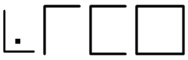
1. For the following cipher (ASCII coding), determine the decoded string: %62%69%6F%6D%65%74%72%69%63

Additional information:

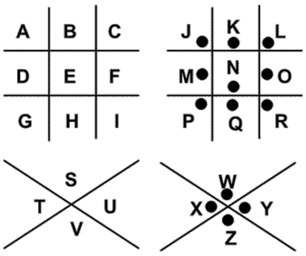
```
a (%61) b (%62) c (%63) d (%64) e (%65) f (%66) g (%67) h (%68) i (%69) j (%6A) k (%6B)
l (%6C) m (%6D) n (%6E) o (%6F) p (%70) q (%71) r (%72) s (%73) t (%74) u (%75) v (%76)
w (%77) x (%78) y (%79) z (%80) SPACE (%20)
```

Ans: b-------c

2. Solve this Pigpen cipher:

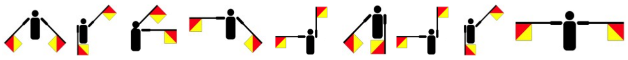


Additional information:

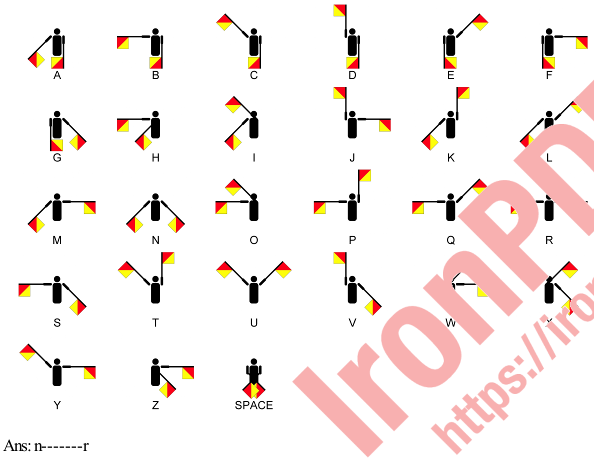


Ans: l--e

3. Solve this semaphore cipher:

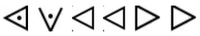


Additional information:

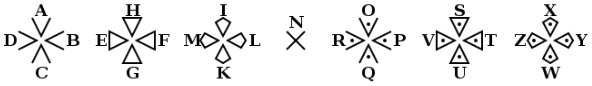


Ans: n-------r

4. Solve this Templar cipher:

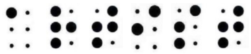


Additional information:

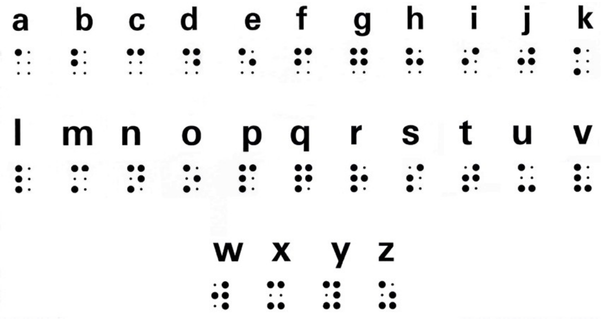


Ans: t----e

5. Solve this Braille cipher:

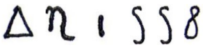


Additional information:

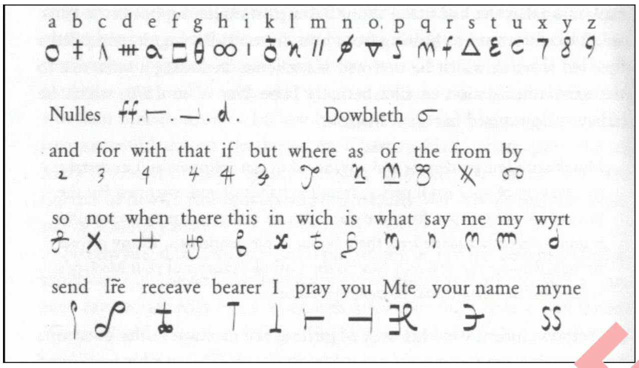


Ans: a----t

6. Solve Mary's cipher:



Additional information:



a b c d e f g h i k l m n o p q r s t u x y z

Nulles Dowbleth

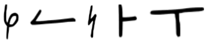
and for with that if but where as of the from by

so not when there this in wich is what say me my wyrt

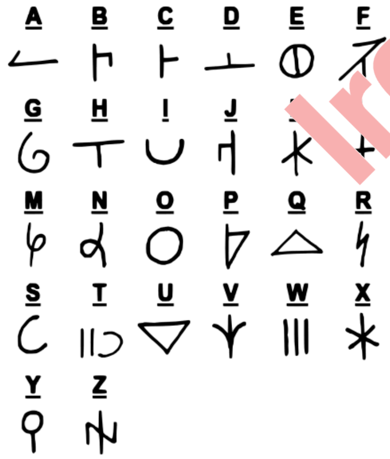
send lře receave bearer I pray you Mte your name myne

Ans: s----y

7. Solve the Dscript cipher:

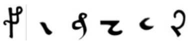


Additional information:

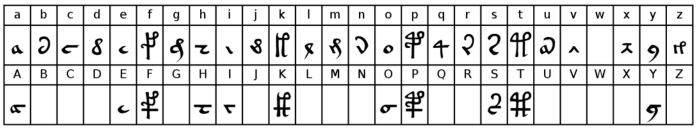


Ans: m---h

8. Solve the Voynich cipher:

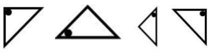


Additional information:

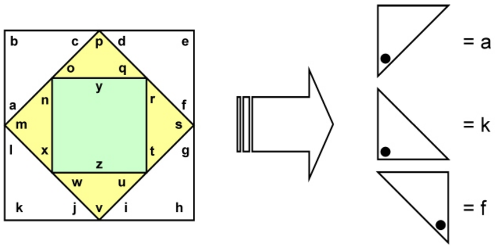

a b c d e f g h i j k l m n o p q r s t u v w x y z
A B C D E F G H I J K L M N O P Q R S T U V W X Y Z

Ans: f----r

9. Solve the three-square cipher:



Additional information:



Ans: b--e

10. Solve the gold bug cipher to recover the plaintext: ;6*708

Additional information:

The Gold-Bug cipher was included in a short story by Edgar Allan Poe and which was published in 1843. It tells the tale of William Legrand and how he w

```
abcdefghijklmnopqrstuvwxyz
52-†81346,709*‡.$();?¶]¢:[
```

In the book he writes:

Here Legrand, having re-heated the parchment, submitted it to my inspection. The following characters were rudely traced, in a red tint, between the de

```
53‡‡†305))6*;4826)4‡.)4‡);806*;48†8¶60))85;1‡(;:‡*8†83(88)5*†;
46(;88*96*?;8)*‡(;485);5*†2:*‡(;4956*2(5*—4)8¶8*;4069285);)6†8
)4‡‡;1(‡9;48081;8:8‡1;48†85;4)485†528806*81(‡9;48;(88;4(‡?
34;48)4‡;161;:188;‡?;
```

This is translated as:

5	-	A
3‡‡†	-	good
305))	-	glass
6*	-	in
;48	-	the

Ans: t----e

11. Solve the ADFGVX cipher to find the plaintext of: AD VV DG FG XD VD V[illegible]V

Additional information:

	A	D	F	G	V	X
A	8	p	3	d	1	[illegible]
D	l	t	4	o	a	[illegible]
F	7	k	b	c	5	z
G	j	u	6	w	[illegible]	[illegible]
V	x	s	v	i	r	[illegible]
X	9	e	y	0	[illegible]	q

Ans: p-------r

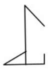
12. What is the plain text for the following Bac[illegible]iphe[illegible]ABBB AA[illegible]AAAA AAABB

Additional information:

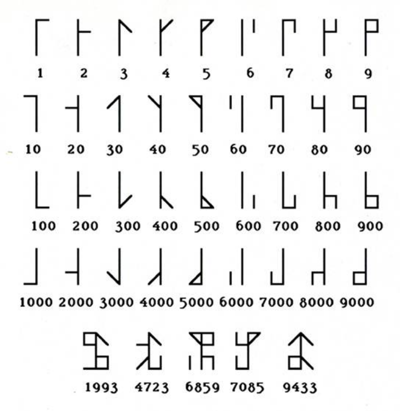
a	AAAAA	g	AABBA	n	ABBAA	t	BAABA
b	AAAAB	h	AABBB	o	ABBAB	u-v	BAABB
c	AAABA	i-j	ABAAA	p	ABBBA	w	BABAA
d	AAABB	k	ABAAB	q	ABBBB	x	BABAB
e	AABAA	l	ABABA	r	BAAAA	y	BABBA
f	AABAB	m	ABABB	s	BAAAB	z	BABBB

Ans: h--d

13. Solve the Monk cipher:



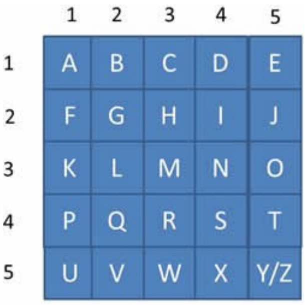
Additional information:



Ans: 5--3

14. What is the plain text for the following Polybius cipher: 24 34 45 15 43 34 15 45

Additional information:



	1	2	3	4	5
1	A	B	C	D	E
2	F	G	H	I	J
3	K	L	M	N	O
4	P	Q	R	S	T
5	U	V	W	X	Y/Z

Ans: i------t

15. What is the plain text for the Dvorak cipher of: X.AJD

Additional information:

```
Plain:  abcdefghijklmnopqrstuvwxyz
Cipher: axje.uidchtnmbrl'poygk,qf;
```

