Cesium [Julia Version]

Cesium is a highly adjustable symmetric cryptosystem that uses an $n \times n$ matrix of integers in $1..b$ as a key, with b and n chosen by the user. Larger values of b and n should be more secure. It's also easy to let $n = b$, but this is not required (or desired, if b is small.)

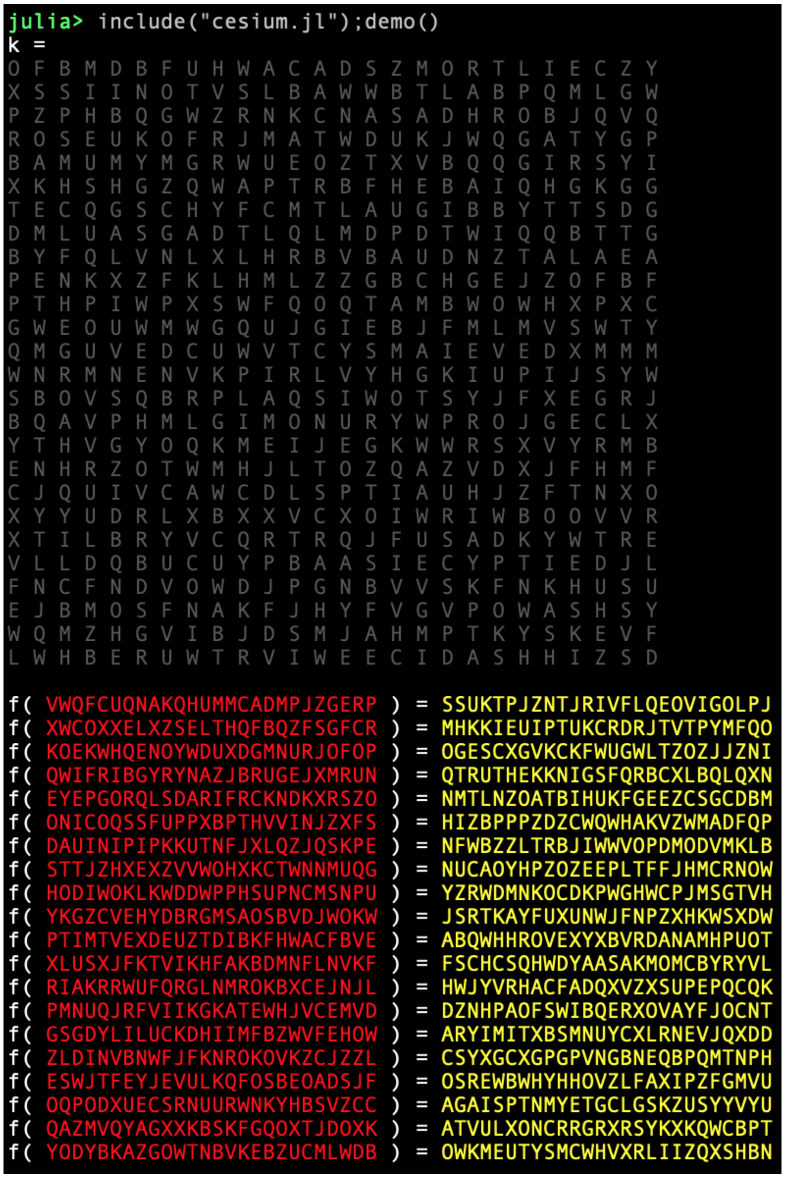
Cesium is a mutation of Cyclone. In Cyclone, each row had to represent a permutation. In Cesium, this constraint is lifted. Indeed there are no constraints, though choosing a matrix of all 7s, for instance, would not be great for security, given how the key is used.

