK+ELEA==
- -----END COMPRESSED RSA ENCRYPTED MESSAGE-----


Here is the public key used to encrypt it. Note that it has a low bit modulus and is therefore breakable:

$VAR1 = bless( {
                 'e' => 65537,
                 'n' => '78808916397911537795302584646496939287334116815815771036902928223331980368647390659163440305126971
                 'Version' => '1.99',
                 'Identity' => '<quaetrix0@gmail.com>'
               }, 'Crypt::RSA::Key::Public' );
```

RSA in 20 seconds

- Given **e** & **n**
- **e** = encryption exponent
- **n** = **p** * **q** (secret 🔒)
- **n** length = 112 digits (372 bits)

Big Number

78808916397911537795302584646496939287334116815815771036902928223331980368647390659163440305126971620685825558 37

(112 digits)

Bruteforce

```
ibotpeaches@foundation# time docker run -it b4den/rsacrack
78808916397911537795302584646496939287334116815815771036902928223331980368647390659163440305126971620685825558 37

[*] pubkey.e: 65537
[*] pubkey.n:
78808916397911537795302584646496939287334116815815771036902928223331980368647390659163440305126971620685825558 37

[*] Key looks like 372 bits
[*] Using cadonfs to compute primes
[*] results are: [u'98007492061325958997349177934627388613835953553459586261',
u'80411114232571782218163489375797613948878398942588985417', 65537L]
[*] Key extraction done.

-----BEGIN RSA PRIVATE KEY-----
MIHsAgEAAi8NG6bqKiUXBAidW7CmF+WTr6owpY+MprGwQrOWuRVHb0ko2zdWiiXkZH1Kv31gvQID
AQABAi8F4v06/GJby7vyr1LNxL2dba6I2lF1YQP3C1P+Jz85VYigO/4Am+s2SkB+4BkDAQIYA/8+
91K7m8jMN43hdcKwWiVe54kqoyTVAhgDR4f9CRgCSsFj8VvilwjwOLfevXiIYEkCGAPbGvIekjHj
y6NiHDcBY+HDuGDQG2gI0wIYALzWdGz/0rb/ydL/oNbpR8aRo4MjE4uHAhgDx+oNUAE2EddY+lDq
EqRxF5D0juT2Kwg=
-----END RSA PRIVATE KEY-----

real    94m12.942s
user    0m0.214s
sys     0m0.115s
```

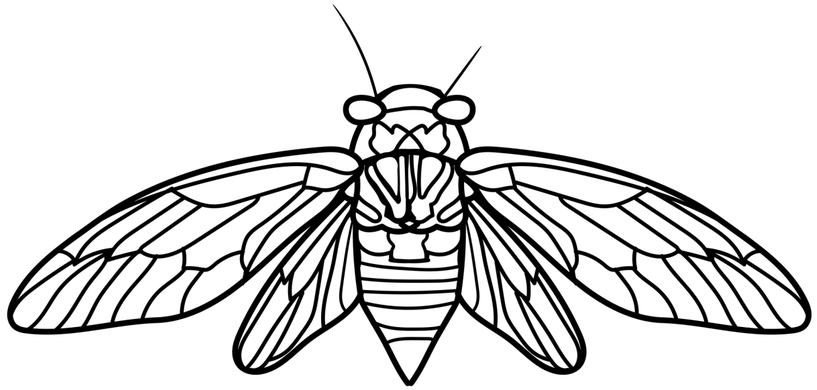
Perl Time

```
use Crypt::RSA;

my $algo = new Crypt::RSA;
my $keychain = new Crypt::RSA::Key;

my ($public, $private) = $keychain->generate(
 'q' => '980074920613259589973491779346273886138359535534595862 6
 'p' => '804111142325717822181634893757976139488783989425889854 1
 'e' => '65537'
);

$encrypted = "
-----BEGIN COMPRESSED RSA ENCRYPTED MESSAGE-----
Version: 1.99
Scheme: Crypt::RSA::ES::OAEP

eJwBzQAy/zEwADE4OABDeXBoZXJ0ZXh0Ca4y//uzl/HvFoP9Klf53nEFH0T4c+ui
9DlrsWQe+xxVaPaYgKAD9Wn9VWQ6A5o254r5pa4hkDIY5RRmVfqOm88HJpGdbGGT
tHzZWAZ0FIVj6fH2whErHoVmZ82zQJ64OLtzr1gYk+2kIZuqtLclV9RDhs6j7meT
d33awv0txxrgXRhd/FDFVtKb0K84cQs2xtO/9A0yLs5GEK2xpG2yM4AeWWft
=I1r6Wtzf/29vTggAK+ELEA==
-----END COMPRESSED RSA ENCRYPTED MESSAGE-----
";

print $algo->decrypt(
 Cyphertext => $encrypted,
 Key        => $private,
 Armour     => 1,
);
```

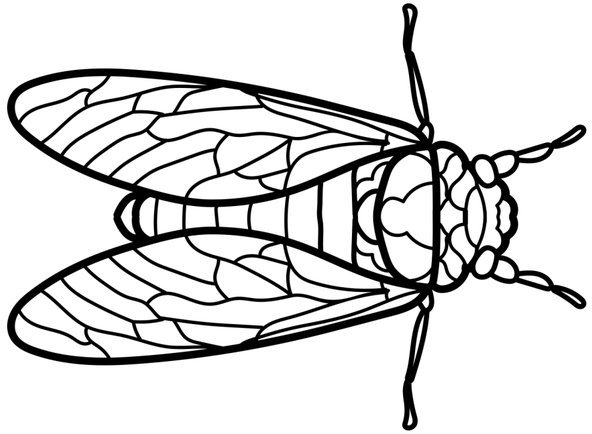
The Solve