Ans: b---h

16. What is the Atbash cipher for the word: ZOKSZ

Additional information:

```
Plain:  abcdefghijklmnopqrstuvwxyz
Cipher: ZYXWVUTSRQPONMLKJIHGFEDCBA
```

Ans: a---a

17. What is the plain text for the Rot13 cipher of: PURRFR

Additional information:

```
Plain:  abcdefghijklmnopqrstuvwxyz
Cipher: NOPQRSTUVWXYZABCDEFGHIJKLM
```

Ans: c----e

18. What is the ROT47 cipher for: apessemisticpestexists

Additional information:

```
Plain:  abcdefghijklmnopqrstuvwxyz 1234567890!.:,;'
Cipher: 23456789:;<=>?@ABCDEFGHIJK `abcdefgh_P]i[jV
```

Ans: 2----------------------

19. What is the plaintext for the ROT47 cipher of: 32C<:?8FAE96HC@?8EC66

Additional information:

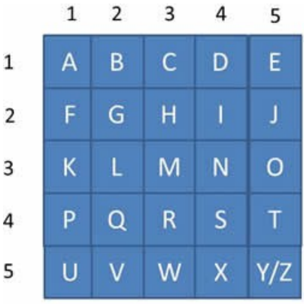
```
Plain:  abcdefghijklmnopqrstuvwxyz 1234567890!.:,;'
Cipher: 23456789:;<=>?@ABCDEFGHIJK `abcdefgh_P]i[jV
```

Ans: b-------------------e

20. What is the plain text for the following tap cipher: ... .

Additional information:

```
The tap cipher uses a Polybius mapping, and where we tap (.) out the row and then tap the column count:
```



	1	2	3	4	5
1	A	B	C	D	E
2	F	G	H	I	J
3	K	L	M	N	O
4	P	Q	R	S	T
5	U	V	W	X	Y/Z

```
For example:
.... ..... . . .... .... .... ..... . .....
 T          A   S         T          E
```

Ans: l----n

21. With a Caeser cipher, if we use either a 1 letter, 2 letter or 3 letter shift (as defined below), which is the plaintext for: RCUURQTV

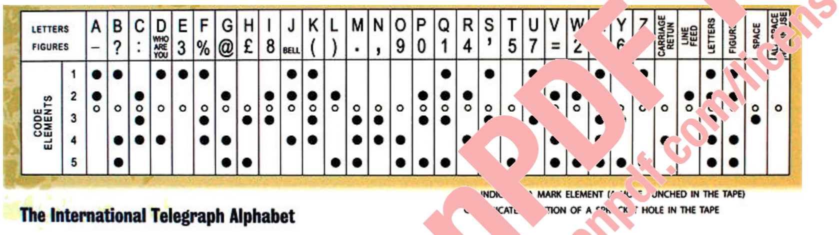
Additional information:

```
For a 1 letter shift:

abcdefghijklmnopqrstuvwxyz
BCDEFGHIJKLMNOPQRSTUVWXYZA

for two shifts:

abcdefghijklmnopqrstuvwxyz
CDEFGHIJKLMNOPQRSTUVWXYZAB

and three shifts:

abcdefghijklmnopqrstuvwxyz
DEFGHIJKLMNOPQRSTUVWXYZABC
```

Ans: p------t

22. What the plaintext for the following Baudot code: 00101001101110010110100100000 1

Additional information:


LETTERS
FIGURES
CODE ELEMENTS
1
2
3
4
5
A B C D E F G H I J K L M N O P Q R S T U V W X Y Z
– ? : WHO ARE YOU 3 % @ £ 8 BELL ( ) . , 9 0 1 4 ' 5 7 = 2 6
CARRIAGE RETURN
LINE FEED
LETTERS
FIGURES
SPACE
ALL SPACE NOT IN USE
INDICATES MARK ELEMENT PUNCHED IN THE TAPE
INDICATES POSITION OF A SPROCKET HOLE IN THE TAPE

The International Telegraph Alphabet

```
The coding is:

0     1   2     3    4    5    6    7   8     9
'*' 'E' '\n'  'A'  ' '  'S'  'I'  'U' '\r'  'D'

10   11   12  13  14  15  16  17  18
'R'  'J' 'N' 'F' 'C' 'K' 'T' 'Z' 'L'

20   21  22   23   24   25   26   27   28
'H' 'Y'  'P'  'Q'  'O'  'B'  'G'  ''   'M'  'X',

Binary           Letter  Figure
00000   Null   Null
00001   E     3
00010   LF     LF
00011   A     -
00100   ' '    ' '
00101   S     Bell
00110   I     8
00111   U     7
01000   CR    CR
01001   D
01010   R     4
01011   J     '
01100   N     ,
01101   F     !
01110   C     :
01111   K     (
10000   T     5
10001   Z     "
10010   L     )
10011   W     2
10100   H     #
10101   Y     6
10110   P     0
10111   Q     1
11000   O     9
11001   B     ?
11010   G     &
11011   Shift to figures
11100   M     .
11101   X     /
11110   V     ;
11111       Shift to letters
```

Ans: s----e

23. For the scrambled alphabet given below, which is the plaintext for the cipher of: CTOPZA

Additional information:

```
Plain:  abcdefghijklmnopqrstuvwxyz
Cipher: TUCSZBMDLXHKEGWPYOQAVNRJFI
```

Ans: c----t

24. For the following Morse code, what is the plaintext: (—) (·—) (···) (—) (·)

Additional information:

```
A(·—) B(—···)
C(—·—·) D(—··)
E(·) F(··—·)
G(— —·) G(····)
I(··) J(·— — —)
K(—·—) L(·—··)
M(— —) N(—·)
O(— — —) P(·— —·)
Q(— —·—) R(·—·)
S(···) T(—)
U(··—) V(···—)
W(·— —) X(—··—)
Y(—·— —) Z(— —··)
```

Ans: t---e

25. A homomorphic cipher uses several codes for each plaintext character. For the homomorphic cipher given below, which is the plaintext for the cipher of: 81 69 08 78

Additional information:

```
a  b  c  d  e  f  g  h  i  j  k  l  m  n  o  p  q  r  s  t  u  v  w  x  y  z
07 11 17 10 25 08 44 19 02 18 41 42 40 00 16 01 15 04 06 05 13 22 45 12 55 47
31 64 33 27 26 09 83 20 03       81 52 43 30 62    24 34 23 14    46    93
50    49 51 28       21 29       86    80 61       39 56 35 36
63       76 32       54 53       95    88 65       58 57 37
66          48       70 68             89 91       71 59 38
77          67       87 73                94       00 90 60
84          69                            96             74
            72                                           78
            75                                           92
            79
            82
            85
```

Ans: l--t

26. For the keyword cipher, for a cipher word (and key word of "ANKLE") determine the plaintext: sl[illegible]ar[illegible]

Additional information:

```
The following uses a keyword of Krytos, and a message of "knowledgeispower". Here, and it would give DGHVETPSTBMIHVTL.

Plaintext:   A B C D E F G H I J K L M N O P Q R S T U V W X Y Z
Encrypted:   K R Y P T O S A B C D E F G H I J L M N Q U V W X Z

With KRYPTOS as the keyword, all As become Ks, all Bs become Rs and so on. Encrypting the message "knowledge is power" using the keyword "kryptos":

Plaintext:   K N O W L E D G E I S P O W E R
Encoded:     D G H V E T P S T B M I H V T L
```

Ans: s------d

27. For the Bifid cipher, for a cipher word of the following determine the plaintext: poenm

Additional information:

```
First we start with a grid:

  1 2 3 4 5
1 B G W K Z
2 Q P N D S
3 I O A X E
4 F C L U M
5 T H Y V R

Next we look up the grid, and the arrange the two character values into two rows. For example is we have a plaintext of "marylan", then "m" is "4" and

maryland
43554322
53533334

Next we read along the rows and merge, to give:

43 55 43 22 53 53 33 34

Next we convert them back to letters from the grid:

L R L P Y Y A X

Let’s try the reverse, with DXETE. For we look up the grid to get:

24 34 35 51 35

We can then put then into rows to give:

2 4 3 4 3
5 5 1 3 5

This gives us 25 (s) 45 (m), 31 (i) 43 (l) 35 (e) - which is smile.
```

Ans: s---e

28. What is gray cipher code for the value of 4?

Additional information:

```
With a Gray cipher each binary value in a sequence differs by just one bit. Take a value of i, and calculatoe i EX-OR (i >> 1), and where >> is a shift

i     0100
EX-OR 0010
      ----
      0110
```

Ans: 1-0

29. Bob and Alice are using a secret cipher key generated from the first row of a Sudoku puzzle. Can you find the secret cipher key from this:

```
0 0 0 0 8 4 0 3 0
0 0 0 5 1 0 0 0 7
0 8 9 0 0 0 0 4 0
0 0 0 0 0 0 2 0 8
0 6 0 2 0 1 0 5 0
1 0 2 0 0 0 0 0 0
0 7 0 0 0 0 5 2 0
9 0 0 0 6 5 0 0 0
0 4 0 9 7 0 0 0 0
```

Ans: 7---------------2

30. For the following Straddling cipher, what is the plain text: 3 63 22 8 4

Additional information:

```
  0  1  2  3  4  5  6  7  8  9
   E  T     A  O  N     R  I  S
2  B  C  D  F  G  H  J  K  L  M
6  P  Q  /  U  V  W  X  Y  Z  .
```

