1. SpongeConstruction

a-Padding

* input string
* fixed length of bits to 1600

b- absorbing

* b= 1600 , w=64 L=6
* rate= 1088, capacity= 512
* S=input string (1600 len)
* A= 5x5x64 (x,y,z) array

Convert string to state array

* A[x,y,z] =S[w(5y+x)+z]

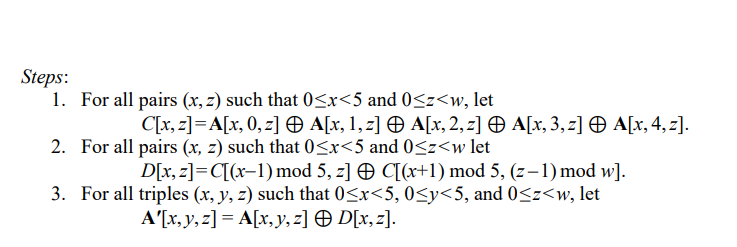
c-squeezing

Convert Array to string

* Lane (i,j) =A[I,j,0] ||A[i,j…. W-1]–––––

2- Keccak function

c-Mapping (5 stage process θ, ρ, π, χ, and ι.) 🡺Rnd(A, ir) = ι(χ(π(ρ(θ(A)))), ir).

Note: 24 times all 5 steps need to be done

* Theta

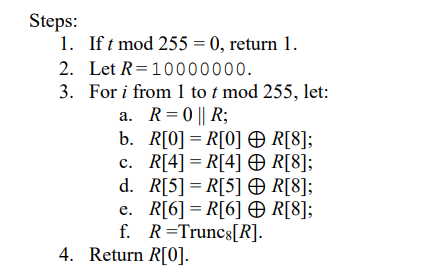
A picture containing logo

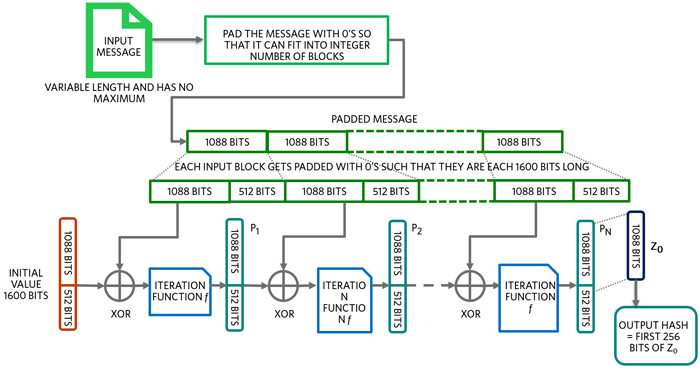
Description automatically generated

* Rho
* Text, letter

  Description automatically generatedPi
* Text

  Description automatically generatedX
* Iota





**Input**

**Message**

Keccak function:

24 rounds   
each of 5 steps

THETA

RHO

Iota

CHI

PI