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

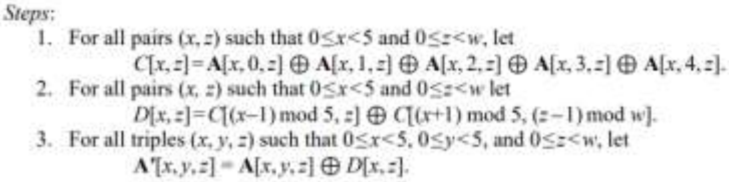
     Convert Array to string
   - Lane (i,j) =A[I,j,0] ||A[i,j…. W-1]———

2- Keccak function

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

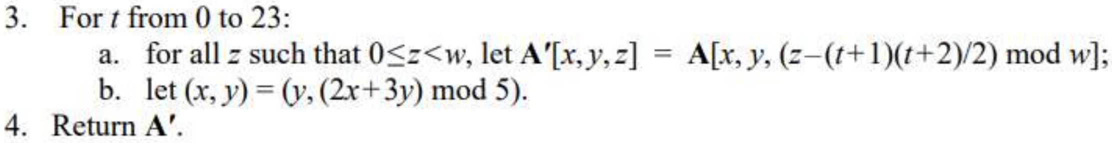
Note: 24 times all 5 steps need to be done

- Theta



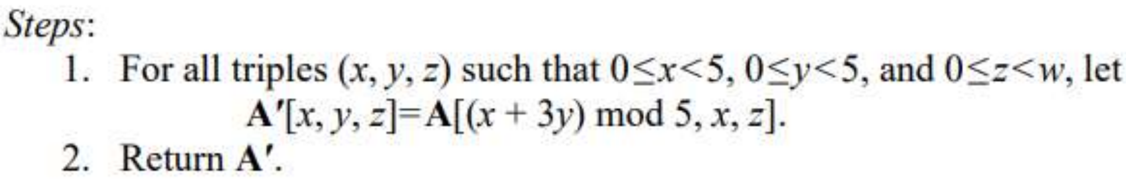
```
Steps:
  1. For all pairs $(x, z)$ such that $0 \leq x < 5$ and $0 \leq z < w$, let
         $C[x,z] = \mathbf{A}[x,0,z] \oplus \mathbf{A}[x,1,z] \oplus \mathbf{A}[x,2,z] \oplus \mathbf{A}[x,3,z] \oplus \mathbf{A}[x,4,z]$.
  2. For all pairs $(x, z)$ such that $0 \leq x < 5$ and $0 \leq z < w$ let
         $D[x,z] = C[(x-1) \bmod 5, z] \oplus C[(x+1) \bmod 5, (z-1) \bmod w]$.
  3. For all triples $(x, y, z)$ such that $0 \leq x < 5$, $0 \leq y < 5$, and $0 \leq z < w$, let
         $\mathbf{A}'[x,y,z] = \mathbf{A}[x,y,z] \oplus D[x,z]$.
```

- Rho



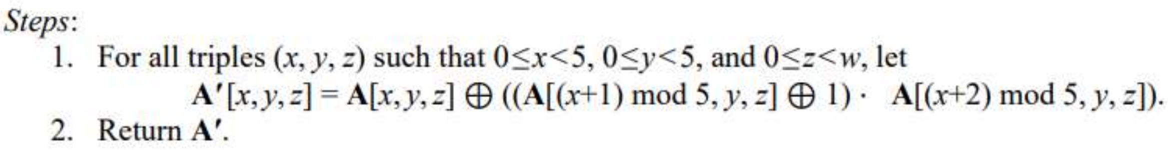
```
3. For $t$ from 0 to 23:
    a. for all $z$ such that $0 \leq z < w$, let $\mathbf{A}'[x,y,z] = \mathbf{A}[x, y, (z-(t+1)(t+2)/2) \bmod w]$;
    b. let $(x, y) = (y, (2x+3y) \bmod 5)$.
4. Return $\mathbf{A}'$.
```

- Pi



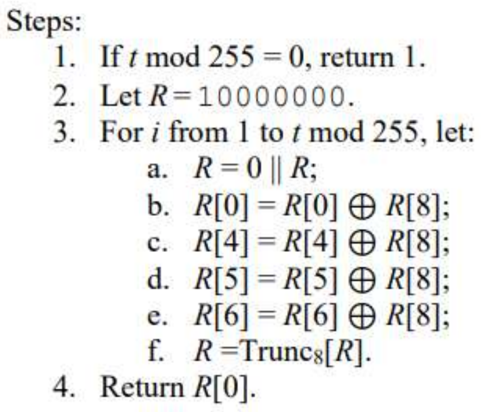
```
Steps:
  1. For all triples $(x, y, z)$ such that $0 \leq x < 5$, $0 \leq y < 5$, and $0 \leq z < w$, let
         $\mathbf{A}'[x, y, z] = \mathbf{A}[(x + 3y) \bmod 5, x, z]$.
  2. Return $\mathbf{A}'$.
```