Ans: a---o

31. For the follow cipher, we use a 3-rail code (an example given below). Which is the plaintext for the following 3-rail cipher code: SGNHW RUDOO

Additional information:

```
'WE ARE DISCOVERED. FLEE AT ONCE', gives:

W . . . E . . . C . . . R . . . L . . . T . . . E
. E . R . D . S . O . E . E . F . E . A . O . C .
. . A . . . I . . . V . . . D . . . E . . . N . .

to give:

WECRL TEERD SOEEF EAOCA IVDEN
```

Ans: s--------d

32. The Pollux cipher, we use Morse code (see below) to determine a code (see below). Which is the plaintext for the following Pollux cipher: 7890097879887277752503

Additional information:

```
To determine a code, and then map a dot, dash or seperator with the following:
Dot - 0, 7 or
Dash - 1, 8 or 5
Seperator - 2, 9, 6 or 3
If we take a code of "784067897459184640779", we can determine the following:
784067897459184640779
.-.. .- ..- --. ....
L    A  U   G   H

For example "GE" becomes "— — ·" and "·", so we can then encode to 1 [illegible] 2 7 [illegible] to give 1[illegible]79.
Morse code:
A(·—)
B(—···
C(—·—·)
D(—··)
E(·)
F(··—·)
G(— —·)
H(····)
I(··)
J(·— — —)
K(—·—)
L(·—··)
M(— —)
N(—·)
O(— — —)
P(·— —·)
Q(— —·—)
R(·—·)
S(···)
T(—)
U(··—)
V(···—)
W(·— —)
X(—··—)
Y(—·— —
Z(— —··)
```

Ans: a----n

33. The following Fractional cipher (see below), determine the plaintext: JGQDWQI

Additional information:

```
"Hello World" is Morse Code is:

.... . .-.. .-.. --- /      .-- --- .-. .-.. -..
H    E  L    L   O  SPACE    W  O   R   L    D

We can then make this into a string with an 'x' between characters:

Plain text:    H    e l    l    o    w   o   r   l    d
Morse string:  ....x.x.-..x.-..x---xx.--x---x.-.x.-..x-..

We can now use three-character mappings to convert them back to text:

['...', '..-', '..x', '.-.', '.--', '.-x', '.x.', '.x-', '.xx', '-..', '-.-', '-.x', '--.', '---', '--x', '-x.', '-x-','-xx', 'x..', 'x.-', 'x.x', 'x-.


This mapping is:

A B C D E F G H I J K L M N O P Q R S T U V W X Y Z
. . . . . . . . . - - - - - - - - - x x x x x x x x
. . . - - - x x x . . . - - - x x x . . . - - - x x
. - x . - x . - x . - x . - x . - x . - x . - x . -
```

```
which will map to "ABCDEF...Z". Next we can convert them back with:

AGTCDHOTQODTCJ

For "Peter piper picked " we get:

.--.x.x-x.x.-.xx.--.x..x.--.x.x.-.xx.--.x..x-.-.x-.-x.x-..xx
P   e t e r ' ' p   i   p  e  r' ' p   i  c   k  e  d' '

Standard Morse code

E .   S ...  H ....  B -...  1 .----  period  .-.-.-
T -   U ..-  V ...-  X-..-   2 ..---  comma   --..--
I ..  R .-.  F ..-.  C-.-.   3 ...--  query   .-.-.-
A .-  W .--  L .-..  Y --.-  4 ....-  colon   ---...
N -.  D -..  P .--.  Z --..  5 .....  s/colon -.-.-.
M --  K -.-  J .---  Q --.-  6 -....  dash    -....-
      G --.                  7 --...  slash   -..-.
      O ---                  8 ---..  equals  -...-
                             9 ----.
                             0 -----
```

Ans: b---n

34. With the column cipher we lay our plain text in columns, and then use a column key, and reconstruct the columns: Using key of 21430, what is the plaintext for "bgo dra eulwnhg igs "

Additional information:

```
With the column cipher we lay our plain text in columns, and then use a column key, and recontruct the colums. If we use an order of column 3, 1, 4, 2

31420
-----
which
wrist
watch
esare
swiss
wrist
watch
es

We now rearrange the columns back in order:

  0    1    2    3    4
['h', 'h', 'c', 'w', 'i']
['t', 'r', 's', 'w', 'i']
['h', 'a', 'c', 'w', 't']
['e', 's', 'r', 'e', 'a']
['s', 'w', 's', 's', 'i']
['t', 'r', 's', 'w', 'i']
['h', 'a', 'c', 'w', 't']
[' ', 's', ' ', 'e', ' ']

The result is then:

Cipher: hthesth hraswrascscrssc wwweswweiitaiit
```

Ans: e-------------w

35. Find 10 cipher related words in this grid:

```
n i e k x b i f m b x q y a
h h o w g z d r q j t h l g
t o h e x a d e c i m a l v
m h c d g j w n b t o e d l
o c c s x f m i e e c s e p
r a o c u i m d z m t t c t
s e m r i b p w b p a g r [illegible]
e s p i w k h k s l l c y y
c a u p b r s d z a w d p g
o r t t f r e k m r w i t p
d x e n c r y p t i o n i o
e n r u s u p j c n m d o l
q s n v q t h e y b s j n m
d d f c i p h e r h b g d z
```

Ans: c---l

36. Find 15 cipher related words in this grid:

```
a u q m c m p o p n i b b l e s f u
k a v w a r o s s b o b v y b x j m
m r a l o u y r z y h z r r p j k v
c l i r t b s p s f r x u a y f c r
r c u s y z a o t e v c i n t j q o
e i t m k z f h v o c u m i c u e c
m l b j w v d z o f g o j b c b f t
a a t j y r v d a u e r d c d i g a
d m k z m w n q n f p v a e w y u l
u i t t s c r a m b l e d p n n b t
w c y u d i r v t q d b v e h n d s
c e t c s e l e g q e v p a z y l i
u d c r d p b n s a n g s e s r o y
d a k o r a e v i o i e h m a c g l
r x c q h c o w z p t b f b y h i t
k e f p t d p c t y f l c i b t w i
d h l p t f n s b h t s h i x o j a
h a v t j a j j c w n a a v e l t g
```

Ans: m--e

37. What is the Four Square cipher for the plaintext of: retina

Additional information:

It uses four 5x5 matrices arranged in a square. Each matrices contains 25 letters. The upper-left and lower-right matrices are the "plaintext squares"

First we break the message into bigrams, such as ATTACK AT DAWN gives:

AT TA CK AT DA WN

We now uses the four 'squares' and locate the bigram to encrypt in the plain alphabet squares. With 'AT', we take the first letter from the top left sq

```
    a b c d e   Z G P T F
    f g h i k   O I H M U
    l m n o p   W D R C N
    q r s t u   Y K E Q A
    v w x y z   X V S B L

    M F N B D   a b c d e
    C R H S A   f g h i k
    X Y O G V   l m n o p
    I T U E W   q r s t u
    L Q Z K P   v w x y z
```

Now, like Playfair, determine the the characters in the ciphertext around the corners of the rectangle for 'AT' and this makes:

```
    a b c d e   Z G P T F
    f g h i k   O I H M U
    l m n o p   W D R C N
    q r s t u   Y K E Q A
    v w x y z   X V S B L

    M F N B D   a b c d e
    C R H S A   f g h i k
    X Y O G V   l m n o p
    I T U E W   q r s t u
    L Q Z K P   v w x y z
```

And so we pick off 'TI'

The result becomes:

```
    ATTACKATDAWN
    TIYBFHTIZBSY
```

Ans: A------

38. The exponential cipher uses the form of Cipher=M^e mod N. Calulate the cipher values for the following: Message=[illegible]23, N=379 e=7

Additional information:

If we have a message of 1234, and an e value of 7 with an N value of 33, we get:

Cipher=12347 mod 33

Cipher=7;

The mod operator is the remainder after an integer division. Let’s [illegible] G [illegible] N=7

Bob and Alice generate random numbers (x and y):

X = 3
Y = 4

Bob calculates A:

A=G^x mod N=4^3 mod 7=64 mod 7= 1

Alice calculates B:

B=G^y mod N= 4^4 mod 7= 256 mod 7=4

They swap values and they generate the key.

KeyBob=B^x mod N=4^3 mod 7=256 mod 7=1

KeyAlice=A^y mod N=1^4 mod7=1 mod7=1

This is their shared key: "1"

Ans: 2-8

39. The Diffie Hellman method allows Bob and Alice to exchange values and end up with the same result. Calculate the shared value for: G=1201, N=7687, x=7, y=12

Additional information:

In Diffie-Hellman, Bob and Alice agree on G (a generator) and N (a prime number), and then Bob picks a random value of x, and Alice picks a random valu
Bob (x) Alice (y)
b=G^x mod N
 a=G^y mod N
Bob sends Alice the value of b Alice sends Bob the value of a
Key=a^x mod N
 Key=b^y modN

Ans: 7--4

40. Create the cipher for a multiplication cipher with a plaintext of: finland (with multiplier of 3)

Additional information:

This cipher uses multiplication cipher theory. In this case we take each letter (P) and multiply it by a value (a). For example "c" becomes 2, and mult

C=(a x P) mod 26

Where P is the character in the plain text, and a is the multiplier. The mod operator is the remainder from an integer divide (for example 11 mod 4 giv