```
➜  perl script.pl
```

335214940434302586 76



Correct. We'll email you



The Song

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

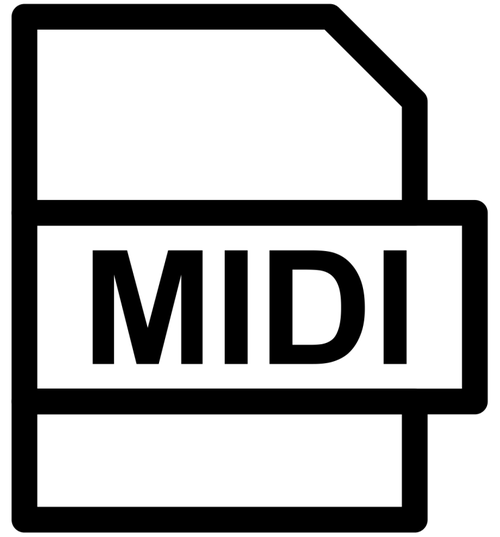
This song is your own path
Another stop on the road toward enlightenment
Follow it, and share not

Let the Chorus be your guide to the depths :

> Let the Priests of the Raven of dawn,
> no longer in deadly black, with hoarse note
> curse the sons of joy. Nor his accepted
> brethren, whom, tyrant, he calls free lay the
> bound or build the roof. Nor pale religious
> letchery call that virginity, that wishes
> but acts not.
>
> For every thing that lives is Holy.

Good luck.

3301



midicsv

0, 0, Header, 1, 3, 96

1, 0, Start_track

1, 0, Text_t, "Cicada at Fri Jan 20 03:57:39 2012"

1, 0, End_track

2, 0, Start_track

2, 0, Text_t, "Cicada at Fri Jan 20 03:57:39 2012"

2, 0, Tempo, 500000

2, 0, Program_c, 1, 6

midicsv

track	time	event	channel	note	velocity
2	0	Note_on_c	1	63	96
2	192	Note_off_c	1	63	0
2	192	Note_on_c	1	61	96
2	216	Note_off_c	1	61	0

midicsv

track	time	event	channel	note	velocity
2	0	Note_on_c	1	63	96
2	192	Note_off_c	1	63	0
2	192	Note_on_c	1	61	96
2	216	Note_off_c	1	61	0

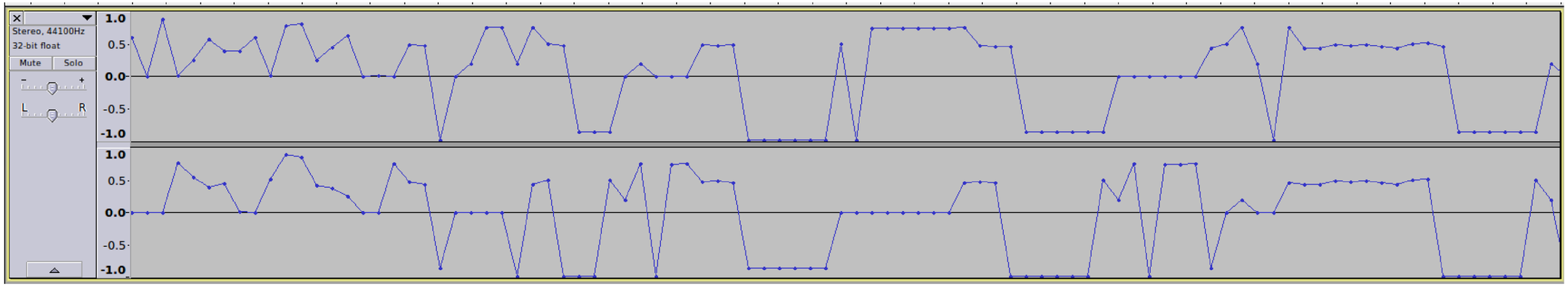
Duration & Note

- Duration = (Off - On)
- Note = Note

time	event	note	duration
96	Note_on_c	63	-
120	Note_off_c	63	**24**

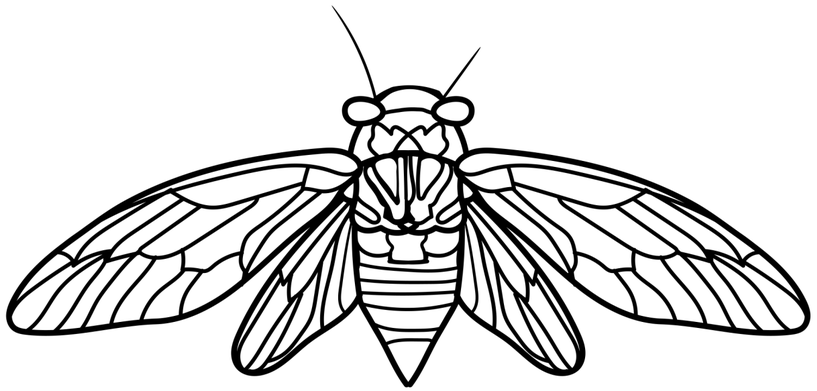
Cipher

- Iterate 2nd track
- Work through chorus
- Skip previously used characters



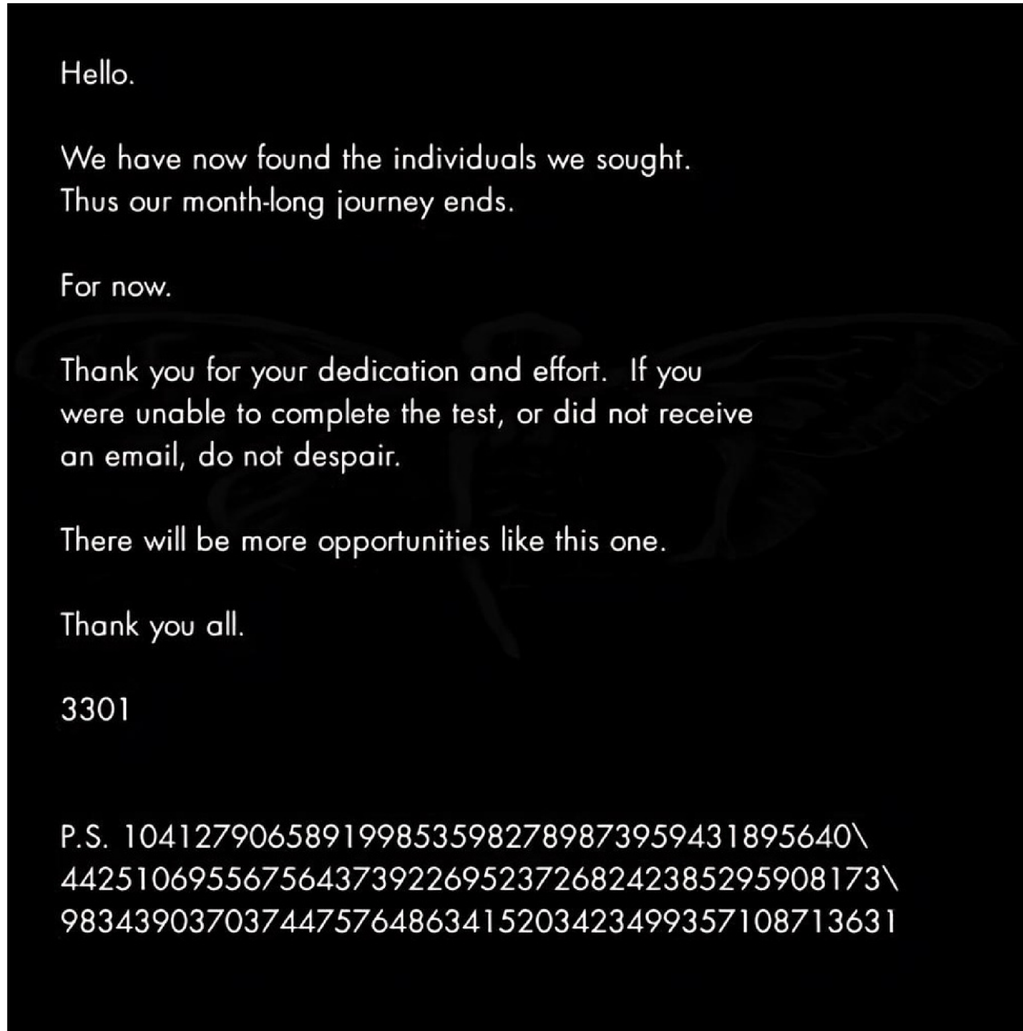
Solved

Very good you have proven to be most dedicated to come this far to attain enlightenment.



Puzzle 1 - Done

- Released on Reddit
- End of 2012 Puzzle



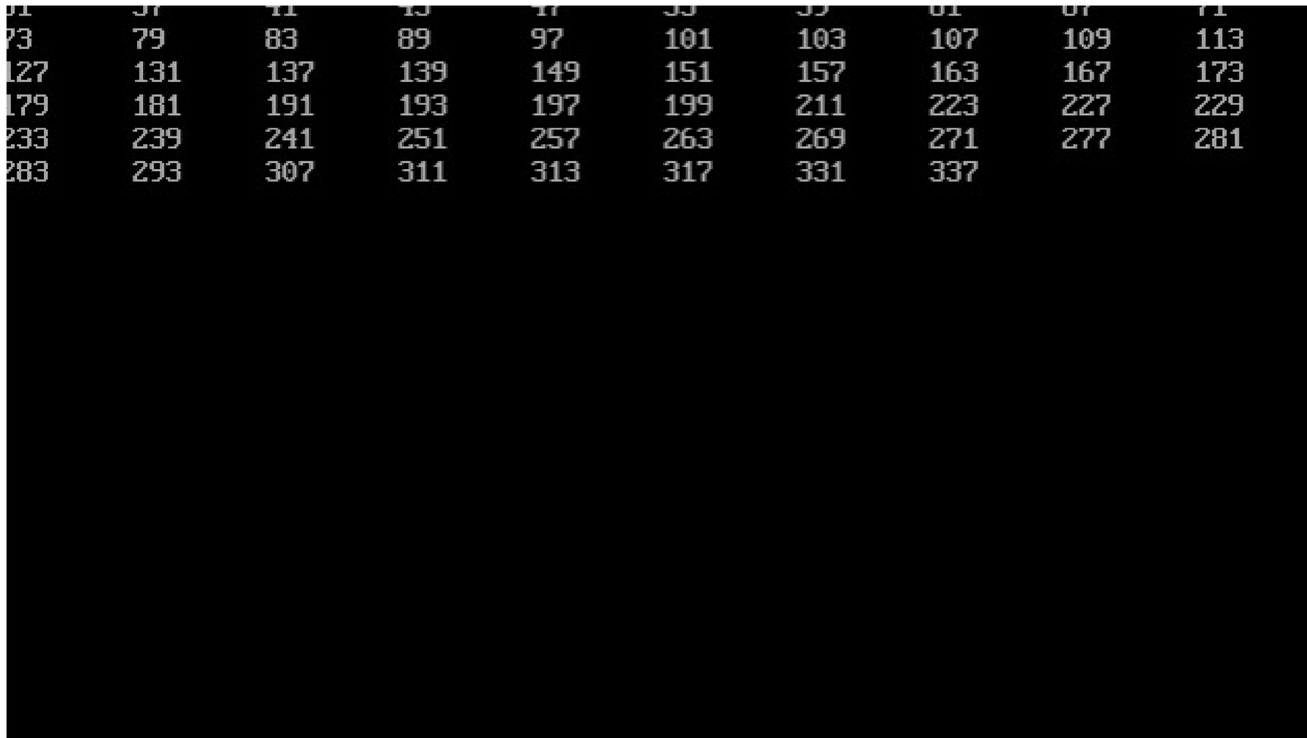
Jan 5, 2013

reddit.com

- We go again

Puzzle 2 - ISO

- Riddle, Book Code, Book
- Dropbox URL
- ISO



The OS

@1231507051321

The key is all around you.

Good luck.

3301

Twitter

- Offset: Data
- Gibberish

Tweet Collection