The diagonal of the matrix does the work here. Let's look at the crucial functions:

```
function encode(p,q)
    k = copy(q)
    c = Int64[]
    for i in eachindex(p)
        x = tr(k)%b
        push!(c,(p[i] + x)%b )
        isodd((x + p[i])%b) ? spincols(k,p[i]) : spinrows(k,p[i])
    end
    c
end
function spinrows(k,p)
    for j in 1:size(k)[begin]
            k[j,:] = circshift(k[j,:],k[j,j]+p + 1)
    end
end
function spincols(k,p)
    for j in 1:size(k)[begin]
        k[:,j] = circshift(k[:,j],k[j,j]+ p + 1)
    end
end
```

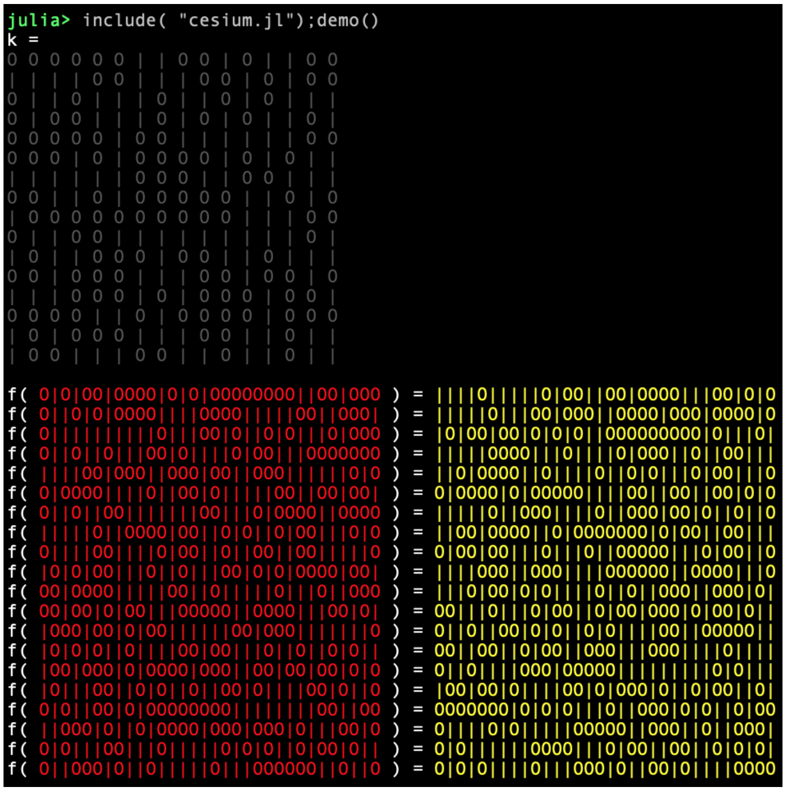
The next cipher symbol is the sum of the trace of the key matrix and the plain symbol (mod b, so that $c \in 1..b$). Then each row is circular-shifted by $p + 1$ units, so that the key's evolution is strongly dependent on the plaintext (which should add security.)

An adjustable "alphabetic mask" is also used for a more human-readable output. For instance, we can set $n = 26$ and then translate representations of the key, plaintexts, and ciphertexts by $1 \rightarrow a, 2 \rightarrow b, 3 \rightarrow c, ...$ The images below show outputs from the demo function.



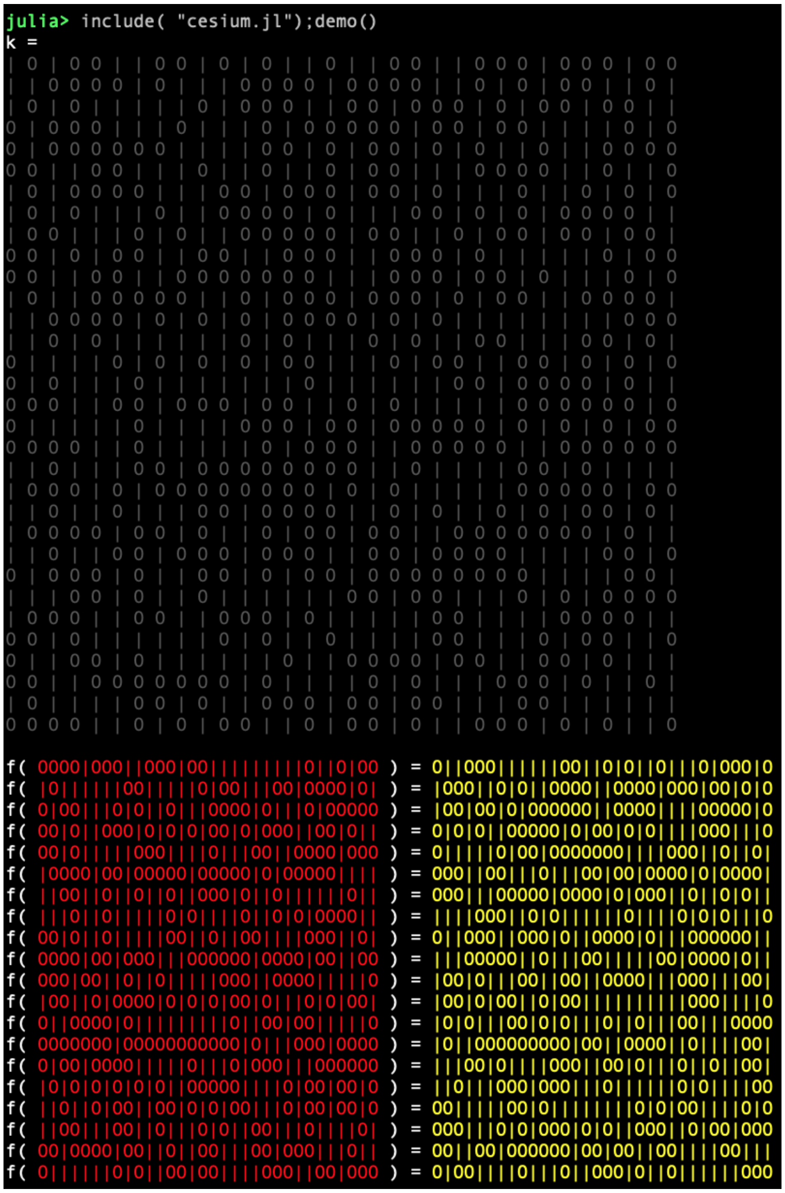
```
julia> include("cesium.jl");demo()
k =
O F B M D B F U H W A C A D S Z M O R T L I E C Z Y
X S S I I N O T V S L B A W W B T L A B P Q M L G W
P Z P H B Q G W Z R N K C N A S A D H R O B J Q V Q
R O S E U K O F R J M A T W D U K J W Q G A T Y G P
B A M U M Y M G R W U E O Z T X V B Q Q G I R S Y I
X K H S H G Z Q W A P T R B F H E B A I Q H G K G G
T E C Q G S C H Y F C M T L A U G I B B Y T T S D G
D M L U A S G A D T L Q L M D P D T W I Q Q B T T G
B Y F Q L V N L X L H R B V B A U D N Z T A L A E A
P E N K X Z F K L H M L Z Z G B C H G E J Z O F B F
P T H P I W P X S W F Q O Q T A M B W O W H X P X C
G W E O U W M W G Q U J G I E B J F M L M V S W T Y
Q M G U V E D C U W V T C Y S M A I E V E D X M M M
W N R M N E N V K P I R L V Y H G K I U P I J S Y W
