VEGENERE CIPHER TEXT MODULE

|  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| 1 | 2 | 3 | 4 | 5 | 6 | 7 | 8 | 9 | 10 | 11 | 12 | 13 | 14 | 15 | 16 | 17 | 18 | 19 | 20 | 21 | 22 | 23 | 24 | 25 | 26 |
| 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 |
| Z | Y | X | W | V | U | T | S | R | Q | P | O | N | M | L | K | J | I | H | G | F | E | D | C | B | A |

|  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| 1 | 2 | 3 | 4 | 5 | 6 | 7 | 8 | 9 | 10 | 11 | 12 | 13 | 14 | 15 | 16 | 17 | 18 | 19 | 20 | 21 | 22 | 23 | 24 | 25 | 26 |
| 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 |
| 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 |
| 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 |
| 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 |
| 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 |
| 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 |
| 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 |
| 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 |
| 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 |
| 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 |
| 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 |
| 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 |
| 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 |
| 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 |
| 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 |
| 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 |
| 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 |
| 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 |
| 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 |
| 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 |
| 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 |
| 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 |
| 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 |
| 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 |
| 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 |
| 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 |

ATBASH CIPHER

Transposition Rail Fence Cipher

Plain Text: "WELCOME TO MY SESSION"

W L O E O Y E S O

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

E C M T M S S I N

Cipher Text: WLOEOYESOECMIMSSIN

Row Transposition Cipher

Plain Text: "WELCOME TO MY SESSION"

KEY:32541(Unique numbers should be considered and from 0 to 9)

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| 3 | 2 | 4 | 5 | 1 |
| W | E | L | C | O |
| M | E | T | O | M |
| Y | S | E | S | S |
| I | O | N | X | Y |

Cipher Text: OMSYEESOWMYILTENCOSX

Play Fair Cipher

Rules:

* First make a table of 5x5 and fill the table with letter of key and the sequence of letters from A to Z. In the letters there have no repetition and I & j are in same block.
* Divide plaintext to pair of letters.
* Differentiate repeated letters in the pair with dummy letters.
* If pair of plaintext letters are in same row, then replace them with rightmost letters.
* If pair of plaintext letters are in same column, then replace them with beneath letters.
* If pair of plaintext letters are in different row and column, then replace them with each diagonal letters.

Plaintext: HELLO

Key: NETWORK

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

HE| LL| O ------🡪HE|LX|LO

HE----🡪WF

LX----🡪UP

LO----🡪NS

HELXLO----🡪WFUPNS

Cipher Text: WFUPNS

Another Example:

Plaintext: BALLOON

Key: NETWORK

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

BA||LL|OO|N------🡪BA|LX|LO|ON

BA----🡪CB

LX----🡪UP

LO----🡪NS

ON----🡪NE

BALXLOON----🡪CBUPNSNE

Cipher Text: CBUPNSNE

Rot (1-25)

Rule:

Just change letters with the Rot number.

|  |  |  |
| --- | --- | --- |
| Rot number | Plaintext | Cipher Text |
| 1 | MY NAME | NZ OBNF |
| 2 | MY NAME | OA PCOG |
| 3 | MY NAME | PB QDPH |
| 4 | MY NAME | QC REQI |
| 5 | MY NAME | RD SFRJ |
| 6 | MY NAME | SE TGSK |
| 7 | MY NAME | TF UHTL |
| 8 | MY NAME | UG VIUM |
| 9 | MY NAME | VH WJVN |
| 10 | MY NAME | WI XKWO |
| 11 | MY NAME | XJ YLXP |
| 12 | MY NAME | YK ZMYQ |
| 13 | MY NAME | ZL ANZR |
| 14 | MY NAME | AM BOAS |
| 15 | MY NAME | BN CPBT |
| 16 | MY NAME | CO DQCU |
| 17 | MY NAME | DP ERDV |
| 18 | MY NAME | EQ FSEW |
| 19 | MY NAME | FR GTFX |
| 20 | MY NAME | GS HUGY |
| 21 | MY NAME | HT IVHZ |
| 22 | MY NAME | IU JWIA |
| 23 | MY NAME | JV KXJB |
| 24 | MY NAME | KW LYKC |
| 25 | MY NAME | LX MZLD |

Gronsfeld Cipher

Rule: With the key the letters are shifted forward. Key must be numbers not letters.

Plain text: MY NAME key:2 Cipher Text: OAPCOG

Plain text: MY NAME key:3 Cipher Text: PBQDPH

Unknown Cipher

Rules:

* Key may be numbers or letters.
* First write down the key value. If the key is in text, then the key value will be same as box value.

|  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| 0 | 1 | 2 | 3 | 4 | 5 | 6 | 7 | 8 | 9 | 10 | 11 | 12 | 13 | 14 | 15 | 16 | 17 | 18 | 19 | 20 | 21 | 22 | 23 | 24 | 25 |
| 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 |

* Then find each letter value of plaintext and find out the subtraction between key value and plaintext value.
* Then as per value from the box you set up the letters and find the cipher text.

Plaintext: MY NAME. KEY: 124

M--🡪12 Y--🡪24 N--🡪13 A--🡪0 E--🡪4

SO,M--🡪12-1=11--🡪L Y--🡪24-2=22--🡪W N--🡪13-4=9--🡪J A--🡪1-0=1--🡪B

M--🡪12-2=10--🡪K E--🡪4-4=0--🡪A

Cipher Text: LW JBKA

Plaintext: SAKIB KEY: HE

H--🡪7 E--🡪4 S--🡪18 A--🡪0 K--🡪10 I--🡪8 B--🡪1

SO,S--🡪18-7=11--🡪L A--🡪4-0=4--🡪E K--🡪10-7=3--🡪D I--🡪8-4=4--🡪E B--🡪7-1=6--🡪G

Cipher Text: LEDEG

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=--..