```
0000000: b69ccce300104a4648025459595800010008d0000ff8b6131616a6a632737293d3e322b3b3e3f263a203c0c4762677c326767713d73716d697b6e3000505b494e47
0000041: 404a727b0843460c44595114476a555f5c5b57604064511292ae7337217a616c682b636d7f2d77454f3c425b4051475f545740575c515741096e5c745b5c561246
0000082: 5a5712565b445b5c5b464b12455b465a5b5c12535c5612575f5740559aee54585c314a025616012200567964235 86f8cb0616d20456c607366646f626454504531
00000c3: 0000000501020337363636f7f2ba6fffc400b5100002010303020403050504040000017d0102030004110512213141 4f7d370e0722711b3281895d081e70afc117
0000104: 57d6fa283c736695101608363b3f320e08171b1c120e0876757d7e700f0b1412101115143237333f3c362929161c1f1be7eaecedf9f8fae4e3efe0e61d2526202e
0000145: 23273a21262c2f2b575a5c5d686f6b77727071757453505 25c5d59484a4f3a3839c5c6c7f1858b9f96e7fbefefaad860e1e2e3e4e5e6e7e8dd2ad5f533b9f5f637
0000186: f8c4c8e1e50c2cae000301010101010101010100000000000001020304050607080 90a0bffc400b51100020102040403040705040400010277000102031104052 1
00001c7: 3106124151076171132232810814429 1a1b1c109233352f0156272d10a162434e125f11718191a262728292a35363738393a434445464748494a53545556575859
0000208: 5a636465666768696a737475767778797a828384858687888 98a92939495969798999aa2a3a4a5a6a7a8a9aab2b3b4b5b6b7b8b9bac2c3c4c5c6c7c8c9cad2d3d4
0000249: d5d6d7d8d9dae2e3e4e5e6e7e8e9eaf2f3f4f5f6f7f8f9faffda000c03010002110311003f00f00a28a2800a28a2800a28a2800a28a2800a28a2800a28a2800a28
000028a: a2800a4a5a2800a28a2800a28a2800a28a2800a28a2800a28a2800a28a2800a28a2800a28a2800a28a2800a28a2800a28a2800a28a2800a29296800a28
00002cb: a2800a28a2800a28a2800a28a2800a28a2800a28a2800a28a2800a28a2800a28a2800a4a5a2800a28a2800a28a2800a28a28012968a2800a28a2800a28a2800a28
000030c: a2800a28a2800a28a2800a28a2800a4a5a2800a28a2800a28a2800a28a2800a28a2800a28a2800a28a2800a28a2800a28a2800a275d3b0c68a24058cf2140884e9
000034d: da4c44df8937c35f5a993b56ba1aef5fb76b9414138cf8bea450e2fb63ae550832e069a3d975e5cc784c6479ca379f01b5a8c501300fdc8461304d46bd665e0084
...
```

To Binary?