S B O V S Q B R P L A Q S I W O T S Y J F X E G R J
B Q A V P H M L G I M O N U R Y W P R O J G E C L X
Y T H V G Y O Q K M E I J E G K W W R S X V Y R M B
E N H R Z O T W M H J L T O Z Q A Z V D X J F H M F
C J Q U I V C A W C D L S P T I A U H J Z F T N X O
X Y Y U D R L X B X X V C X O I W R I W B O O V V R
X T I L B R Y V C Q R T R Q J F U S A D K Y W T R E
V L L D Q B U C U Y P B A A S I E C Y P T I E D J L
F N C F N D V O W D J P G N B V V S K F N K H U S U
E J B M O S F N A K F J H Y F V G V P O W A S H S Y
W Q M Z H G V I B J D S M J A H M P T K Y S K E V F
L W H B E R U W T R V I W E E C I D A S H H I Z S D

f( VWQFCUQNAKQHUMMCADMPJZGERP ) = SSUKTPJZNTJRIVFLQEOVIGOLPJ
f( XWCOXXELXZSELTHQFBQZFSGFCR ) = MHKKIEUIPTUKCRDRJTVTPYMFQO
f( KOEKWHQENOYWDUXDGMNURJOFOP ) = OGESCXGVKCKFWUGWLTZOZJJZNI
f( QWIFRIBGYRYNAZJBRUGEJXMRUN ) = QTRUTHEKKNIGSFQRBCXLBQLQXN
f( EYEPGORQLSDARIFRCKNDKXRSZO ) = NMTLNZOATBIHUKFGEEZCSGCDBM
f( ONICOQSSFUPPXBPTHVVINJZXFS ) = HIZBPPPZDZCWQWHAKVZWMADFQP
f( DAUINIPIPKKUTNFJXLQZJQSKPE ) = NFWBZZLTRBJIWWVOPDMODVMKLB
f( STTJZHXEXZVVWOHXKCTWNNMUQG ) = NUCAOYHPZOZEEPLTFFJHMCRNOW
f( HODIWOKLKWDDWPPHSUPNCMSNPU ) = YZRWDMNKOCDKPWGHWCPJMSGTVH
f( YKGZCVEHYDBRGMSAOSBVDJWOKW ) = JSRTKAYFUXUNWJFNPZXHKWSXDW
f( PTIMTVEXDEUZTDIBKFHWACFBVE ) = ABQWHHROVEXYXBVRDANAMHPUOT
f( XLUSXJFKTVIKHFAKBDMNFLNVKF ) = FSCHCSQHWDYAASAKMOMCBYRYVL
f( RIAKRRWUFQRGLNMROKBXCEJNJL ) = HWJYVRHACFADQXVZXSUPEPQCQK
f( PMNUQJRFVIIKGKATEWHJVCEMVD ) = DZNHPAOFSWIBQERXOVAYFJOCNT
f( GSGDYLILUCKDHIIMFBZWVFEHOW ) = ARYIMITXBSMNUYCXLRNEVJQXDD
f( ZLDINVBNWFJFKNROKOVKZCJZZL ) = CSYXGCXGPGPVNGBNEQBPQMTNPH
f( ESWJTFEYJEVULKQFOSBEOADSJF ) = OSREWBWHYHHOVZLFAXIPZFGMVU
f( OQPODXUECSRNUURWNKYHBSVZCC ) = AGAISPTNMYETGCLGSKZUSYYVYU
f( QAZMVQYAGXXKBSKFGQOXTJDOXK ) = ATVULXONCRRGRXRSYKXKQWCBPT
f( YODYBKAZGOWTNBVKEBZUCMLWDB ) = OWKMEUTYSMCWHVXRLIIZQXSHBN
```



```
julia> include( "cesium.jl");demo()
k =
0 0 0 0 0 0 | | 0 0 | 0 | | 0 0
| | | | 0 0 | | | 0 0 | 0 | 0 0