Ans: p-----j

41. The LZ coding scheme is especially suited to data which has a high degree of repetition, and makes back references to these repeated parts. Typically a flag is normally used to identify coded and unencoded parts, where the flag creates back references to the repeated sequence. With the LZ table given below, solve the following: 'P', 'i', 'c', 'k', 'y', ' ', 'p', 'e', 'o', 'p', 'l', 'e', 261, 257, 'k', ' ', 'P', 'e', 't', 'e', 'r', 271, 'a', 'n', 271, 'e', 278, 'u', 't', '-', 'B', 283, 274, 'r', ',', ' ', 't', 'i', 's', 291, 'h', 267, 262, 282, 284, 'b', 287, 275, 294, 'p', 269, 260, 262, 264, 266, 268, 258 (use Table 2 below)

Additional information:

```
The following is the LZ Coding Table 1:

[256] Co
[257] ow
[258] ws
[259] s
[260]  g
[261] gr
[262] ra
[263] az
[264] ze
[265] e
[266]  i
[267] in
[268] n
[269]  gr
[270] ro
[271] ov
[272] ve
[273] es
[274] s o
[275] on
[276] n g
[277] gra
[278] as
[279] ss
[280] s w
[281] wh
[282] hi
[283] ic
[284] ch
[285] h
[286]  gro
[287] ows
[288] s i
[289] in
[290]  groo
[291] ove
[292] es
[293]  a
[294] an
[295] n gr
[296] rov
[297] ves

The following is LZ Coding Table 2:

[256] Pi
[257] ic
[258] ck
[259] ky
[260] y
[261]  p
[262] pe
[263] eo
[264] op
[265] pl
[266] le
[267] e
[268]  pi
[269] ick
[270] k
[271]  P
[272] Pe
[273] et
[274] te
[275] er
[276] r
[277]  Pa
[278] an
[279] n
[280]  Pe
[281] ea
[282] anu
[283] ut
[284] t-
[285] -B
[286] Bu
[287] utt
[288] ter
[289] r,
[290] ,
[291]  t
[292] ti
[293] is
[294] s
[295]  th
[296] he
[297] e p
[298] pea
[299] anut
[300] t-b
[301] bu
[302] utte
[303] ers
[304] s p
[305] pi
[306] icky
[307] y p
[308] peo
[309] opl
[310] le
[311]  pic

Example

In he example above, we have:

Input:  Cows graze in groves on grass which grows in grooves in groves

Compressed:
['C', 'o', 'w', 's', ' ', 'g', 'r', 'a', 'z', 'e', ' ', 'i', 'n', 260, 'r', 'o', 'v', 'e', 259, 'o', 268, 261, 'a', 's', 259, 'w', 'h', 'i', 'c', 'h',

Deompressed:
Cows graze in groves on grass which grows in grooves in groves
```

```
The first entry in the dictionary add position 256 will be 'Co', next it will be 'ow'. We can see that the following index values have been defined:

    The code ' g' has been defined with an index of 260.
    The code 's ' has been defined with an index of 259.
    268, 261 represents 'n ' and 'gr', representively.

The resulting dictionary entries that are added:

Adding: [256] Co
Adding: [257] ow
Adding: [258] ws
Adding: [259] s
Adding: [260]  g
Adding: [261] gr
Adding: [262] ra
Adding: [263] az
Adding: [264] ze
Adding: [265] e
Adding: [266]  i
Adding: [267] in
Adding: [268] n
Adding: [269]  gr
Adding: [270] ro
Adding: [271] ov
Adding: [272] ve
Adding: [273] es
Adding: [274] s o
Adding: [275] on
Adding: [276] n g
Adding: [277] gra
Adding: [278] as
Adding: [279] ss
Adding: [280] s w
Adding: [281] wh
Adding: [282] hi
Adding: [283] ic
Adding: [284] ch
Adding: [285] h
Adding: [286]  gro
Adding: [287] ows
Adding: [288] s i
Adding: [289] in
Adding: [290]  groo
Adding: [291] ove
Adding: [292] es
Adding: [293]  in
Adding: [294] n gr
Adding: [295] rov
Adding: [296] ves
```

Ans: P---k

42. Decode the following Huffman cipher for the plaintext: 0101101011011001110111110111011

Additional information:

```
Symbol  Weight  Huffman Code
        287     111
e       167     000
a       95      0101
i       110     1010
n       90      0100
o       106     0111
s       107     1001
t       116     1011
c       43      00101
d       50      01101
h       44      00110
l       70      11010
m       56      10001
p       44      00111
r       84      11011
u       47      01100
b       20      001000
f       23      001001
g       28      110000
y       26      100001
,       18      1100110
.       15      1100010
k       17      1100101
v       15      1100011
w       18      1100111
0       8       11001000
1       6       10000001
'       5       110010011
-       3       100000001
3       3       100000100
?       3       100000101
x       4       110010010
2       2       1000001101
5       2       1000001111
9       1       1000000000
j       1       1000000001
(       1       10000011000
)       1       10000011001
4       1       10000011100
6       1       10000011101

For example "hello" will be coded as:

00110 000 11010 11010 0111

and as a bit stream:

0011000011010110100111
```

Ans: a-----t

43. With this OTP we EX-OR the message with a one-time key (see below). Calculate the hex values for the following cipher: Word: accident Key: connection

Additional information:

```
If we take a message of "hello" and a key of "goodbye", we get:

hello    01101000 01100101 01101100 01101100 01101111
```

```
goodbye  01100111 01101111 01101111 01100100 01100010 01111001 01100101
```

Now if we EX-OR them we get:

```
01101000 01100101 01101100 01101100 01101111
01100111 01101111 01101111 01100100 01100010
--------------------------------------------
00001111 00001010 00000011 00001000 00001101
0   f    0   a    0   3    0   8    0   d
```

So the result is 0f0a03080d
Binary values

To help you, here are a list of binary values:

a	chr(97)	01100001
b	chr(98)	01100010
c	chr(99)	01100011
d	chr(100)	01100100
e	chr(101)	01100101
f	chr(102)	01100110
g	chr(103)	01100111
h	chr(104)	01101000
i	chr(105)	01101001
j	chr(106)	01101010
k	chr(107)	01101011
l	chr(108)	01101100
m	chr(109)	01101101
n	chr(110)	01101110
o	chr(111)	01101111
p	chr(112)	01110000
q	chr(113)	01110001
r	chr(114)	01110010
s	chr(115)	01110011
t	chr(116)	01110100
u	chr(117)	01110101
v	chr(118)	01110110
w	chr(119)	01110111
x	chr(120)	01111000
y	chr(121)	01111001
z	chr(122)	01111010

With hex values, we take four bits at a time and convert the values:

0000	0
0001	1
0010	2
0011	3
0100	4
0101	5
0110	6
0111	7
1000	8
1001	9
1010	A
1011	B
1100	C
1101	D
1110	E
1111	F

Ans: 0--------------d

44. For the following jump cipher with jump of 4 (see below), what is the plaintext: gobeody (Jump: 2)

Additional information:

If we have a skip of 3, then:

The social network said its members had expressed concerns that they were missing 'important updates' from the people they cared about.

becomes:

T cleo ii mrh psdoesh eweii mrnuasfmhpp eceauT cleo ii mrh psdoesh eweii mrnuasfmhpp eceauT cleo ii mrh psdoesh eweii mrnuasfmhpp eceau

For example if we have plain text of "01234567", with a jump of 3 we get:

03614725

Now we take "epnlhtea", and match:

```
03614725
epnlhtea
```

Let's take the first three charactersof 0, 1 and 2, which are e, l and e:

eleXXXX

Next 3, 4 and 5, which are p, h and a:

elephaXX

Finally for 6 and 6, which are n and t

elephant

Ans: g-----e

45. What is the Affine cipher for the word: accident [a=3, b=6]

Additional information:

The Affine cipher uses a mathematical formula to encrypt, such as for a linear equation of E(x)=(ax+b). If we use a 26 letter alphabet the operation be

```
A B C D E F G H I J K L M N O P Q R S T U V W X Y Z
0 1 2 3 4 5 6 7 8 9 10 11 12 13 14 15 16 17 18 19 20 21 22 23 34 25
```

Example

We can use any value of b (apart from 1), but a should not share a factor with 26 (this is defined as being co-prime). Thus a can be 1, 3, 5, 7, 9, 11,

The following is taken from Wikipedia:

```
plaintext  A  F  F  I  N  E  C  I  P  H  E  R
x  0  5  5  8  13  4  2  8  15  7  4  17
```

Now, take each value of x, and solve the first part of the equation, (5x + 8). After finding the value of (5x + 8) for each character, take the remaind

```
plaintext  A  F  F  I  N  E  C  I  P  H  E  R
```

```
x  0  5  5  8  13  4  2  8  15  7  4  17
(5x + 8)  8  33  33  48  73  28  18  48  83  43  28  93
(5x + 8) mod 26  8  7  7  22  21  2  18  22  5  17  2  15
```

```
The final step in encrypting the message is to look up each numeric value in the table for the corresponding letters. In this example, the encrypted te
plaintext  A  F  F  I  N  E  C  I  P  H  E  R
x  0  5  5  8  13  4  2  8  15  7  4  17
(5x + 8)  8  33  33  48  73  28  18  48  83  43  28  93
(5x + 8) mod 26  8  7  7  22  21  2  18  22  5  17  2  15
ciphertext  I  H  H  W  V  C  S  W  F  R  C  P
```

```
The cipher is generally weak as it is a monoalphabet and doesn't use a key. Overall there are 12 possible values of a (1, 3, 5, 7, 9, 11, 15, 17, 19, 2
```

Ans: g-----l

46. Find the next value: 4, 5, 9, 14, 23, 37 ...

Ans: 60

47. Find the next value: 13, 29, 61, 125, 253, 509, ...

Ans: 1--1

48. Find the next value: d, i, n, s, x, c, ...

Ans: h

49. What is next value in sequence of 6, 15, 35, 77, 143, ...

Additional information:

```
Hint: think of prime numbers
```

Ans: 2-1

50. What is next value in sequence of 01, 06, 0B, 10, 15, ...

Additional information:

```
Hint: think of hex numbers
```

Int	Hex
0	00
1	01
2	02
3	03
4	04
5	05
6	06
7	07
8	08
9	09
10	0A
11	0B
12	0C
13	0D
14	0E
15	0F

Ans: 1A

51. What is next value in sequence of 4, 6, 10, 12, 14, ...

Additional information:

```
Hint: think of octal numbers
```

Int	Oct
0	00
1	01
2	02
3	03
4	04
5	05
6	06
7	07
8	10
9	11
10	12
11	13
12	14
13	15
14	16
15	17

Ans: 16

52. Find the next value. Enter this as the equivalent Greek alphabet character (eg 'alpha' for 'α'): κ, ν, π, τ, χ, α, ...