```
binwalk 3301_twitter.bin

DECIMAL       HEXADECIMAL     DESCRIPTION
--------------------------------------------------------------------------------
```

OS Files

- AUDIO/761.mp3
- DATA/_560.00
- DATA/560.13
- DATA/560.17

OS Files

- **AUDIO/761.mp3**
- DATA/_560.00
- DATA/560.13
- DATA/560.17

The Instar Emergence

XOR

- XOR Twitter data & 761.mp3
- Obtain an image

Gematria Primus

an order and a value as revealed through 3301

Rune	Letter	Value	Rune	Letter	Value
ᚠ	F	2	ᛋ	S/Z	53
ᚢ	U	3	ᛏ	T	59
ᚦ	TH	5	ᛒ	B	61
ᚩ	O	7	ᛖ	E	67
ᚱ	R	11	ᛗ	M	71
ᚳ	C/K	13	ᛚ	L	73
ᚷ	G	17	ᛝ	NG/ING	79
ᚹ	W	19	ᛟ	OE	83
ᚻ	H	23	ᛞ	D	89
ᚾ	N	29	ᚪ	A	97
ᛁ	I	31	ᚫ	AE	101
ᛄ	J	37	ᚣ	Y	103
ᛇ	EO	41	ᛡ	IA/IO	107
ᛈ	P	43	ᛠ	EA	109
ᛉ	X	47			

Gematria Primus

an order and a value as revealed through 3301

Rune	Letter	Value
ᚠ	F	2
ᚢ	U	3
ᚦ	TH	5
ᚩ	O	7
ᚱ	R	11
ᚳ	C/K	13
ᚷ	G	17
ᚹ	W	19
ᚻ	H	23
ᚾ	N	29
ᛁ	I	31
ᛄ	J	37
ᛇ	EO	41
ᛈ	P	43
ᛉ	X	47

Rune	Letter	Value
ᛋ	S/Z	53
ᛏ	T	59
ᛒ	B	61
ᛖ	E	67
ᛗ	M	71
ᛚ	L	73
ᛝ	NG/ING	79
ᛟ	OE	83
ᛞ	D	89
ᚪ	A	97
ᚫ	AE	101
ᚣ	Y	103
ᛡ	IA/IO	107
ᛠ	EA	109

Outguess

- Blank (?)
- Tabs/Spaces

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

-----BEGIN PGP SIGNATURE-----
Version: GnuPG v1.4.11 (GNU/Linux)

iQIcBAEBAgAGBQJQ5lDTAAoJEBgfAeV6NQkP7nMQAJVg7DQilA7NpkacR0RA4eBs
NZHJBQNHO2P22h+aFfP/rl1gjGaV3hMWaa2sQ4Vbi/W8eZuH40AsmZUy3EOb+4j0
3cJRJgAJl99ZjDcVXITm5VyUv+WIqCzBr+bHMK7pkMYQ/rEzeWD56tlsrDgFdjmh
PA/b7XrDcofd9JfBNFI7D/sF84HL2ig5baNo+MGjYl4Dq2cHX+SAafXmlN9PXFjx
HRBbuoMLlviKywQ8MnePBPYG6V8sIMmrJlHS5ZcNEaSJ9nGL4X0XbECqV79ermye
1EeNKcckoeeZMU86SabfMeyZozG04Vkbemn8JH5cssbuF8hf4fdN/LSP4NG0r5y9
jfRv7z59pL577ZpGAju5zBtlCBUvmxxNYR5IGLg+Fi/ICqcRC98mzesFnQ7wbDLS
HKyV95SBQK82bbqSREBfIrrNb+MjVtJwIvOY5OPTBViHPqrIuMw8KDGfSvw9ncCt
dase7vUjXxIrn36xDSRN6cMzTmFZ9lkQYkRAYq5ApERud+JfKCwszG/UxRwo1WOU
0ALaWXq5VMp+w5pvQkqg9eHpOriG9Z11VLdb53eTmxKrwyX/2eaiybsnMrRNuxv1
iE8PVRkifCcJccw1bGq8TyCQF3a5ozeiBRngAUT7BwZhLa4bShtki7amR0ZZgbKk
8JRMGvoSA5NNTEwvUhwl
=ZeNf
-----END PGP SIGNATURE-----

Binary Time

01000011011011110110110101100101001000000111010001101111001000000110010101101101011010010111011011100000011010001101101011101010111010100110010011010110111010001110111011010110111011001100110001011100110111101101110011010010110111101101110

01010111011001010010000001110011011010000110000101101100011011000010000001100001011101110110000101101001011101000010000011110010110111101110101001000000111010001101000011001010111001001100101011100100110010100101110

01000111011011110110111101100100001000000110110001110101011000110110101100101110

00110011001100110011000000110001

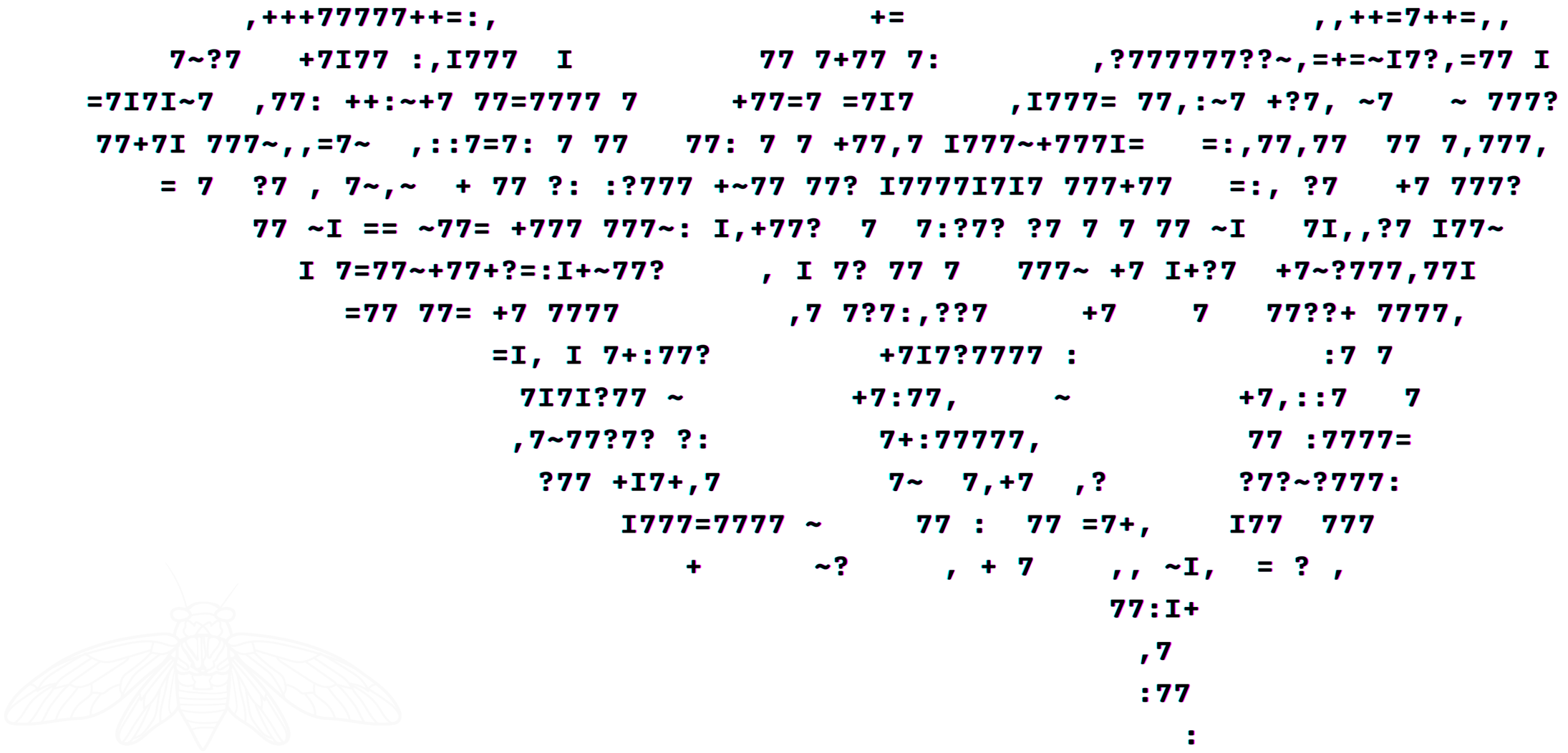
"Come to emiwp4muu2ktwknf.onion"

"We shall await you there."

"Good luck."

"3301"

Web browsers are useless here.



Welcome.

Telnet?