0 | | 0 | | | 0 | | 0 | 0 | | |
0 | 0 0 | | | 0 | 0 | 0 | | 0 |
0 0 0 0 0 | 0 0 | | | | | | 0 0
0 0 0 | 0 | 0 0 0 0 | 0 | 0 | |
| | | | | | 0 0 0 | | 0 0 | | |
0 0 | | 0 | 0 0 0 0 0 | | 0 | 0
| 0 0 0 0 0 0 0 0 0 0 | | | 0 0
0 | | 0 0 | | | | | | | | | 0 |
| 0 | | 0 0 0 | 0 0 | | 0 | | |
0 0 | 0 0 0 | | | 0 0 | 0 0 | 0
| | | 0 0 0 | 0 | 0 0 0 | 0 0 |
0 0 0 0 | | 0 | 0 0 0 0 | 0 0 0
| 0 | 0 0 0 | | | 0 0 | | 0 | |
| 0 0 | | | 0 0 | | 0 | | 0 | |

f( 0|0|00|0000|0|0|00000000||00|000 ) = ||||0|||||0|00||00|0000|||00|0|0
f( 0||0|0|0000||||0000|||||00||000| ) = |||||0|||00|000||0000|000|0000|0
f( 0||||||||||0|||00|0||0|0|||0|000 ) = |0|00|00|0|0|0||000000000|0|||0|
f( 0||0||0|||00|0||||0|00|||0000000 ) = |||||0000|||0||||0|000||0||00|||
f( ||||00|000||000|00||000||||||0|0 ) = ||0|0000||0||||0||0|0|||0|00|||0
f( 0|0000||||0||00|0|||||00||00|00| ) = 0|0000|0|00000||||00||00||00|0|0
f( 0||0||00|||||||00|||0|0000||0000 ) = |||||0||000||||0||000|00|0||0||0
f( |||||0||0000|00||0|0||0|00|||0|0 ) = ||00|0000||0|0000000|0|00||00|||
f( 0||||00||||0|00||0||00||00|||||0 ) = 0|00|00|||0|||0||00000|||0|00||0
f( |0|0|00|||0||0|||00|0|0|0000|00| ) = ||||000||000||||000000||0000|||0
f( 00|0000|||||00||0|||||0|||0||000 ) = |||0|00|0|0||||0||0||000||000|0|
f( 00|00|0|00|||00000||0000|||00|0| ) = 00|||0|||0|00||0|00|000|0|00|0||
f( |000|00|0|00||||||00|000|||||||0 ) = 0||0||00|0|0||0|0||||00||00000||
f( |0|0|0||0||||00|00|||0||0||0|0|| ) = 00||00||0|00||000|||000||||0||||
f( |00|000|0|0000|000||00|00|00|0|0 ) = 0||0||||000|00000|||||||||0|0|||
f( |0|||00||0|0||0||00|0||||00|0||0 ) = |00|00|0||||00|0|000|0||0|00||0|
f( 0|0||00|0|00000000||||||||00||00 ) = 0000000|0|0|0||0|||000|0|0||0|00
f( ||000|0||0|0000|000|000|0|||00|0 ) = 0||||0|0|||||00000||000||0||000|
f( 0|0||00||||0|||||0|0|0||0|00|0|| ) = 0|0||||||0000|||0|00||00||0|0|0|
f( 0||000|0||0|||||0|||000000||0||0 ) = 0|0|0||||0|||000|0||00|0||||0000
```



```
julia> include( "cesium.jl");demo()
k =