Additional information:

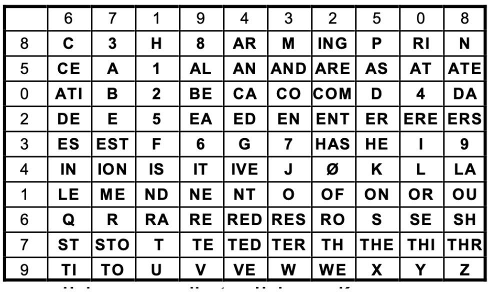
alpha	beta	gamma	delta	epsilon	zeta	eta	theta	iota	kappa	lambda	mu	nu	xi	omicron	pi	rho	sigma	tau	upsilon	phi	chi	psi	omega
α	β	γ	δ	ε	ζ	η	θ	ι	κ	λ	μ	ν	ξ	ο	π	ρ	σ	τ	υ	φ	χ	ψ	ω

Ans: d---a

53. What is plaintext for SYLLABARY cipher of: [71] [57] [65] [71] [27]

Additional information:

```
With the Syllabary cipher, we generate the row/column  coordinates  (CT) from:
```



	6	7	1	9	4	3	2	5	0	8
8	C	3	H	8	AR	M	ING	P	RI	N
5	CE	A	1	AL	AN	AND	ARE	AS	AT	ATE
0	ATI	B	2	BE	CA	CO	COM	D	4	DA
2	DE	E	5	EA	ED	EN	ENT	ER	ERE	ERS
3	ES	EST	F	6	G	7	HAS	HE	I	9
4	IN	ION	IS	IT	IVE	J	Ø	K	L	LA
1	LE	ME	ND	NE	NT	O	OF	ON	OR	OU
6	Q	R	RA	RE	RED	RES	RO	S	SE	SH
7	ST	STO	T	TE	TED	TER	TH	THE	THI	THR
9	TI	TO	U	V	VE	W	WE	X	Y	Z

Ans: t---e

54. Bob has hidden secret values for x in the equation x²-7x+10=0. Can you find the secret values?

Ans: 5-2

55. For a g value of 2 and a prime number of 59, what is next value in sequence of 2, 4, 8, 16, 32, 5, ...

Additional information:

```
For a ring in encryption, we create a g value and have a prime number of N. For values of x, we get g^x (mod N). For example if we use g=2 and N=42:
x  2^x (mod 59)
1 2
2 4
3 8
4 16
5 32
6 5
7 10
8 20
```

Ans: 10

56. For prime numbers of 67 and 47 and a seed of x0=8, what is next value in sequence of 64, 947, 2493, 2072, ...

Additional information:

```
The Blum Blum Shub (BBS) method is as pseudorandom number generator and was created by Lenore Blum, Manuel Blum and Michael Shub in 1968. It uses the f

x[n+1]=x[n]^2 (mod M)

and where x0 is a random seed. The value of M is equal to pq, and where p and q are prime numbers. Let's try a simple example in Python:

>>> p=7
>>> q=11
>>> M=p*q
>>> x0=5
>>> x1=(x0**2)%M
>>> x2=(x1**2)%M
>>> x3=(x2**2)%M
>>> x4=(x3**2)%M
>>> print (x1,x2,x3,x4)
25 9 4 16
```

Ans: 1--7

57. With a key of 'CRYPTOGRAM' and a starting shift of 10, what is Condi cipher of: right

Additional information:

```
First we start with the keyword ('CRYPTOGRAM') and layout the rest of the alphabet:

1  2  3  4  5  6  7  8  9  10 11 12 13
C  R  Y  P  T  O  G  A  M  B  D  E  F

14 15 16 17 18 19 20 21 22 23 24 25 26
H  I  J  K  L  N  Q  S  U  V  W  X  Z

For a message of  'On the first day I got lost.', we select an initial shift of 10.  We start with 'O' and then move 10 places to 'J'. Next we have an


plaintext:  On the first day I got lost.
ciphertext: JX WNZ XRKVZ JND L UFD VWCZ.
```

Ans: e-----

58. With a key of 'CRYPTOGRAM' and a starting shift of 10, what is plaintext for Condi cipher of: szrzrjvhv

Additional information:

```
First we start with the keyword ('CRYPTOGRAM') and layout the rest of the alphabet:

1  2  3  4  5  6  7  8  9  10 11 12 13
C  R  Y  P  T  O  G  A  M  B  D  E  F

14 15 16 17 18 19 20 21 22 23 24 25 26
H  I  J  K  L  N  Q  S  U  V  W  X  Z

For a message of  'On the first day I got lost.', we select an initial shift of 10.  We start with 'O' and then move 10 places to 'J'. Next we have an


plaintext:  On the first day I got lost.
ciphertext: JX WNZ XRKVZ JND L UFD VWCZ.
```

Ans: d-------t

59. With a key of '54312', what is AMSCO cipher of: tobeornottobethatisthequestion

Additional information:

```
For the AMSCO cipher, we take alternative two letter and one letter occurances, and then fit to a grid with a sequence key. For example, if we have  a
4  1  3  2   5
ap e  ss e  mi
```

```
s  ti c  pe  s
te x  is t  s
```

```
And thus is becomes 'e ti x e pe t ss c is a ps t em i s s'
, and so the cipher is 'etixepetsscisapstemiss'
```

Ans: r-----------------------------

60. With a key of '51423', what is AMSCO plaintext for the ciphertext version of: oasltlehewrntsstcal

Additional information:

```
For the AMSCO cipher, we take alternative two letter and one letter occurances, and then fit to a grid with a sequence key. With a key of '32415', what

X  X  X  X  X
2  1  2  1  2
1  2  1  2  1
2  1  2  1

First we lay out the key, and then populate the first column:

3  2  4  1  5
         n
         wr
         e

And now the next column:

3  2  4  1  5
   r     n
   th    wr
   t     e

And next:

3  2  4  1  5
ba r     n
p  th    wr
ng t     e

And next:

3  2  4  1  5
ba r  ki n
p  th e  wr
ng t  re e

And finally:

3  2  4  1  5
ba r  ki n  gu
p  th e  wr o
ng t  re e

And the result is "barkingupthewrongtree"
```

Ans: s-----------------s

61. For a NULL cipher of 'horrors bat adder prior pools', which is the plaintext?

Additional information:

```
In the NULL cipher we use the middle letter in each word. For example with the word 'radio', we can create a cipher of 'horrors bat adder prior pools'
```

Ans: r---o

62. What is the Vigenère cipher (see below) using a key of 'Kl[illegible]' for the word te[illegible]

Additional information:

```
The great advantage of this type of code is that the same plaintext  character will be encrypted with different values, depending on the position of th

Plain a b c d e f g h i j k l m n o p q r s t u v w x y z
1     b c d e f g h i j k l m n o p q r s t u v w x y z a
2     c d e f g h i j k l m n o p q r s t u v w x y z a b
3     d e f g h i j k l m n o p q r s t u v w x y z a b c
4     e f g h i j k l m n o p q r s t u v w x y z a b c d
5     f g h i j k l m n o p q r s t u v w x y z a b c d e
6     g h i j k l m n o p q r s t u v w x y z a b c d e f
7     h i j k l m n o p q r s t u v w x y z a b c d e f g
8     i j k l m n o p q r s t u v w x y z a b c d e f g h
9     j k l m n o p q r s t u v w x y z a b c d e f g h i
10    k l m n o p q r s t u v w x y z a b c d e f g h i j
11    l m n o p q r s t u v w x y z a b c d e f g h i j k
12    m n o p q r s t u v w x y z a b c d e f g h i j k l
13    n o p q r s t u v w x y z a b c d e f g h i j k l m
14    o p q r s t u v w x y z a b c d e f g h i j k l m n
15    p q r s t u v w x y z a b c d e f g h i j k l m n o
16    q r s t u v w x y z a b c d e f g h i j k l m n o p
17    r s t u v w x y z a b c d e f g h i j k l m n o p q
18    s t u v w x y z a b c d e f g h i j k l m n o p q r
19    t u v w x y z a b c d e f g h i j k l m n o p q r s
20    u v w x y z a b c d e f g h i j k l m n o p q r s t
21    v w x y z a b c d e f g h i j k l m n o p q r s t u
22    w x y z a b c d e f g h i j k l m n o p q r s t u v
23    x y z a b c d e f g h i j k l m n o p q r s t u v w
24    y z a b c d e f g h i j k l m n o p q r s t u v w x
25    z a b c d e f g h i j k l m n o p q r s t u v w x y
```

