# **Intro to SHA**

Text

Description automatically generated

Text

Description automatically generated

# **SHA-512**

Diagram

Description automatically generated

We have N-blocks each of 1024 bits.   
So N\*1024 🡪 bits are generated.  
N is the number of blocks.

Diagram

Description automatically generated

Adding 872 to 24, I will get 896 to match the standard criteria.

## **Padding**

Diagram, text

Description automatically generated

A picture containing text

Description automatically generated

Appending Message Length

A picture containing diagram

Description automatically generated

Text

Description automatically generated

Continuing from the above example

Diagram

Description automatically generated

Here ‘+’ 🡪 addition modulo 2^64

What is module F ???

Diagram

Description automatically generated

Diagram

Description automatically generated

How a word is calculated ???

Text

Description automatically generated

ROTR^1 🡪 Right Circular Shift of 1 bit.

ROTR^8 🡪 Right Circular Shift of 8 bits.

SHR^6 🡪 Left Shift of 6 bits.

A picture containing text, appliance, screenshot

Description automatically generated