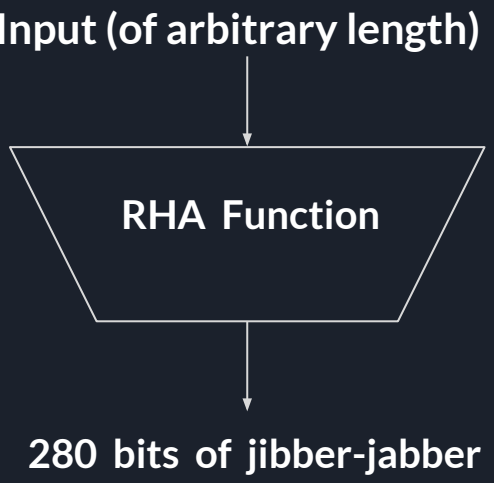
Internals of RHA

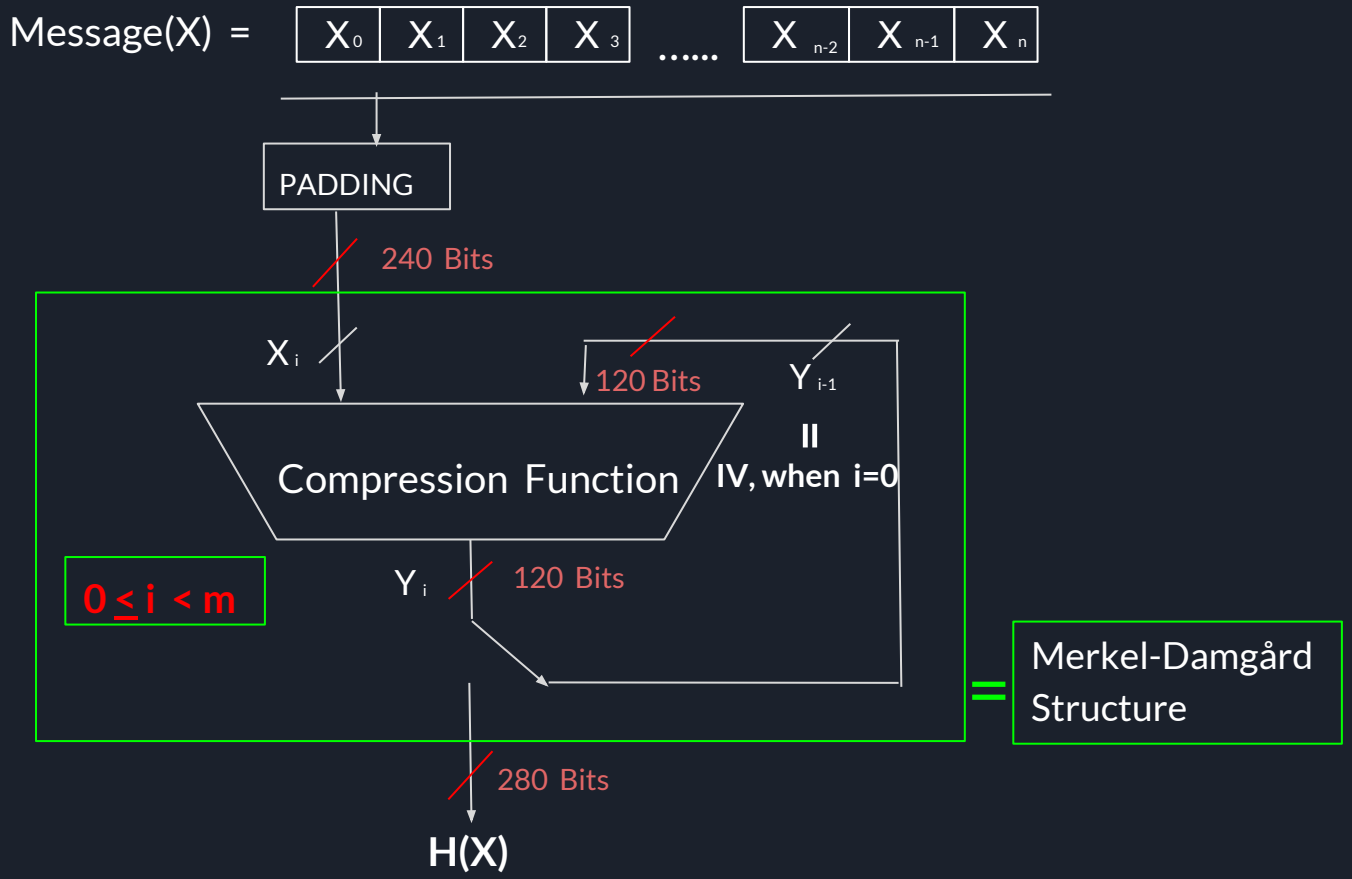
RHA: Revised Hashing Algorithm...

IS WHAT WE ARE CALLING IT :)

RHA (Revised Hashing Algorithm) produces a 280 bit digest for a given input of arbitrary length.



What happens inside RHA Function ?



What happens inside Compression Function ?