```
hello
A message for you:

0000000: 2d2d2d2d2d424547494e20504750205349474e4544204d455353414745 2d2d2d2d2d0a486173683a20534841310a0a20202020200a5665727920676f6f642e0a20
0000041: 20200a596f75206861766520646f6e652077656c6c20746f20636f6d65207468697320666172e0a20200a7873786e616b7369637436656778 6b712e6f6e696f6e
0000082: 0a20200a476f6f64206c75636b2e0a2020200a333330310a20202020200a2d2d2d2d2d424547494e20504750205349474e41545552452d2d2d2d2d0a5665727369
00000c3: 6f6e3a20476e7550472076312e342e31312028474e552f4c696e7578290a0a695149634241454241674147425 14a5136533048414 16f4a4542676641655 6364e51
0000104: 6b502f4a3051414c44716133564a7939784c4c6c6749356a506852497034 0a66786562624e6874454c4f4859466b44355a397a745159476c65376c4b504d386c6b
0000145: 4d536e636949593035394b4969354e53545637493937734a626f473377740a6b6848745a674e527731763257513575757243753 56c31772b38342f4c354a7a324e
0000186: 6d456c784f427a57723638646c515974327166425178 6b327a522f6654490a544c43454776465a746c6e724e66426b376a7349794a596358585067616253343 76f
00001c7: 5039764f45586c42312b506d3043377550504250 4e3761716b665550476c0a6f3166326873634a66374a65324476625a742b3665787859736d3537467039353358
0000208: 414e41642f557046567a542f3835325867363367745a72492b536d66335a0a4256636a70437a7948337753385230694d2b7270303243774a704a7a7357474c7865
0000249: 51476d584c325358424234337a565a414a716c355564584c5447586b62640a6e504d64332f43624a2b6c37724f3059416735703 34a66344b617558375a64365a63
000028a: 3277484b4c4f76666a5176455758495931434d68493638426a30725a6f2f0a4d2f6669333133464654504 16d3678684b52762f74482f387756726172326a593777
00002cb: 6e4538587868527379373441 5a35477141326f484d6566544171335975570a3550583873363832 4a34706b44554b4847613479363576 6a49703136706d45496e4d
000030c: 414c4a4762777a366d7461754251716c5336415273516665 6b446e336f5a0a796f73532b675743336a6449764835733557555147566c376a797a3974342b335467
000034d: 35635439526e367058324e564e585378677a585842346e493258727259610a346b5172356157423 6c737361763372796a3543673246486c312b4d4b4f30675976
000038e: 2f554633515437354d6978514d75344d2b3577436e4e656b676675794f360a5a7679627a70347334537a526a6b6b39734d4d360a3d5759564f0a2d2d2d2d2d454e
00003cf: 4420504750205349474e41545552452d2d2d2d2d0a
Offset: 3301, Skip: 0, Col: 65, Line: 16.
```

XXD

- To Binary


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


Very good.

You have done well to come this far.

xsxnaksict6egxkq.onion

Good luck.

3301

-----BEGIN PGP SIGNATURE-----
Version: GnuPG v1.4.11 (GNU/Linux)
```

Another Hint


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

You already have everything you need to continue.

Sometimes one must "knock on the sky and listen to the sound."

Good luck.

3301

-----BEGIN PGP SIGNATURE-----
Version: GnuPG v1.4.11 (GNU/Linux)
```

Ping away

```
1f8b080843f5ee5000036d6573736167652e7478742e617363006d93
49b3aa460085f7fd2b582645dd8b80a2bcaa2c8046684406914176 20
202d43338bfefadc57c92e39db337cabf3f5f52359d59045399a4379
48b354489d55cf9334f5b7f705f4642c7f519e2eb1008030af6b2a23
6dfe4d5137325365b2e4d49d34395524c337005d55372b97e7a5503c
a7fda7f8262d262d001a211955cff7ea27c3f39bdf535fff454b57ff
f22f35c887f1a7f98bd2dad9d1a885fdde7eb32cf58766f98c89db79
fd1300eca2bb2ca9b2f49034d935dcfd12404922862a3f0a290f04cb
ad1c71dd3a0ccf4a3bd3f9a0b2c2f830cacf3958d1dd6ec1f674746d
7a0e82f1b2e33fa8f1fabaec051c48aa489fc87e41fd1372aff28afc
...
```

XXD - Part 2

- To Binary


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


Well done.  You have come far.

pklmx2eeh6fjt7zf.onion

Good luck.

3301


-----BEGIN PGP SIGNATURE-----
Version: GnuPG v1.4.11 (GNU/Linux)
```

Coordinates

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


Standby for coordinates.

-----BEGIN PGP SIGNATURE-----
Version: GnuPG v1.4.11 (GNU/Linux)
```

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

37.182685, -3.605801
-----BEGIN PGP SIGNATURE-----
Version: GnuPG v1.4.11 (GNU/Linux)

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

38.977845, -76.486451
-----BEGIN PGP SIGNATURE-----
Version: GnuPG v1.4.11 (GNU/Linux)

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

33.092817, -96.08265
-----BEGIN PGP SIGNATURE-----
Version: GnuPG v1.4.11 (GNU/Linux)

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

34.7477910, -92.2690863
-----BEGIN PGP SIGNATURE-----
Version: GnuPG v1.4.11 (GNU/Linux)

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

26.41968, 127.73254
-----BEGIN PGP SIGNATURE-----
Version: GnuPG v1.4.11 (GNU/Linux)

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

32.478944, -84.983674
-----BEGIN PGP SIGNATURE-----
Version: GnuPG v1.4.11 (GNU/Linux)

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

37.182685, -3.605801
-----BEGIN PGP SIGNATURE-----
Version: GnuPG v1.4.11 (GNU/Linux)

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

38.977845, -76.486451
-----BEGIN PGP SIGNATURE-----
Version: GnuPG v1.4.11 (GNU/Linux)

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

33.092817, -96.08265
-----BEGIN PGP SIGNATURE-----
Version: GnuPG v1.4.11 (GNU/Linux)

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

34.7477910, -92.2690863
-----BEGIN PGP SIGNATURE-----
Version: GnuPG v1.4.11 (GNU/Linux)

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

26.41968, 127.73254
-----BEGIN PGP SIGNATURE-----
Version: GnuPG v1.4.11 (GNU/Linux)

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

32.478944, -84.983674
-----BEGIN PGP SIGNATURE-----
Version: GnuPG v1.4.11 (GNU/Linux)

Locations

- Japan
- Russia
- Texas
- Arkansas
- Maryland
- Oregon
- Georgia

Phone Call

- Call Number
- Asks for Code
- Enter “*L (5) & M (6)*”
- **Failed**

Phone Call

- Call Number again
- Asks for Code
- Enter “*L (73) & M (71)*”
- **Accepted**

Gematria Primus

an order and a value as revealed through 3301

Rune	Letter	Value	Rune	Letter	Value
ᚠ	F	2	ᛋ	S/Z	53
ᚢ	U	3	ᛏ	T	59
ᚦ	TH	5	ᛒ	B	61
ᚩ	O	7	ᛖ	E	67
ᚱ	R	11	ᛗ	M	71
ᚳ	C/K	13	ᛚ	L	73
ᚷ	G	17	ᛝ	NG/ING	79
ᚹ	W	19	ᛟ	OE	83
ᚻ	H	23	ᛞ	D	89
ᚾ	N	29	ᚪ	A	97
ᛁ	I	31	ᚫ	AE	101
ᛄ	J	37	ᚣ	Y	103
ᛇ	EO	41	ᛡ	IA/IO	107
ᛈ	P	43	ᛠ	EA	109
ᛉ	X	47			

Phone Call

*dataset **13**, offset **12821***

data

28C07E1B102D4D5C4C1A376E0644

77E1416FCC94928765

Read Data

- Read DATA/560.13
  - Extract file chunk
- XOR (Phone data & above)

4l6uipnstbggwjyv.onion

SSSS

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

ssss, Threshold: 5

07-f3adb3aacb0b4336fa28178bc1e5edce940c16ce5caa

Good luck.

3301
-----BEGIN PGP SIGNATURE-----
Version: GnuPG v1.4.11 (GNU/Linux)
```

Shamir Secret Sharing Scheme

- Break secret into chunks
- Need a few to recreate
- 5 minimum from Cicada

Working Together


```
➜ ssss-combine -t 5
Enter 5 shares separated by newlines:
Share [1/5]: 05-fcd82965b6632ea25d80edc3e58baafb4b2938895cbd
Share [2/5]: 07-f3adb3aacb0b4336fa28178bc1e5edce940c16ce5caa
Share [3/5]: 09-82a98a7fe06014f783b752506cf6cd1fabaa3d8b3750
Share [4/5]: 03-7678a5f6b72042d839151b34b02ffe161cf997fed484
Share [5/5]: 02-41cc481a51fe77f91600f593c1db2ce9babd2626ea6e
Resulting secret: p7amjopgric7dfdi.onion
```

The Test

Question:

Disregarding color blindness, any arbitrary color looks the same to all people.