| 0 | 0 0 | | 0 0 | 0 | 0 | | 0 | | 0 0 | | 0 0 0 | 0 0 0 | 0 0
| | 0 0 0 0 | 0 | | | 0 0 0 0 | 0 0 0 0 | | 0 | 0 | 0 0 | | 0 |
| 0 | 0 | | | | | 0 | 0 0 0 | | 0 0 | 0 0 0 | 0 | 0 0 | 0 0 | |
0 | 0 0 0 | | | 0 | | | 0 | 0 0 0 0 0 | 0 0 | 0 0 | | | | 0 | 0
0 | 0 0 0 0 0 0 | | | | 0 0 | 0 | 0 0 | 0 | 0 | | 0 | | 0 0 0 0
0 0 | | 0 0 | | | 0 | | 0 | | 0 | 0 0 | | | 0 0 0 0 | | 0 | | 0
| 0 | 0 0 0 0 | | | 0 0 | 0 0 0 | 0 0 | 0 | | | 0 | | 0 | 0 | 0
| 0 | 0 | | | 0 | | 0 0 0 0 | 0 | | | 0 0 | 0 | 0 | 0 0 0 0 | |
| 0 0 | | | 0 | 0 | | 0 0 0 0 0 | 0 0 | | 0 | 0 0 | 0 0 | 0 0 |
0 0 | 0 | 0 0 | | 0 0 | | 0 0 0 | | 0 0 0 | 0 | | | | | 0 | 0 0
0 0 | | 0 0 | | 0 0 0 0 0 0 0 | | | 0 0 0 | 0 0 | 0 | | | 0 | 0
| 0 | | 0 0 0 0 0 | | 0 | 0 0 0 | 0 0 0 | 0 | 0 0 | | 0 0 0 0 |
| | 0 0 0 0 | 0 | 0 | 0 | 0 0 0 0 | 0 | 0 | | | | | | | | 0 0 0
| | 0 | 0 | | | | | | 0 | 0 | | | 0 | 0 | | 0 0 | | | 0 0 | 0 |
0 | | | | 0 | 0 | 0 | 0 | 0 0 | | | 0 | 0 0 | | 0 0 | 0 | 0 | 0
0 | 0 | | | 0 | | | | | | 0 | | | | | | 0 0 | 0 0 0 0 | 0 | |
0 0 0 | | 0 0 | 0 0 0 | 0 0 | | 0 | 0 | | | | | 0 0 0 0 0 0 | 0
0 | | | | | 0 | | | | 0 0 0 | 0 0 | 0 0 0 0 0 | 0 | 0 | 0 | 0 0
0 0 0 0 | | 0 | | | | | 0 | 0 0 0 | | 0 0 0 0 0 | | 0 0 0 0 0 0
| | 0 | | | 0 0 | 0 0 0 0 0 0 0 0 | | 0 | | | | 0 0 | 0 | | | |
| 0 0 0 | 0 | 0 0 0 0 0 0 0 0 | 0 | 0 | | | | | 0 0 0 0 0 | 0 0
| | 0 | | 0 | | | 0 0 | 0 0 0 0 | | 0 | 0 | | 0 | 0 | 0 0 | 0 |
| 0 0 0 0 | 0 0 | 0 | | 0 | 0 0 | 0 0 | | 0 0 0 0 0 0 0 | 0 | |
| | 0 | | 0 0 | 0 0 0 | 0 0 0 | | 0 0 | 0 0 0 0 | | | | 0 0 | 0
0 | 0 0 0 | 0 | | 0 0 | 0 | 0 0 | 0 0 0 0 0 0 0 0 | | | | 0 0 |
| | | 0 0 | 0 | | 0 | | | | | | 0 0 | 0 0 | | | 0 | 0 | 0 0 0 0
| 0 0 0 | | 0 0 | | 0 0 0 | 0 | | | | | 0 0 | | | | 0 0 0 0 | |
0 0 | 0 | | | | | | 0 | 0 | | 0 | | | | 0 0 | | | 0 | 0 0 | | 0
0 | | 0 0 | 0 | | | | | | 0 | | 0 0 0 0 | 0 0 | | 0 0 | 0 | | |
0 0 | | 0 0 0 0 0 0 0 | 0 | | | | 0 | 0 | | | 0 0 0 | 0 | | 0 |
| 0 | | | | 0 0 | 0 | | 0 0 0 | 0 0 | 0 0 | | | 0 0 | | | | | |