Ans: d--z

63. What is the Porta cipher for the following plaintext: CWEPKN

Additional information:

```
We take two characters at a time and use the following mapping:

 Keys| a b c d e f g h i j k l m n o p q r s t u v w x y z
 -------------------------------------------------------
 A,B | n o p q r s t u v w x y z a b c d e f g h i j k l m
 C,D | o p q r s t u v w x y z n m a b c d e f g h i j k l
 E,F | p q r s t u v w x y z n o l m a b c d e f g h i j k
 G,H | q r s t u v w x y z n o p k l m a b c d e f g h i j
 I,J | r s t u v w x y z n o p q j k l m a b c d e f g h i
 K,L | s t u v w x y z n o p q r i j k l m a b c d e f g h
 M,N | t u v w x y z n o p q r s h i j k l m a b c d e f g
 O,P | u v w x y z n o p q r s t g h i j k l m a b c d e f
 Q,R | v w x y z n o p q r s t u f g h i j k l m a b c d e
 S,T | w x y z n o p q r s t u v e f g h i j k l m a b c d
 U,V | x y z n o p q r s t u v w d e f g h i j k l m a b c
 W,X | y z n o p q r s t u v w x c d e f g h i j k l m a b
 Y,Z | z n o p q r s t u v w x y b c d e f g h i j k l m a
```

```
For example with a key of FORTIFICATION and a phase of "DEFENDTHEEASTWALLOFTHECASTLE", we get:

Plain text:    DEFENDTHEEASTWALLOFTHECASTLE
Cipher text:   SYNNJSCVRNRLAHUTUKUCVRYRLANY
Plain text:    DEFENDTHEEASTWALLOFTHECASTLE
```

Ans: r----a

64. A columnar transposition does a row-column transpose (see below). Calculate the ciphertext value for the following: Word: afoolandhismoneyaresoonparted, Key:GERMAN

Additional information:

```
The following is taken from http://practicalcryptography.com/ciphers/columnar-transposition-cipher/. First we use a key, such as "GERMAN", and where th

defend the east wall of the castle

We then write the message with the key word in the first row:

G E R M A N
d e f e n d
t h e e a s
t w a l l o
f t h e c a
s t l e

and then arrange alphabetically for the key word:

A E G M N R
n e d e d f
a h t e s e
l w t l o a
c t f e a h
  t s e   l

and then read the cipher from the columns down:

NALCEHWTTDTTFSEELEEDSOAFEAHL
```

Ans: L--------------------------T

65. What is the Beaufot cipher for the word: tickle [Key: apple]

Additional information:

```
We use a Vigenère method for the key, but change the method of resolving the ciphertext. For this we look along the top row for the plaintext letter, a

Plain a b c d e f g h i j k l m n o p q r s t u v w x y z
1     b c d e f g h i j k l m n o p q r s t u v w x y z a
2     c d e f g h i j k l m n o p q r s t u v w x y z a b
3     d e f g h i j k l m n o p q r s t u v w x y z a b c
4     e f g h i j k l m n o p q r s t u v w x y z a b c d
5     f g h i j k l m n o p q r s t u v w x y z a b c d e
6     g h i j k l m n o p q r s t u v w x y z a b c d e f
7     h i j k l m n o p q r s t u v w x y z a b c d e f g
8     i j k l m n o p q r s t u v w x y z a b c d e f g h
9     j k l m n o p q r s t u v w x y z a b c d e f g h i
10    k l m n o p q r s t u v w x y z a b c d e f g h i j
11    l m n o p q r s t u v w x y z a b c d e f g h i j k
12    m n o p q r s t u v w x y z a b c d e f g h i j k l
13    n o p q r s t u v w x y z a b c d e f g h i j k l m
14    o p q r s t u v w x y z a b c d e f g h i j k l m n
15    p q r s t u v w x y z a b c d e f g h i j k l m n o
16    q r s t u v w x y z a b c d e f g h i j k l m n o p
17    r s t u v w x y z a b c d e f g h i j k l m n o p q
18    s t u v w x y z a b c d e f g h i j k l m n o p q r
19    t u v w x y z a b c d e f g h i j k l m n o p q r s
20    u v w x y z a b c d e f g h i j k l m n o p q r s t
21    v w x y z a b c d e f g h i j k l m n o p q r s t u
22    w x y z a b c d e f g h i j k l m n o p q r s t u v
23    x y z a b c d e f g h i j k l m n o p q r s t u v w
24    y z a b c d e f g h i j k l m n o p q r s t u v w x
25    z a b c d e f g h i j k l m n o p q r s t u v w x y

For example if we have a message of 'hello" and a key of 'bike', we first take h and 'b':

Start with char (h)-↓
Plain a b c d e f g h
1     - - - - - - - i
2     - - - - - - - j
3     - - - - - - - k
4     - - - - - - - l
5     - - - - - - - m
6     - - - - - - - n
7     - - - - - - - o
8     - - - - - - - p
9     - - - - - - - q
10    - - - - - - - r
11    - - - - - - - s
12    - - - - - - - t
13    - - - - - - - u
14    - - - - - - - v
15    - - - - - - - w
16    - - - - - - - x
17    - - - - - - - y
18    - - - - - - - z
19    - - - - - - - a
20    u←-----------b ← Go down to key character (b)


Next we take 'e' and a key of 'i':

Char (e)------↓
Plain a b c d e
1     - - - - f
2     - - - - g
```

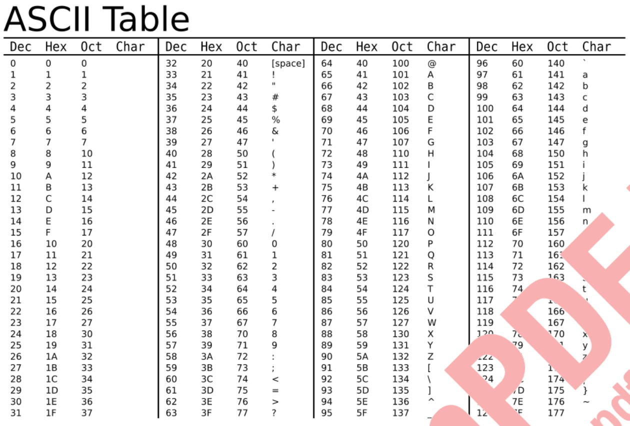
```
3     - - - - h
4     e←-----i  ← Go down to key character (i)


So that text of 'he' and a key of 'bi' will translate to a cipher text of 'ue'.
```

Ans: h----w

66. What is the XOR cipher for the cipher bitstream of (with a repeated key of 'a' - 0x61 or 0110 0001b): 00001001 00000100 00000000 00010011 00010101

Additional information:

```
The bitwise operation we use is Z=A XOR B:

A B Z
-----
0 0 0
0 1 1
1 0 1
1 1 0

If we use an 'a' (0110 0001) and plain text of "shape" we get:

          's'       'h'     'a'       'p'      'e'
Input:  01110011 01101000 01100001 01110000 01100101
Key:    01100001 01100001 01100001 01100001 01100001
---------------------------------------------------
Cipher  00010010 00001001 00000000 00010001 00000100

If we use an 'a' (0110 0001) again we get:

Input:  00010010 00001001 00000000 00010001 00000100
Key:    01100001 01100001 01100001 01100001 01100001
---------------------------------------------------
Decoded 01110011 01101000 01100001 01110000 01100101
          's'       'h'    'a'       'p'      'e'
```



ASCII Table

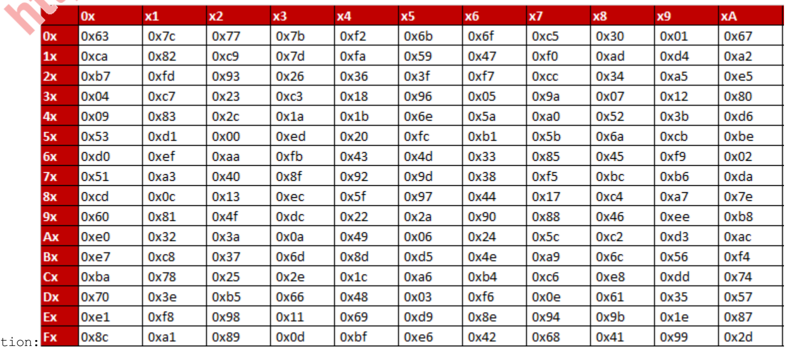
Dec	Hex	Oct	Char	Dec	Hex	Oct	Char	Dec	Hex	Oct	Char	Dec	Hex	Oct	Char
0	0	0		32	20	40	[space]	64	40	100	@	96	60	140	`
1	1	1		33	21	41	!	65	41	101	A	97	61	141	a
2	2	2		34	22	42	"	66	42	102	B	98	62	142	b
3	3	3		35	23	43	#	67	43	103	C	99	63	143	c
4	4	4		36	24	44	$	68	44	104	D	100	64	144	d
5	5	5		37	25	45	%	69	45	105	E	101	65	145	e
6	6	6		38	26	46	&	70	46	106	F	102	66	146	f
7	7	7		39	27	47	'	71	47	107	G	103	67	147	g
8	8	10		40	28	50	(	72	48	110	H	104	68	150	h
9	9	11		41	29	51	)	73	49	111	I	105	69	151	i
10	A	12		42	2A	52	*	74	4A	112	J	106	6A	152	j
11	B	13		43	2B	53	+	75	4B	113	K	107	6B	153	k
12	C	14		44	2C	54	,	76	4C	114	L	108	6C	154	l
13	D	15		45	2D	55	-	77	4D	115	M	109	6D	155	m
14	E	16		46	2E	56	.	78	4E	116	N	110	6E	156	n
15	F	17		47	2F	57	/	79	4F	117	O	111	6F	157	[illegible]
16	10	20		48	30	60	0	80	50	120	P	112	70	160	[illegible]
17	11	21		49	31	61	1	81	51	121	Q	113	71	161	[illegible]
18	12	22		50	32	62	2	82	52	122	R	114	72	162	[illegible]
19	13	23		51	33	63	3	83	53	123	S	115	73	163	[illegible]
20	14	24		52	34	64	4	84	54	124	T	116	74	[illegible]	t
21	15	25		53	35	65	5	85	55	125	U	117	[illegible]	[illegible]	[illegible]
22	16	26		54	36	66	6	86	56	126	V	118	[illegible]	166	[illegible]
23	17	27		55	37	67	7	87	57	127	W	119	[illegible]	167	[illegible]
24	18	30		56	38	70	8	88	58	130	X	120	78	170	x
25	19	31		57	39	71	9	89	59	131	Y	[illegible]	79	[illegible]	y
26	1A	32		58	3A	72	:	90	5A	132	Z	122	[illegible]	[illegible]	z
27	1B	33		59	3B	73	;	91	5B	133	[	123	[illegible]	[illegible]	[illegible]
28	1C	34		60	3C	74	<	92	5C	134	\	124	[illegible]	174	[illegible]
29	1D	35		61	3D	75	=	93	5D	135	]	[illegible]	7D	175	}
30	1E	36		62	3E	76	>	94	5E	136	^	[illegible]	7E	176	~
31	1F	37		63	3F	77	?	95	5F	137	_	127	7F	177	[illegible]