- X

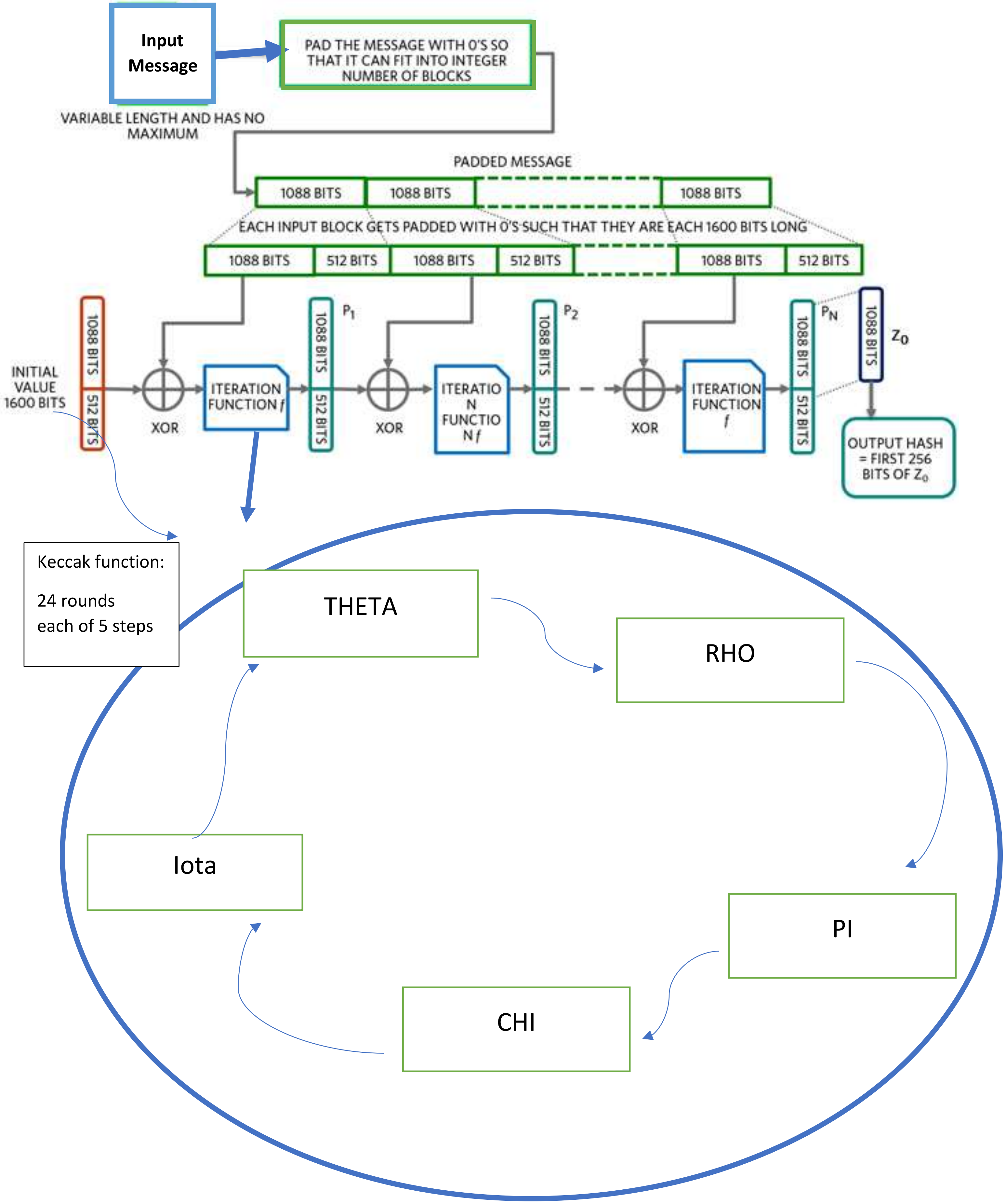


```
Steps:
  1. For all triples $(x, y, z)$ such that $0 \leq x < 5$, $0 \leq y < 5$, and $0 \leq z < w$, let
         $\mathbf{A}'[x,y,z] = \mathbf{A}[x,y,z] \oplus ((\mathbf{A}[(x+1) \bmod 5, y, z] \oplus 1) \cdot \mathbf{A}[(x+2) \bmod 5, y, z])$.
  2. Return $\mathbf{A}'$.
```

- Iota



```
Steps:
    1. If $t$ mod 255 = 0, return 1.
    2. Let $R$ = 10000000.
    3. For $i$ from 1 to $t$ mod 255, let:
        a. $R = 0 \| R$;
        b. $R[0] = R[0] \oplus R[8]$;
        c. $R[4] = R[4] \oplus R[8]$;
        d. $R[5] = R[5] \oplus R[8]$;
        e. $R[6] = R[6] \oplus R[8]$;
        f. $R = \text{Trunc}_8[R]$.
    4. Return $R[0]$.
```


Input Message
VARIABLE LENGTH AND HAS NO MAXIMUM
PAD THE MESSAGE WITH 0'S SO THAT IT CAN FIT INTO INTEGER NUMBER OF BLOCKS
PADDED MESSAGE
1088 BITS
1088 BITS
1088 BITS
EACH INPUT BLOCK GETS PADDED WITH 0'S SUCH THAT THEY ARE EACH 1600 BITS LONG
1088 BITS
512 BITS
1088 BITS
512 BITS
1088 BITS
512 BITS
INITIAL VALUE 1600 BITS
1088 BITS
512 BITS
XOR
ITERATION FUNCTION f
1088 BITS
512 BITS
P1
XOR
ITERATIO N FUNCTIO N f
1088 BITS
512 BITS
P2
XOR
ITERATION FUNCTION f
1088 BITS
512 BITS
PN
1088 BITS
Z0
OUTPUT HASH = FIRST 256 BITS OF Z0
Keccak function:
24 rounds
each of 5 steps
THETA
RHO
PI
CHI
Iota