0 0 0 0 | | 0 | 0 | 0 0 | | 0 | 0 0 | 0 | | 0 0 0 | 0 | 0 | | 0

f( 0000|000||000|00|||||||||0||0|00 ) = 0||000||||||00||0|0||0|||0|000|0
f( |0||||||00|||||0|00|||00|0000|0| ) = |000||0|0||0000||0000|000|00|0|0
f( 0|00|||0|0||0|||0000|0|||0|00000 ) = |00|00|0|000000||0000||||00000|0
f( 00|0||000|0|0|0|00|0|000||00|0|| ) = 0|0|0||00000|0|00|0|0||||000|||0
f( 00|0|||||000||||0|||00||0000|000 ) = 0|||||0|00|0000000||||000||0||0|
f( |0000|00|00000|00000|0|00000|||| ) = 000||00|||0|||00|00|0000|0|0000|
f( ||00||0||0||0||000|0||0||||||0|| ) = 000|||00000|0000|0|000||0||0|0||
f( |||0||0|||||0|0||||0||0|0|0000|| ) = ||||000||0|0||||||0||||0|0|0|||0
f( 00|0||0|||||00||0||00||||000||0| ) = 0||000||000|0||0000|0|||000000||
f( 0000|00|000|||000000|0000|00||00 ) = |||00000||0|||00|||||00|0000|0||
f( 000|00||0||0|||||000||0000|||||0 ) = |00|0|||00||00||0000|||000|||00|
f( |00||0|0000|0|0|0|00|0|||0|0|00| ) = |00|0|00||0|00||||||||||000||||0
f( 0||0000|0|||||||||0||00|00|||||0 ) = |0|0|||00|0|0|||0||0|||00|||0000
f( 0000000|00000000000|0|||000|0000 ) = |0||000000000|00||0000||0||||00|
f( 0|00|0000|||||0|||0|000|||000000 ) = |||00|0||||000||00|0|||0||0||00|
f( |0|0|0|0|0|0||00000||||0|00|00|0 ) = ||0|||000|000|||0||||||0|0||||00
f( ||0||0|00||00|0|0|00|||0|00|00|0 ) = 00|||||00|0||||||||0|0|00||||0|0
f( ||00|||00||0|||0|0||00|||0||||0| ) = 000|||0|0|000|0|0||000||0|00|000
f( 00|0000|00||0||00|||00|000|||0|| ) = 00||00|000000|00|00||00||||00|||
f( 0||||||0|0||00|00||||000||00|000 ) = 0|00||||0|||0||000|0||0||||||000
```

The second and third images could also be of the Thorium cryptosystem, which is basically the Cesium system with $b = 2$. I hope to write Thorium so that its bit-centric nature is emphasized. Curium is another variant, where $b = 3$ and the 27 symbols of the alphabet and (for instance) the underscore are encoded in three ternary digits, so that plaintext messages in English are translated into ternary and then encoded.