Project Plan report format – Your first page MUST match this format /10

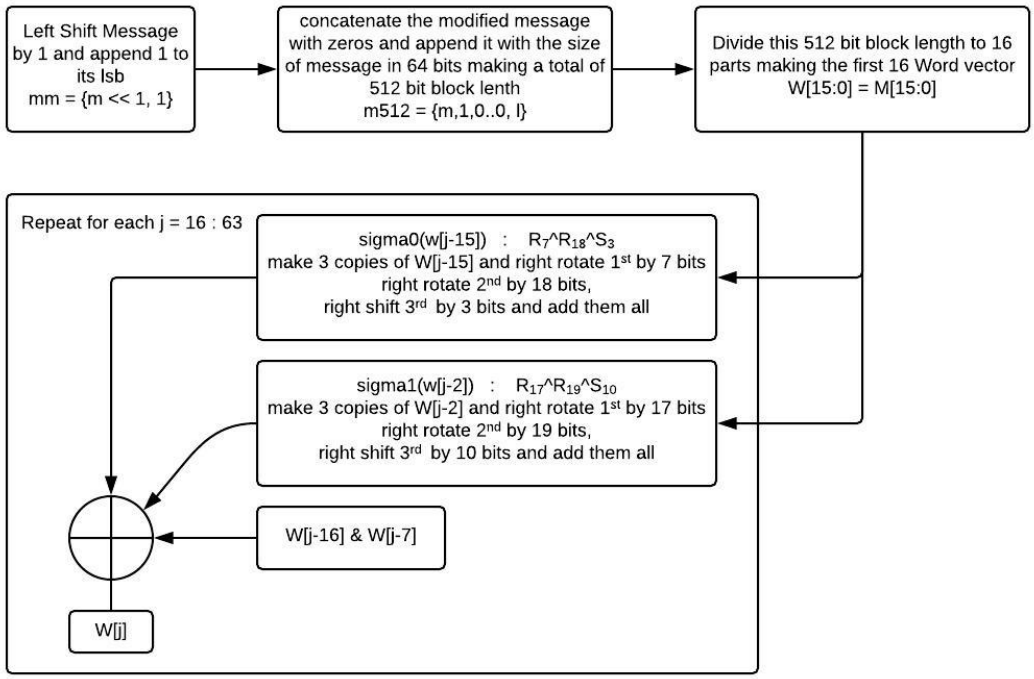
Name: Vishal Ganesh Shitole
Unityid: vgshitol
StudentID: 200258381

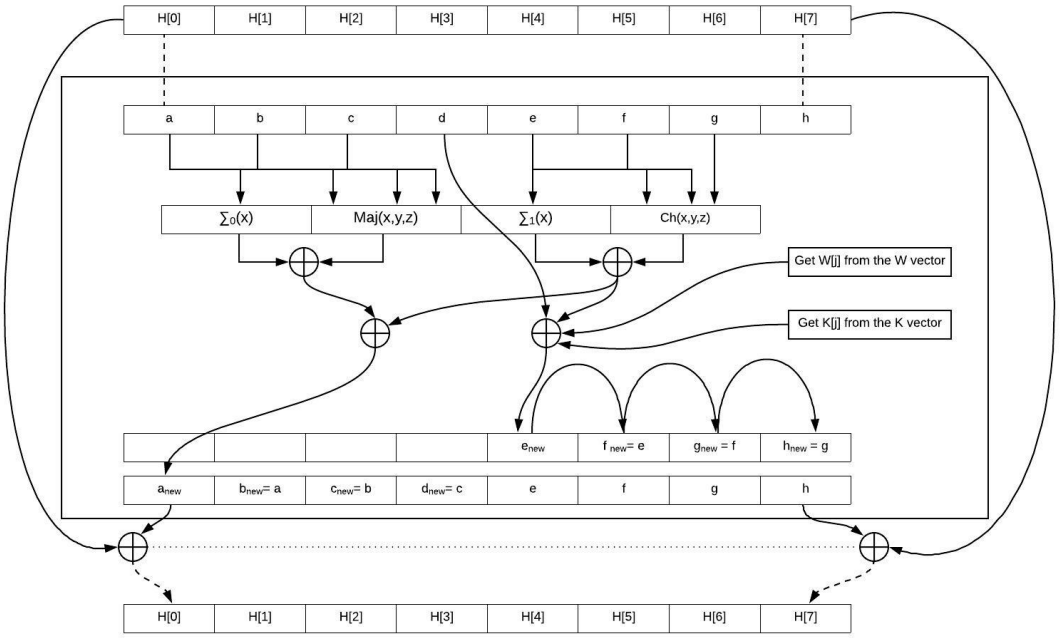
Summary Risk Plan:
Understanding the flow of design. Design before coding.
Debugging Complexity
Repeating logic for 64 word vectors
Serial read to parallel processing synchronization

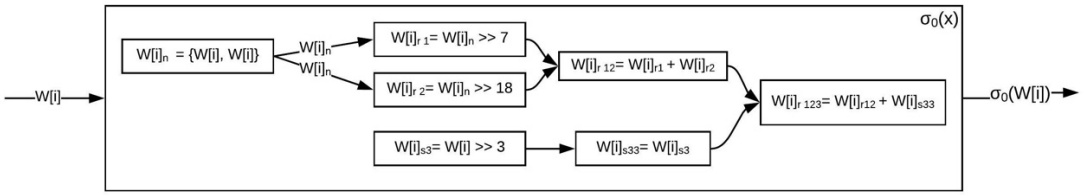
Schedule:
3 Days to form Message vector
1 week to form W vector
1 week to form final hash
1 week debugging and final report submission

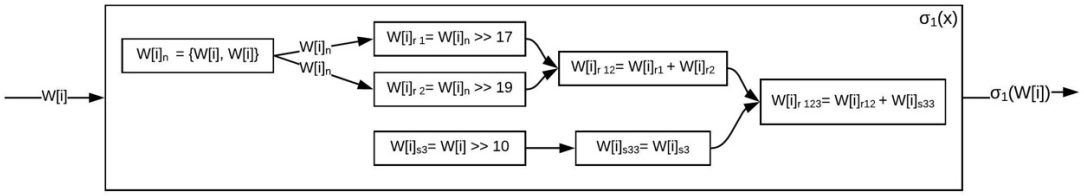
Brief Description of Mode of operation, including selected algorithms
Read data serially from SRAM and store it in register.
Form the 64 block vector
Use this data to calculate the hash using the algorithm.
Update the new hash.