0=----- 1=.---- 2=..--- 3=…-- 4=….- 5=….. 6=-…. 7=--… 8=---.. 9=----.

.(dot)=.-.-.- ?(question mark)=..--.. ()=-.--.- ‘(apostrophe)=.----. ,(comma)=--..—

:(colon)=---… ;(semicolon)=-.-.-. -(dash)=-….-

\*3 space between every letter.

\*3 space and 1 straight slash and 3 space after a word.

\*1 straight slash before and after punctuation mark.

Example:

MY NAME.

-- -.-- | -. .- -- . .-.-.-

Piglatin

Rule: Rest of letters without first letter +first letter+ay.

Examples of piglatin:

will----illway

too----ootay

duck----uckday

sihab----ihabsay

Leetspeak

Alphabet examples:

A: 4,/-\,/\_\,@,/\

B: 8,|3,13,|},|:,|8,18,6,|B,|8,|0,lo

C: <,{,[,(

D: |),|},|]

E: 3

F:|=,ph,|#,|"

G: [,-,[+,6

H: 4,|-|,[-],{-},|=|,[=],{=}

I: 1,|,!,9

J: \_|,\_/,\_7,\_),\_],\_}

K: |<,1<,l<,|{,l{

L: |\_,|,1,][

M: 44,|\/|,^^,/\/\,/X\,[]\/][,[]V[],][\\//]

N: |\|,/\/,/V,][\\][

O: 0,(),[],{},<>

P: |0,l0,|>,|\*,|D,/0

Q: 0\_,9,(,),0,

R: |2,12,.-,|^,

S: 5,$,&

T: 7,+,7','|'

U: |\_|,\\_\,/\_/,\\_/,(\_),[\_],{\_}

V: \/

W: \/\/,(/\),\^|,|/\|,\X/,\\','//,VV

X: %,\*,><,}{,)(

Y: '/,

Z: 2,7\_,>\_

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

Letters for numbers:

0: O,D

1: l,L

2: Z

3: E

4: A,h

5: S

6: G,b

7: T,L,j

8: B

9: P

Leet vocabulary:

l@ym----laughing at your momma

ftw,4tw----for the win

hax,h4x----hacks

haxor,hax0r,h4x0r,haxzor----hacker

j00,joo----you

meh m3h----oh well

n1----nice

hf----have fun

gl----good luck

stronk----strong

BG----bad game

GG----good game

NOWAI----no way

YARLY----yeah really

O RLY----oh really

L2P----learn to play

QQ----cry

ZoMG----oh my god

teh,t3h----the

roxor,r0xorz----rock

phear,ph34r,ph33r----fear

pwnd----owned

pwnage----best

pwn----own

Tap code

* The tap code table:

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

* Rules:

1.Write that amount of dots of row number space column number of the specific letter.

2.After every word for space write NULL.

Example:

Plain Text: HELLO SAMU

Cipher Text: .. … . ….. … . … . … …. NULL …. … . . … .. …. …..

Hill Cipher

* Rules:

1.Make up a table like that:

|  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| 0 | 1 | 2 | 3 | 4 | 5 | 6 | 7 | 8 | 9 | 10 | 11 | 12 | 13 | 14 | 15 | 16 | 17 | 18 | 19 | 20 | 21 | 22 | 23 | 24 | 25 |
| 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 |

2.Create a key that may be numbers or letters but if letter then write letters value from the box and write in a matrix nxn. ( n is a positive integer number)

3.Write your plain text letters value and make them a matrix by whom you can product your key.

4.Then you have to mod every outcome of product and finally get the cipher text.

Example:

Plain text: ACT

KEY:

So, A--🡪0 C--🡪2 T--🡪19

Then, product of :

And matrix is so then, (mod 26)

So, cipher text: POH

One Time Pad

* Rules:1. Make up a table like that:

|  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| 0 | 1 | 2 | 3 | 4 | 5 | 6 | 7 | 8 | 9 | 10 | 11 | 12 | 13 | 14 | 15 | 16 | 17 | 18 | 19 | 20 | 21 | 22 | 23 | 24 | 25 |
| 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 |

2.For every letter fix the value of the letter from the box.

3. Set up a key value or key password then, add that value or password value with the letters value and finally mod them with 26.

4 Then turn them into letter.

Example:

Plain Text: HELLO SAMU

KEY: SAMU

H--🡪7 E--🡪4 L--🡪11 O--🡪14 S--🡪18 A--🡪0 M--🡪12 U--🡪20

Then, H--🡪7+18=25--🡪Z E--🡪4+0=4--🡪E L--🡪11+12=23--🡪X L--🡪11+20=31--🡪5--🡪F

O--🡪14+18=32--🡪6--🡪G S--🡪18+0=18--🡪S A--🡪0+12=12--🡪M M--🡪12+20=32--🡪6--🡪G

U--🡪20+18=38--🡪12--🡪M

Cipher Text: ZEXFG SMGM

Polybius Square or Polybius Checkerboard

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

RSA Algorithm

* Key Generation:

1.Choose two primes p, q.

As example assume that, p= 3 q=7

2.Compute n.

Where n=p\*q

So, n=3\*7=21

3.Compute Euler, .

Where

4.Choose e.

Where 1<e< and must be prime with .

So, e=7

Key is (n, e) = (21, 7)

* Message Encryption:

C (Cipher text) =m (message or plain text) ^e mod n

Encrypt the message M=4(Here it is up to you)

C=4^7 mod 21=16384 mod 21 =4

* Message Decryption:

M=C^ d mod n

D =e^-1 mod

=7^-1 mod 12=7

M=4^7 mod 21 =16384 mod 21=4