Answer:

- ○ True
- ○ False
- ○ Indeterminate
- ○ Meaningless
- ○ Self-Referential
- ○ Game Rule
- ○ Strange Loop
- ○ None of the Above

Post Answer

01 min and 56 sec

The Exam

- Build TCP Server
- Respond to this protocol
- Deadline: Feb 3, 2013

```
2013/02/25 14:32:01 server is running under address [::]:3307
2013/03/03 10:57:48 got connection from 127.0.0.1:42483
2013/03/03 10:58:05 executing 'rand 3' for 127.0.0.1:42483
2013/03/03 10:58:09 executing 'rand 3' for 127.0.0.1:42483
2013/03/03 10:58:18 executing 'rand 0' for 127.0.0.1:42483
2013/03/03 10:58:29 executing 'rand 1' for 127.0.0.1:42483
2013/03/03 10:58:56 executing 'quine' for 127.0.0.1:42483
2013/03/03 10:59:10 executing 'base29 1033' for 127.0.0.1:42483
2013/03/03 10:59:14 executing 'koan' for 127.0.0.1:42483
2013/03/03 10:59:16 executing 'koan' for 127.0.0.1:42483
2013/03/03 10:59:18 executing 'koan' for 127.0.0.1:42483
2013/03/03 10:59:21 executing 'koan' for 127.0.0.1:42483
2013/03/03 10:59:28 executing 'dh 3301' for 127.0.0.1:42483
2013/03/03 10:59:56 executing 'dh 3301' for 127.0.0.1:42483
2013/03/03 11:00:29 executing 'dh 3301' for 127.0.0.1:42483
2013/03/03 11:00:58 executing 'next' for 127.0.0.1:42483
2013/03/03 11:01:11 executing 'dh' for 127.0.0.1:42483
2013/03/03 11:01:18 executing 'goodbye' for 127.0.0.1:42483
2013/03/03 11:01:18 closing connection to 127.0.0.1:42483
```

Puzzle 2 - Over

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

DO NOT SHARE THIS INFORMATION!

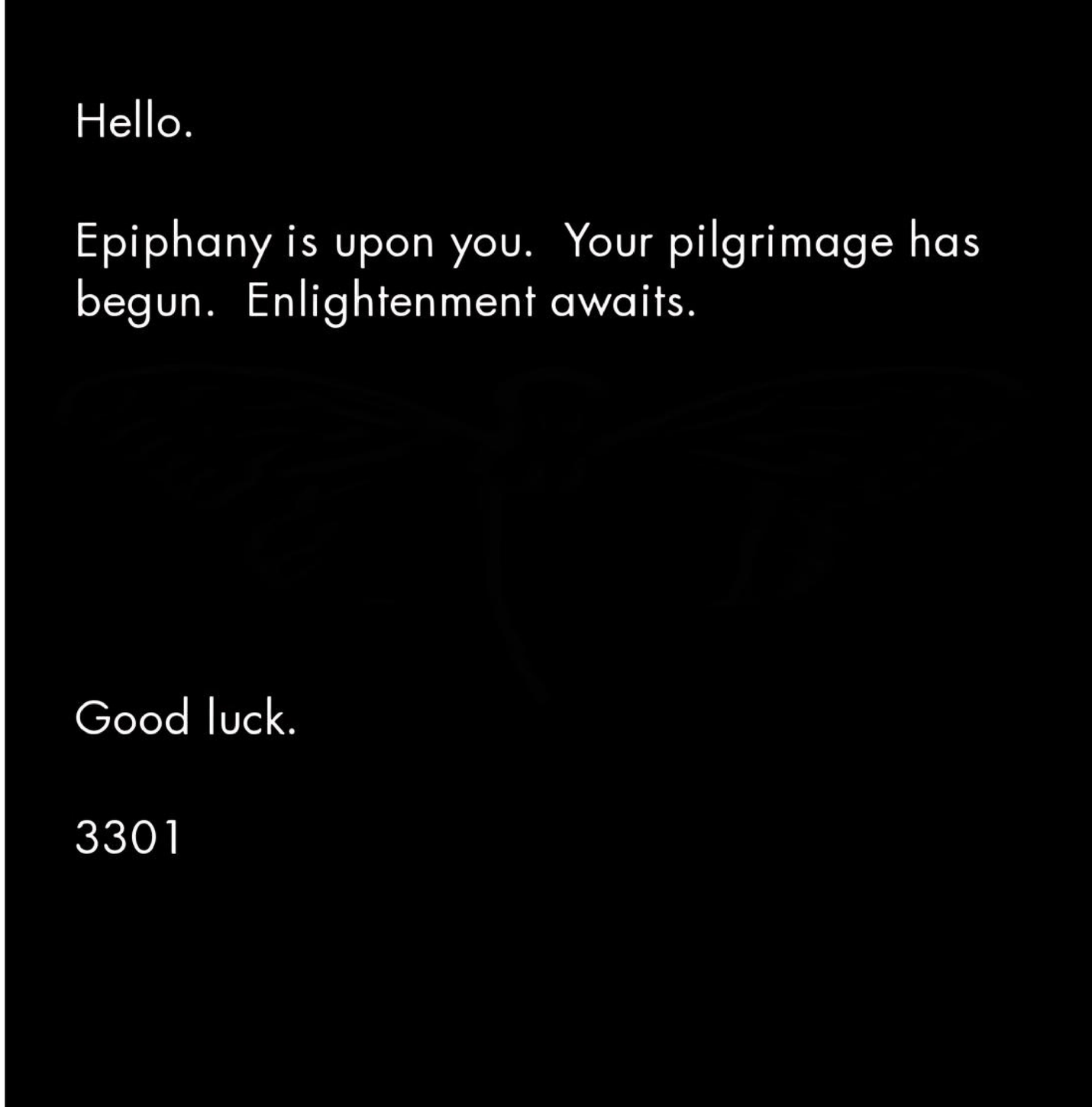
Congratulations. Your testing has finally come to an end. We hope you have enjoyed the "vacation" over the last few weeks. You will be very busy now should you choose to join us.

There are two final steps, although there won't be any hidden codes, or secret messages, or physical treasure hunts. This first of these is only honesty. We have always been honest with you, and we shall continue to be honest with you. And we expect you to be honest with us in return.