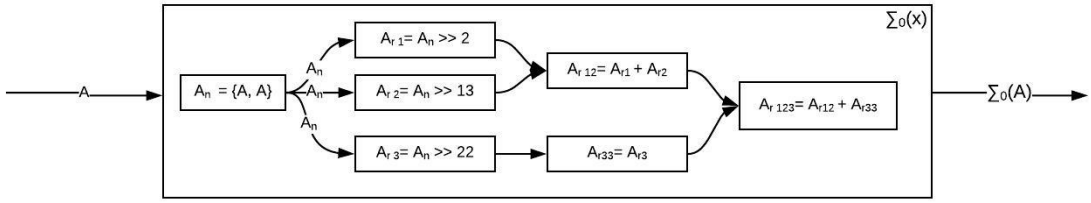
High level sketch. Add details on the following pages if necessary

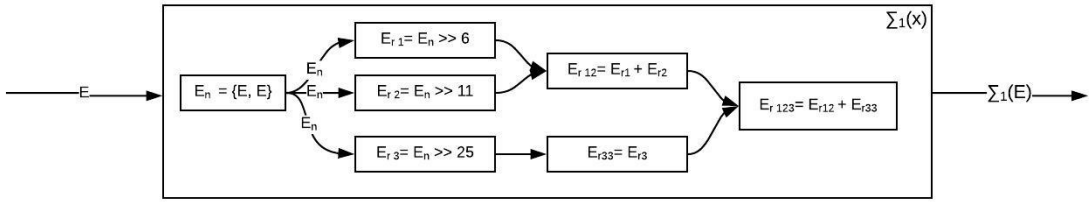


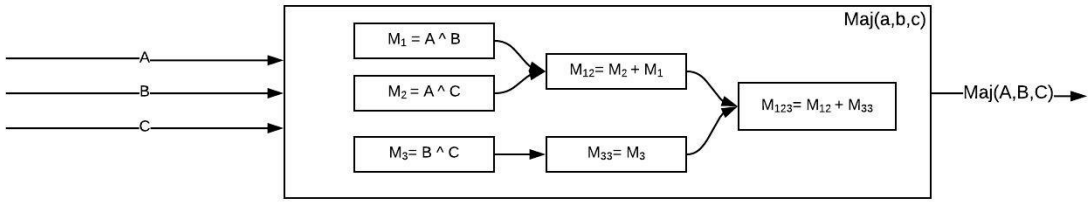

H[0]
H[1]
H[2]
H[3]
H[4]
H[5]
H[6]
H[7]
a
b
c
d
e
f
g
h
∑0(x)
Maj(x,y,z)
∑1(x)
Ch(x,y,z)
Get W[j] from the W vector
Get K[j] from the K vector
enew
f new= e
gnew = f
hnew = g
anew
bnew= a
cnew= b
dnew= c
e
f
g
h
H[0]
H[1]
H[2]
H[3]
H[4]
H[5]
H[6]
H[7]

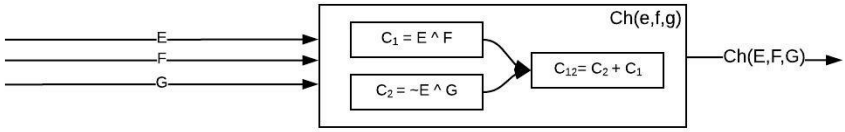

σ0(x)
W[i]
W[i]n = {W[i], W[i]}
W[i]n
W[i]n
W[i]r 1= W[i]n >> 7
W[i]r 2= W[i]n >> 18
W[i]s3= W[i] >> 3
W[i]r 12= W[i]r1 + W[i]r2
W[i]s33= W[i]s3
W[i]r 123= W[i]r12 + W[i]s33
σ0(W[i])


σ1(x)
W[i]
W[i]n = {W[i], W[i]}
W[i]n
W[i]n
W[i]r 1= W[i]n >> 17
W[i]r 2= W[i]n >> 19
W[i]s3= W[i] >> 10
W[i]r 12= W[i]r1 + W[i]r2
W[i]s33= W[i]s3
W[i]r 123= W[i]r12 + W[i]s33
σ1(W[i])


∑0(x)
A
An = {A, A}
An
An
An
Ar 1= An >> 2
Ar 2= An >> 13
Ar 3= An >> 22
Ar 12= Ar1 + Ar2
Ar33= Ar3
Ar 123= Ar12 + Ar33
∑0(A)


∑1(x)
E
En = {E, E}
En
En
En
Er 1= En >> 6
Er 2= En >> 11
Er 3= En >> 25
Er 12= Er1 + Er2
Er33= Er3
Er 123= Er12 + Er33
∑1(E)


Maj(a,b,c)
A
B
C
M1 = A ^ B
M2 = A ^ C
M3= B ^ C
M12= M2 + M1
M33= M3
M123= M12 + M33
Maj(A,B,C)


Ch(e,f,g)
E
F
G
C1 = E ^ F
C2 = ~E ^ G
C12= C2 + C1
Ch(E,F,G)