Ans: h---t

67. With many block ciphers we use an S-box mapping, where we take a value, and map it to another unique value. The S-box used in AES is given below. Use this to map the following data input value: 43D166A3

Additional information:

```
The following is the S-box mapping used in AES encryption:
```



	0x	x1	x2	x3	x4	x5	x6	x7	x8	x9	xA
0x	0x63	0x7c	0x77	0x7b	0xf2	0x6b	0x6f	0xc5	0x30	0x01	0x67
1x	0xca	0x82	0xc9	0x7d	0xfa	0x59	0x47	0xf0	0xad	0xd4	0xa2
2x	0xb7	0xfd	0x93	0x26	0x36	0x3f	0xf7	0xcc	0x34	0xa5	0xe5
3x	0x04	0xc7	0x23	0xc3	0x18	0x96	0x05	0x9a	0x07	0x12	0x80
4x	0x09	0x83	0x2c	0x1a	0x1b	0x6e	0x5a	0xa0	0x52	0x3b	0xd6
5x	0x53	0xd1	0x00	0xed	0x20	0xfc	0xb1	0x5b	0x6a	0xcb	0xbe
6x	0xd0	0xef	0xaa	0xfb	0x43	0x4d	0x33	0x85	0x45	0xf9	0x02
7x	0x51	0xa3	0x40	0x8f	0x92	0x9d	0x38	0xf5	0xbc	0xb6	0xda
8x	0xcd	0x0c	0x13	0xec	0x5f	0x97	0x44	0x17	0xc4	0xa7	0x7e
9x	0x60	0x81	0x4f	0xdc	0x22	0x2a	0x90	0x88	0x46	0xee	0xb8
Ax	0xe0	0x32	0x3a	0x0a	0x49	0x06	0x24	0x5c	0xc2	0xd3	0xac
Bx	0xe7	0xc8	0x37	0x6d	0x8d	0xd5	0x4e	0xa9	0x6c	0x56	0xf4
Cx	0xba	0x78	0x25	0x2e	0x1c	0xa6	0xb4	0xc6	0xe8	0xdd	0x74
Dx	0x70	0x3e	0xb5	0x66	0x48	0x03	0xf6	0x0e	0x61	0x35	0x57
Ex	0xe1	0xf8	0x98	0x11	0x69	0xd9	0x8e	0x94	0x9b	0x1e	0x87
Fx	0x8c	0xa1	0x89	0x0d	0xbf	0xe6	0x42	0x68	0x41	0x99	0x2d

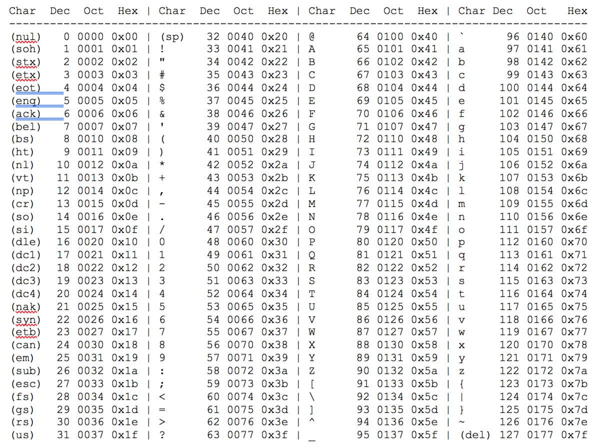
```
So:

230F27CC

becomes:

2676cc4b
```

Ans: l------a

68. An encode cipher table is given below. Determine the code for the following:: \141\x6e\u006b\154\x65\u0031\62\63

Additional information:

```
This is typically done for hex coding (\xZZ), 16-bit unicoding (\uZZZZ) and octal coding (\ZZZ).
```



```
Char  Dec  Oct   Hex | Char  Dec  Oct   Hex | Char  Dec  Oct   Hex | Char Dec  Oct    Hex
-------------------------------------------------------------------------------------------
(nul)   0 0000 0x00 | (sp)   32 0040 0x20 | @      64 0100 0x40 | `      96 0140 0x60
(soh)   1 0001 0x01 | !      33 0041 0x21 | A      65 0101 0x41 | a      97 0141 0x61
(stx)   2 0002 0x02 | "      34 0042 0x22 | B      66 0102 0x42 | b      98 0142 0x62
(etx)   3 0003 0x03 | #      35 0043 0x23 | C      67 0103 0x43 | c      99 0143 0x63
(eot)   4 0004 0x04 | $      36 0044 0x24 | D      68 0104 0x44 | d     100 0144 0x64
(enq)   5 0005 0x05 | %      37 0045 0x25 | E      69 0105 0x45 | e     101 0145 0x65
(ack)   6 0006 0x06 | &      38 0046 0x26 | F      70 0106 0x46 | f     102 0146 0x66
(bel)   7 0007 0x07 | '      39 0047 0x27 | G      71 0107 0x47 | g     103 0147 0x67
(bs)    8 0010 0x08 | (      40 0050 0x28 | H      72 0110 0x48 | h     104 0150 0x68
(ht)    9 0011 0x09 | )      41 0051 0x29 | I      73 0111 0x49 | i     105 0151 0x69
(nl)   10 0012 0x0a | *      42 0052 0x2a | J      74 0112 0x4a | j     106 0152 0x6a
(vt)   11 0013 0x0b | +      43 0053 0x2b | K      75 0113 0x4b | k     107 0153 0x6b
(np)   12 0014 0x0c | ,      44 0054 0x2c | L      76 0114 0x4c | l     108 0154 0x6c
(cr)   13 0015 0x0d | -      45 0055 0x2d | M      77 0115 0x4d | m     109 0155 0x6d
(so)   14 0016 0x0e | .      46 0056 0x2e | N      78 0116 0x4e | n     110 0156 0x6e
(si)   15 0017 0x0f | /      47 0057 0x2f | O      79 0117 0x4f | o     111 0157 0x6f
(dle)  16 0020 0x10 | 0      48 0060 0x30 | P      80 0120 0x50 | p     112 0160 0x70
(dc1)  17 0021 0x11 | 1      49 0061 0x31 | Q      81 0121 0x51 | q     113 0161 0x71
(dc2)  18 0022 0x12 | 2      50 0062 0x32 | R      82 0122 0x52 | r     114 0162 0x72
(dc3)  19 0023 0x13 | 3      51 0063 0x33 | S      83 0123 0x53 | s     115 0163 0x73
(dc4)  20 0024 0x14 | 4      52 0064 0x34 | T      84 0124 0x54 | t     116 0164 0x74
(nak)  21 0025 0x15 | 5      53 0065 0x35 | U      85 0125 0x55 | u     117 0165 0x75
(syn)  22 0026 0x16 | 6      54 0066 0x36 | V      86 0126 0x56 | v     118 0166 0x76
(etb)  23 0027 0x17 | 7      55 0067 0x37 | W      87 0127 0x57 | w     119 0167 0x77
(can)  24 0030 0x18 | 8      56 0070 0x38 | X      88 0130 0x58 | x     120 0170 0x78
(em)   25 0031 0x19 | 9      57 0071 0x39 | Y      89 0131 0x59 | y     121 0171 0x79
(sub)  26 0032 0x1a | :      58 0072 0x3a | Z      90 0132 0x5a | z     122 0172 0x7a
(esc)  27 0033 0x1b | ;      59 0073 0x3b | [      91 0133 0x5b | {     123 0173 0x7b
(fs)   28 0034 0x1c | <      60 0074 0x3c | \      92 0134 0x5c | |     124 0174 0x7c
(gs)   29 0035 0x1d | =      61 0075 0x3d | ]      93 0135 0x5d | }     125 0175 0x7d
(rs)   30 0036 0x1e | >      62 0076 0x3e | ^      94 0136 0x5e | ~     126 0176 0x7e
(us)   31 0037 0x1f | ?      63 0077 0x3f | _      95 0137 0x5f | (del) 127 0177 0x7f
```

Ans: a------3

69. The Beale Cipher is a modified Book Cipher, where we replace each letter in the message with a number. The book is given below: 78 150 13

Additional information:

The book is here (we have arranged in 10 lines each):

```
Still there are times I am bewildered by each mile
I have traveled, each meal I have eaten, each person
I have known, each room in which I have slept.
As ordinary as it all appears, there are times when
it is beyond my imagination. He stepped down, trying not
to look long at her, as if she were the
sun, yet he saw her, like the sun, even without
looking. It was times like these when I thought my
father, who hated guns and had never been to any
wars, was the bravest man who ever lived. There is
a loneliness that can be rocked. Arms crossed, knees drawn
up, holding, holding on, this motion, unlike a ships, smooths
and contains the rocker. Its an inside kind wrapped tight
like skin. Then there is the loneliness that roams. No
rocking can hold it down. It is alive. On its
own. A dry and spreading thing that makes the sound
of ones own feet going seem to come from a
far-off place. Jam, zebras, volts, xenon and queens
```

We start at zero. We move to the word for the number and take the first letter. For example "7 123 34 56 86" gives :"brain"

```
0     1     2    3     4 5  6          7    8    9
Still there are times I am bewildered by each mile
10 11  12        13   14   15  16 17    18   19
I have traveled, each meal I have eaten, each person
20 21  22     23   24   25 26    27 28  29
I have known, each room in which I have slept.
30 31      32 33 34
As ordinary as it all appears, there are times when
it is beyond my imagination. He stepped down, trying not
to look long at her, as if she were the
sun, yet he saw her, like the sun, even without
looking. It was times like these when I thought my
father, who hated guns and had never been to any
wars, was the bravest man who ever lived. There is
a loneliness that can be rocked. Arms crossed, knees drawn
up, holding, holding on, this motion, unlike a ships, smooths
and contains the rocker. Its an inside kind wrapped tight
like skin. Then there is the loneliness that roams. No
rocking can hold it down. It is alive. On its
own. A dry and spreading thing that makes the sound
of ones own feet going seem to come from a
far-off place. Jam, zebras, volts, xenon and queens
```

Ans: t-e

70. The GCD (Great Common Divisor) is used in many cryptography methods, and is determined by the latest divisor that goes into two numbers. For example, the GCD of 9 and 15 is 3. Find the GCD of the following: What is GCD of 57 and 24

Additional information:

The GCD of 15 and 12 is 3, as 3 is the largest divisor that can go into both of these values.

Ans: 3

71. What is the Delastelle cipher (and a key of "EPSDUCVWYM.ZLKXNBTFGORIJHAQ"): march

Additional information:

An example key is:

EPSDUCVWYM.ZLKXNBTFGORIJHAQ

We then make three squares from this:

```
square 1   square 2   square 3

  1 2 3      1 2 3      1 2 3
1 E P S    1 M . Z    1 F G O
2 D U C    2 L K X    2 R I J
3 V W Y    3 N B T    3 H A Q
```

If we take a plain text message of "THIS IS A TEST", we locate the text in the squares defined above:

```
THIS IS A TEST
--------------
```

```
T - 233
H - 331
I - 322
S - 113
I - 322
S - 113
A - 332
T - 233
E - 111
S - 113
T - 233
```

Next we would order as:

```
THISISATEST
-----------
23333132211
33221133322
33111113233
```

And we would read the code in a horizontal way to give:

```
233 333 321 321 311 111 331 233 232 123 123
```

And then substitute back the letters on the grid:

```
233 333 321 321 311 111 331 233 232 123 123
T   Q   R   R   F   E   H   T   B   C   C
```

Ans: K---F

72. What is the Nilist cipher for the plaintext of: course Key: iceland Add Key: apeman

Additional information:

This example is taken from Wikipedia. First we take our key (ZEBRAS) and create a Polybius square:

```
   1  2  3  4  5
1  Z  E  B  R  A
2  S  C  D  F  G
3  H  I  K  L  M
4  N  O  P  Q  T
5  U  V  W  X  Y
```

Next we take our plaintext of "DYNAMITE WINTER PALACE" (Plain Text - PT) and an additive key of "RUSSIAN". We then add the mappings from the square to

```
PT:  23  55   41  15  35  32  45  12  53   32  41  45  12  14  43  15  34  15  22  12
KEY: 14  51   21  21  32  15  41  14  51   21  21  32  15  41  14  51  21  21  32  15
CT:  37  106  62  36  67  47  86  26  104  53  62  77  27  55  57  66  55  36  54  27
```

The cipher is then 37 106 62 36 67 47 86 26 104 53 62 77 27 55 57 66 55 36 54 27
Example

With a key of "HELLO", a message of "WELCOME", with an additive key of "TEST":

```
  1 2 3 4 5
1 H E L O A
2 B C D F G
3 I K M N P
4 Q R S T U
5 V W X Y Z
```

First we convert the message:

```
PT:  W  E  L  C  O  M  E
    52 12 13 22 14 33 12
```

And then the additive key:

```
Add Key: T E  S  T
        44 12 43 44
```

Add: PT and Key

```
52 12 13 22 14 33 12
44 12 43 44 44 12 43
---------------------
96 24 56 66 58 45 55
```

The cipher text is 96245666584555

Ans: 2----------4

73. The Navajo cipher table is given below. What is the plaintext for this: Bi-sodih Gah Ne-ash-jsn Moashi Dzeh Dibeh Dibeh

Additional information:

Alphabets (English)	Code Language (English)	Code Language (Navajo)
A	Ant	Wol-la-chee
B	Bear	Shush
C	Cat	Moashi
D	Deer	Be
E	Elk	Dzeh
F	Fox	Ma-e
G	Goat	Klizzie
H	Horse	Lin
I	Ice	Tkin
J	Jackass	Tkele-cho-gi
K	Kid	Klizzie-yazzi
L	Lamb	Dibeh-yazzi
M	Mouse	Na-as-tso-si
N	Nut	Nesh-chee
O	Owl	Ne-ash-jsn
P	Pig	Bi-sodih
Q	Quiver	Ca-yeilth
R	Rabbit	Gah
S	Sheep	Dibeh
T	Turkey	Than-zie
U	Ute	No-da-ih
V	Victor	a-keh-di-glini
W	Weasel	Gloe-ih
X	Cross	Al-an-as-dzoh
Y	Yucca	Tsah-as-zih
Z	Zinc	Besh-do-gliz

Ans: p-----s

74. A cipher key is created by performing a binary multiplication (modulo 2). For these values, work out cipher key: 01000, 01110

Additional information:

```
GF(2) - Galois field of two elements - is used in many areas including with Checksums and Ciphers. The multiplication function involves multiplying the

   111
  x101
------
   111
  000
 111
 -----
 11011
 =====
```

Ans: 0---------

75. A cipher key is created by performing a binary divide (modulo 2). For these values, work out cipher key: 01110, 1000

Additional information:

```
GF(2) - Galois field of two elements - is used in many areas including with Checksums and Ciphers. It basically involves some bit shifts and an EX-OR f


      1110
    -------
11 | 10010
     11
     ------
      1010
      11
      -----
       110
       11
       ---
        00
```

Ans: 0--

76. An RSA cipher is 65871285245280396088309591448591 7595 and N= 8827853149904727578132487488611[illegible]69 . F[illegible] cra[illegible]ng N into p and q, decrypt cipher message.

Additional information:

```
Details [here].
First factorize N into p and q (here). This will give you p and q (the two prime numbe
Next we determine PHI=(p-1)(q-1).
Next we derive d (the decryption key value) from e and PHI.
Then decipher with Msg=C^d (pmod N).

Sample Python code:

from Crypto.Util.number import *
import gmpy2
import sys

p=954354002755510667
q=801297755486859913
c=607778777406675887172756406181993732
#N=764721720347891218098402268606191971


n = p*q
PHI=(p-1)*(q-1)

e=65537
d=(gmpy2.invert(e, PHI))

res=pow(c,d, n)

print "Cipher: ",c
print "p: ",p
print "q: ",q

print "=== Calc ==="
print "d=",d
print "n=",n
print "Decrypt: %s" % ((long_to_bytes(res)))
```

Ans: f-x

77. Can you crack the RSA Encrypted value with the following parameters:

e: 65537

N: 549868230204995606972768403233756993

Cipher: 826466344254274593047877684649979 41

We are using 60 bit primes

Additional information:

```
Details: [here]. Here is an example:

Encryption parameters
e: 65537
N: 1034776851837418228051242693253376923
Cipher: 582984697800119976959378162843817868
We are using  60 bit primes

Now we have to crack N by finding the primes that make up the value.

If we use this [link], we get:

Factors
-------
1,034,776,851,837,418,228,051,242,693,253,376,923 = 1,086,027,579,223,696,553 x 952,809,000,096,560,291
```

p=1,086,027,579,223,696,553 q=952,809,000,096,560,291

Now we work out PHI, which is equal to (p−1)×(q−1):

```
>>>p=1086027579223696553
>>>q=952809000096560291
>>> print (p-1)*(q-1)
1034776851837418226012406113933120080
```

Now we find e^−1 (mod PHI) (and where (d×e) (mod PHI)=1), such as using [link]:

```
Inverse of  65537  mod  1034776851837418226012406113933120080
Result: 568411228254986589811047501435713
```

This is the decryption key. Finally we decrypt with Message=Cipher^d (mod N):

```
>>> d=568411228254986589811047501435713
>>> cipher=582984697800119976959378162843817868
>>> N=1034776851837418228051242693253376923
>>> print pow(cipher,d,N)
345
```

The message is 345

Finally, let's check the answer. So we can recipher with the encryption key and we use Cipher=M^e (mod N):

```
>>> m=345
>>> e=65537
>>> N=1034776851837418228051242693253376923
>>> print pow(m,e,N)
582984697800119976959378162843817868
```

This is the same as the cipher, so the encryption and decryption keys have worked. Thus the encryption key is [65537, 1034776851837418228051242693253337

Ans: ---------->