Jan 6, 2014

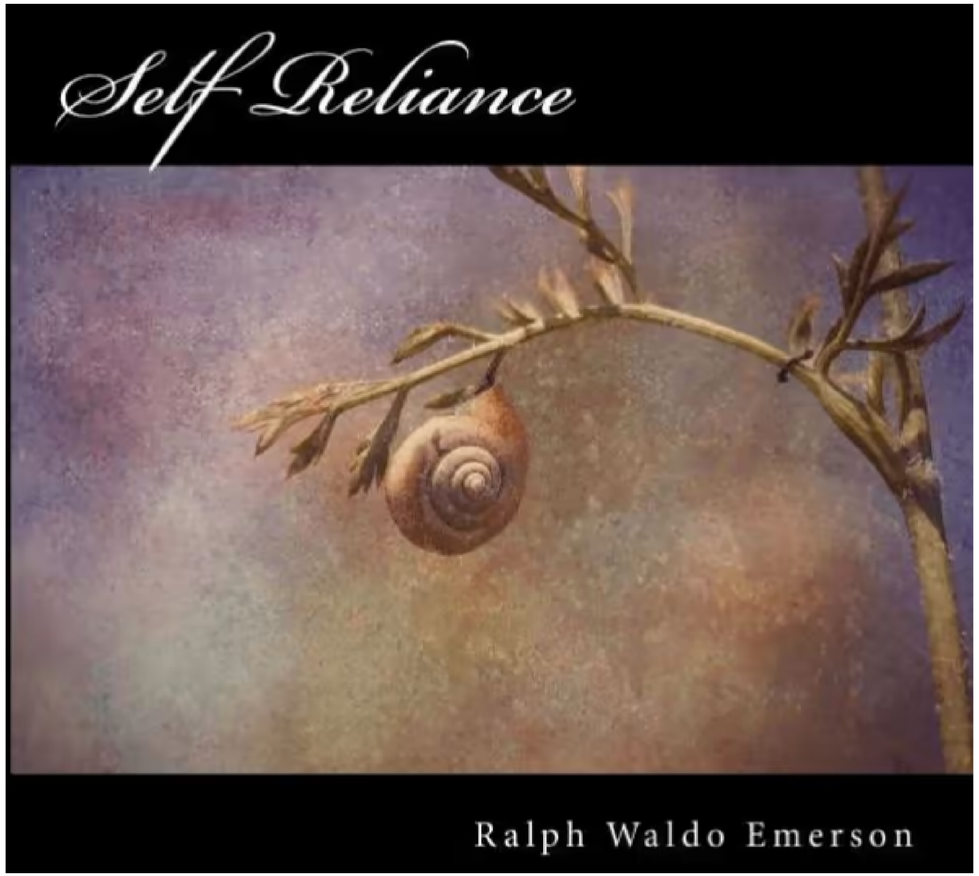
twitter.com

- 3rd times a charm.

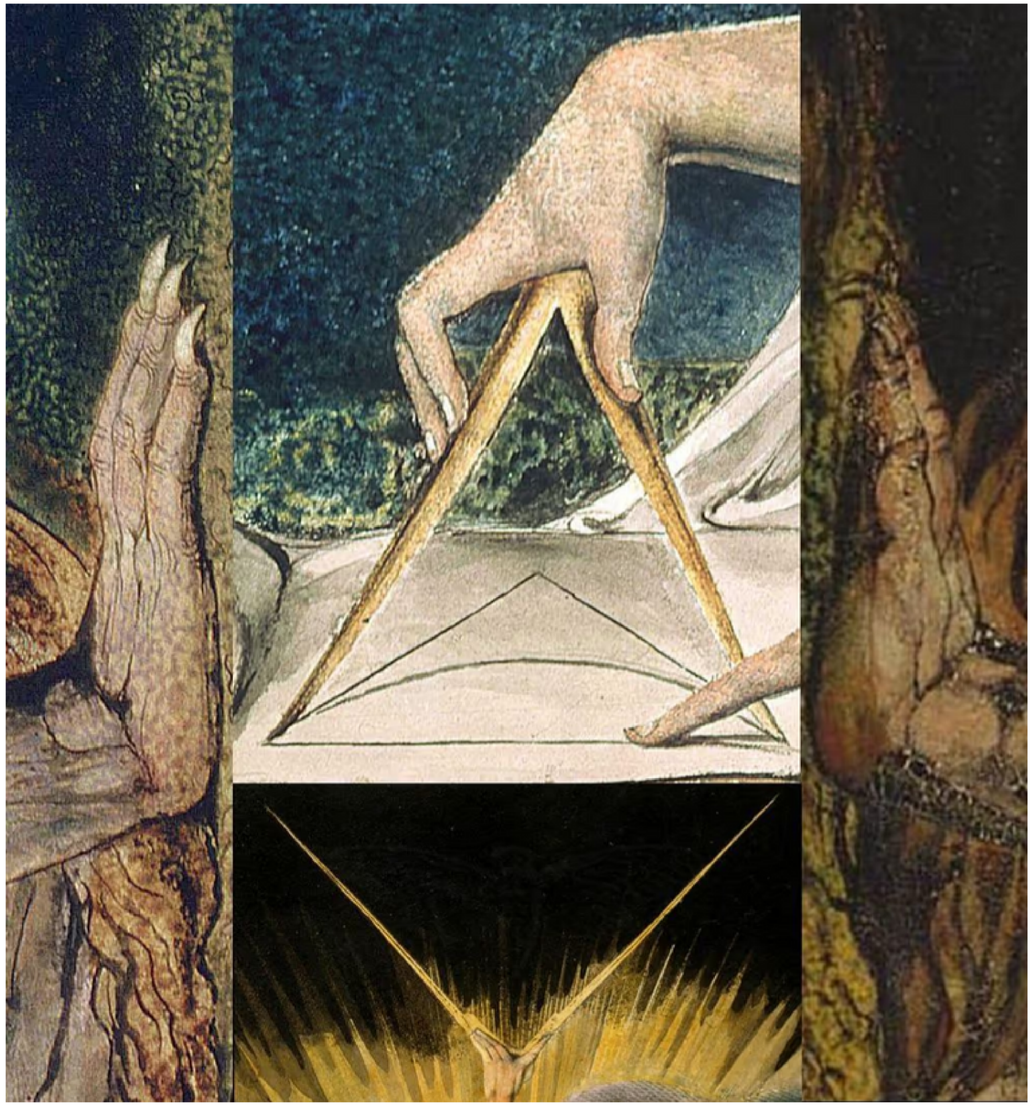


Puzzle 3 - Book Code

- Paragraph
- Sentence
- Word
- Letter



auqgnxjtvdbll3pv.onion



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

Welcome.

Good luck.

