*N* X 1024 bits

*L* bits

128 bits

Message 1000,..,0 *L*

Hash Code

HN =

H2

H1

IV = 512

H0

1024

1024

1024

F

F

F

…

…

+

+

+

1024 bits

1024 bits

1024 bits

MN

M2

M1