1) Message Schedule

2) Round Function

Message Schedule

For each block(Xi) of Message(X) of length 240 bits, we generate 80 Keywords(W) in the following way:

W[0] = Xi[0]
W[1] = Xi[1]
W[2] = Xi[2]
W[3] = Xi[3]
W[4] = Xi[4]
W[5] = Xi[5]
W[6] = Xi[6]
W[7] = Xi[7]
W[8] = W[0]<<1
W[9] = W[1]>>2

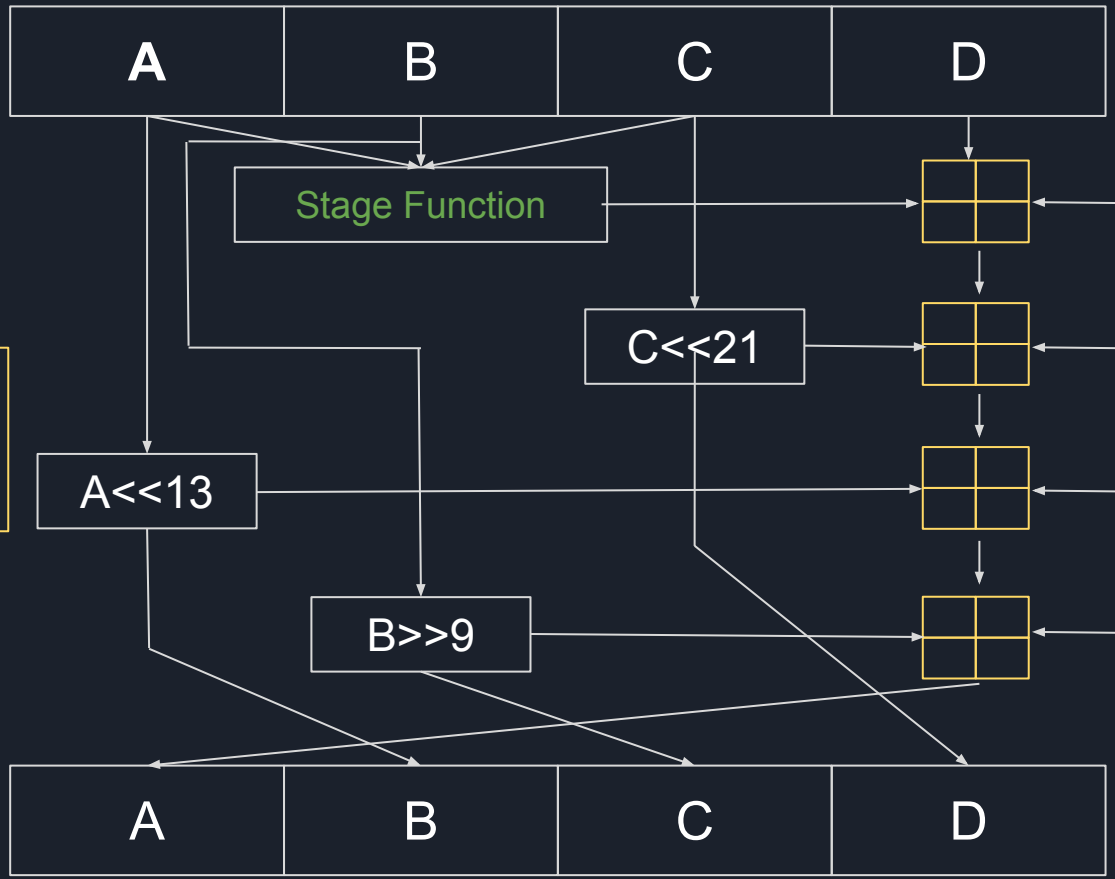
W[10] = W[2]<<3
W[11] = W[3]>>4
W[12] = W[4]<<4
W[13] = W[5]>>3
W[14] = W[6]<<2
W[15] = W[7]>>1
W[16] = W[8]<<1
W[17] = W[9]>>2
W[18] = W[10]<<3
W[19] = W[11]>>4

W[20] = W[12]<<4
W[21] = W[13]>>3
W[22] = W[14]<<2
W[23] = W[15]>>1
W[24] = W[16]<<1
W[25] = W[17]>>2
W[26] = W[18]<<3
W[27] = W[19]>>4
W[28] = W[20]<<4
W[29] = W[21]>>3

W[30] = W[22]<<2
W[31] = W[23]>>1
W[32] = W[24]<<1
W[33] = W[25]>>2
W[34] = W[26]<<3
W[35] = W[27]>>4
W[36] = W[28]<<4
W[37] = W[29]>>3
W[38] = W[30]<<2
W[39] = W[31]>>1

Round Function

Round Function carries the following operations 40 times for each Xi



Binary Addition
(first bit ignored if greater than 120 bits)

What is Stage Constant?

Stage constant is changed after every 10 rounds of operation.

For Rounds 0-9 : 7C20DD68

For Rounds 10-19 : DF89A8AF

For Rounds 20-21 : 99F61F5C

For Rounds 31-39 : A7AB02C9

What is Stage Function?

Stage Function is changed after every 10 rounds of operation.

For Rounds 0-9 : [A & B] ^ [(A<<7) & C] ^ [B & C]

For Rounds 10-19 : [B ^ C] & [(C>>21) | A] ^ [(B>>16) ^ A]

For Rounds 20-21 : [A & B] | [B & C] | [A & C]

For Rounds 31-39 : [A & C] & [(B<<12) | A] & [(C<<13) & (A>>10)]

Basically...

Compression function takes each block of the **Message(Xi)** and operates on it using **Message Schedule** and **Round function**.

The output of the compression function is the calculated hash of **280 Bits.**