3301



e = 65537
n =
75579125746085351644267182920580212556413102071876330957950694457000592102480507572702346799936738442031480131730911737865721166 39

- -----BEGIN COMPRESSED RSA ENCRYPTED MESSAGE-----
```

Big Number Redux

75579125746085351644267182920580

21255641310207187633095795069445

70005921024805075727023467999367

38442031480131730911737865721166

39

(130 digits)

Bruteforce

```
ibotpeaches@foundation$ time docker run -it b4den/rsacrack
755791257460853516442671829205802125564131020718763309579506944570005921024805075727023467999367384420314801317309117378
657211663

[] pubkey.e: 6553
[] pubkey.n:
755791257460853516442671829205802125564131020718763309579506944570005921024805075727023467999367384420314801317309117378
657211663

[] Key looks like 432 bit
[] Using cadonfs to compute prime
[] results are: [u'975137790503221592976646712386708500856610860432665917393380073 21',
u'775060986069287800218299647816952128371959590823704738205093607 59', 65537L
[] Key extraction done

-----BEGIN RSA PRIVATE KEY----
MIIBDAIBAAI3AK50gkj06lhiMbT/iIsA+l1l517rgOiDK25eRHiXDIgpO0NuKFHO3U/5YHNaIjM
YqZZ4ilSnwIDAQABAjZtP5cLOxy6RpvcPh3y9qTS8mrnHVH3yZTcI/lwoIubRaCJaifErsBrjIv
e7LQ1fgyRo+c8hECHADtCvlDTZS6NNntQIAKTebM9nwGSpu4imfXoxkCHAC8aCngGxUhK0bNdTn
h4An2V1NmuWt2dhy0ncCGwcXfSAieOKBt851ZR3Jj1gA/Yd59zPLwxw4uAIbNsOR69rhfdX5eVH
4QFynOdXzrhchHsl3IjkAhsmGCSA2T0fTd6T+mJ7XHMpxqj9oFdz93zmJLk=
-----END RSA PRIVATE KEY-----

real    717m2.977
user    0m1.752
sys     0m0.245
```

cu343l33nqaekrnw.onion

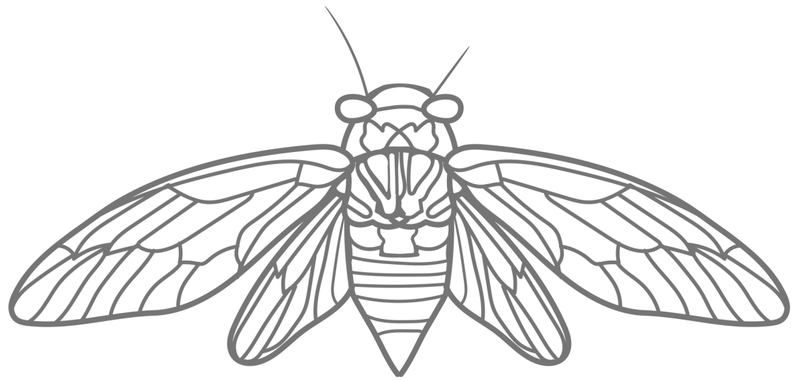
Liber Primus

Chapter 1

Intus

Linear Fracture

- Many pages
- Tough puzzles
- Not in order
- Progress slowed



May 2, 2014

- Released at once
- 76 pages
- 19 solved

Jan 5, 2016

twitter.com

- No new puzzle

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

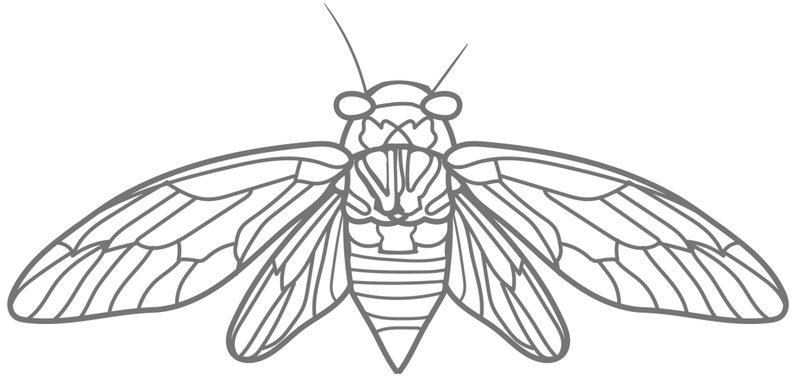
Beware false paths. Verify OpenPGP 7A35090F.

April 2017

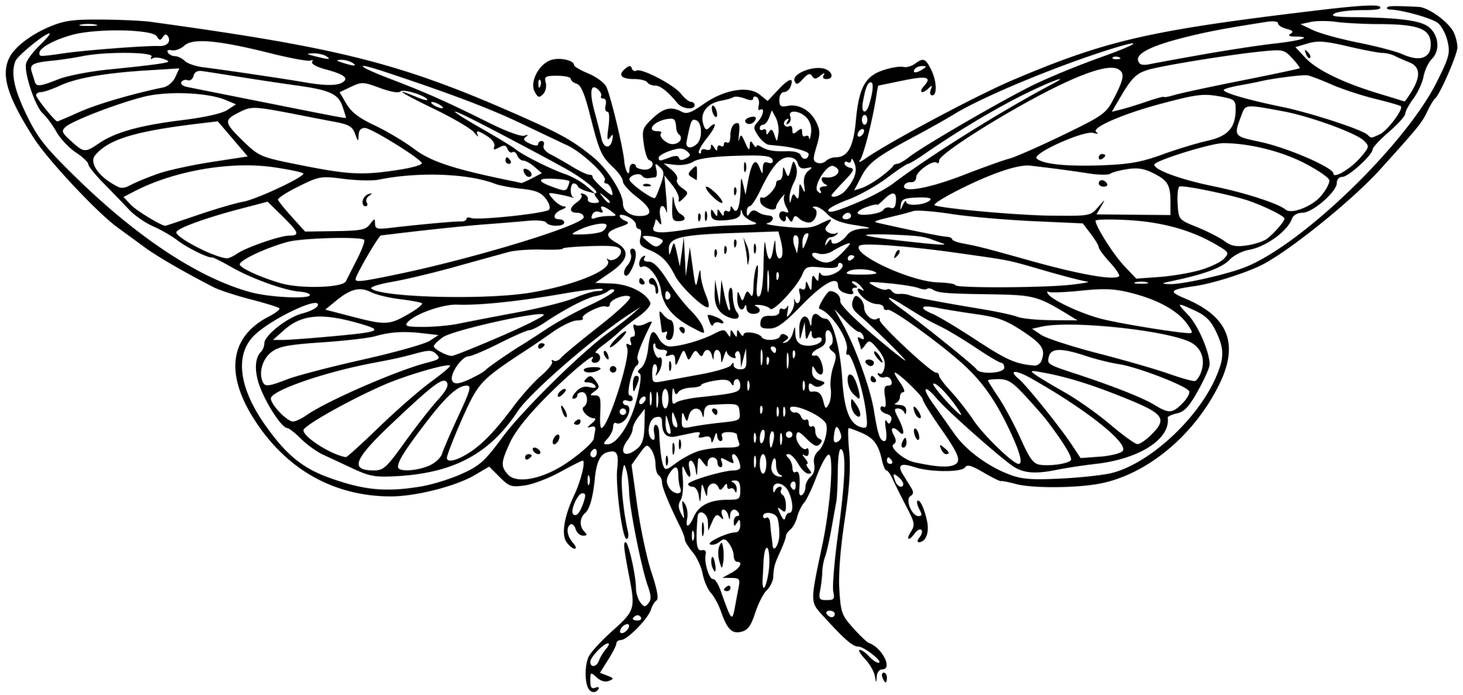
```
-----BEGIN PGP SIGNED MESSAGE-----
Hash: SHA512

Beware false paths.  Always verify PGP signature from 7A35090F.

3301

-----BEGIN PGP SIGNATURE-----
Version: CicadaPG v.3301
```

Cicada 3301

- An organization?
- A 3 letter agency?
- A person?
- A government?

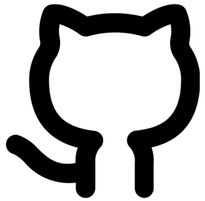


“Question all things.”



Cicada 3301

Thanks!

 iBotPeaches/cicada_3301

 infosec.exchange/@iBotPeaches

 connortumbleson.com

 iBotPeaches