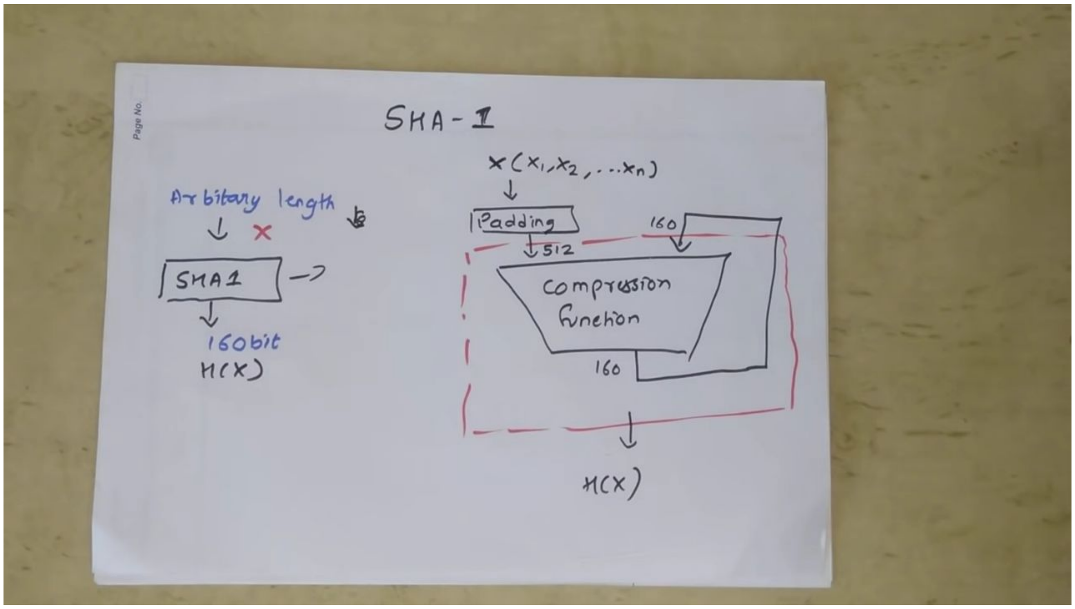
View, add and edit your notes in the app

SHA-1 (Secure hash Algorithm) working in English | CSS series

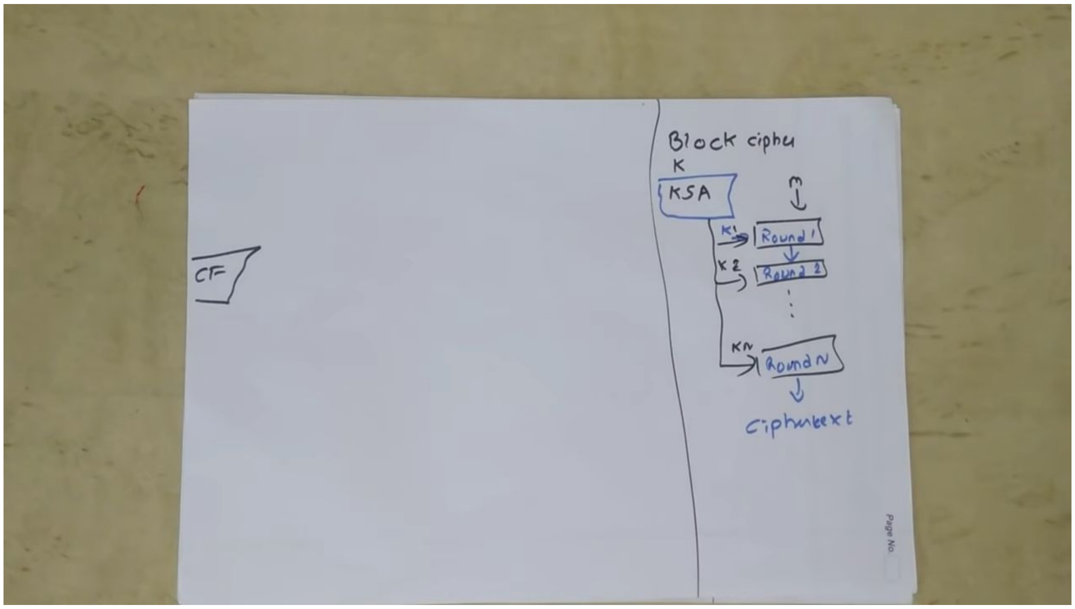
Generated on December 20, 2023

Summary

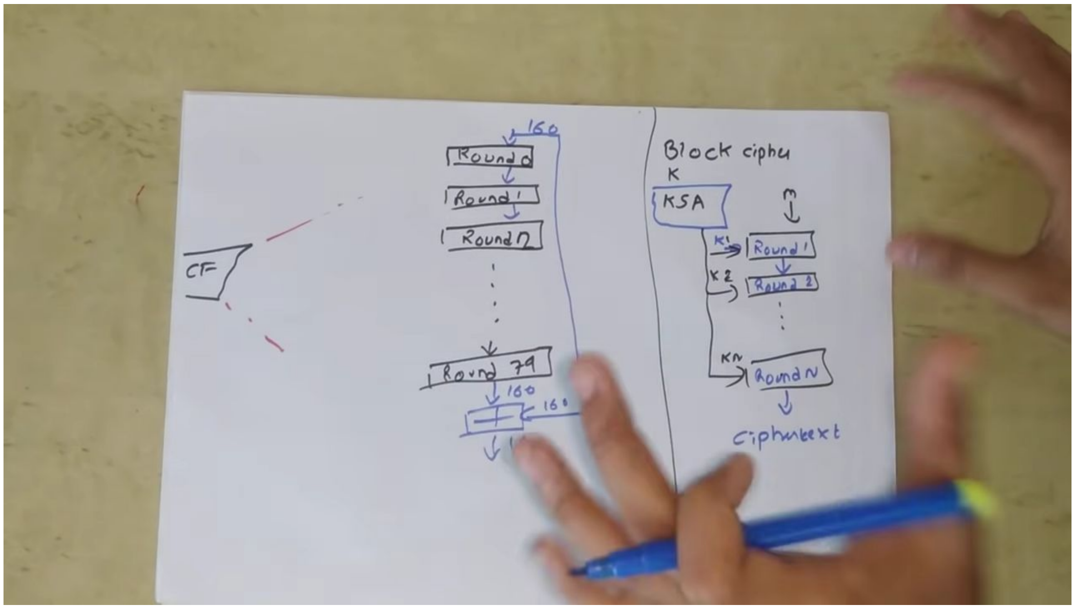
Notes	Screenshots	Bookmarks
0	11	0



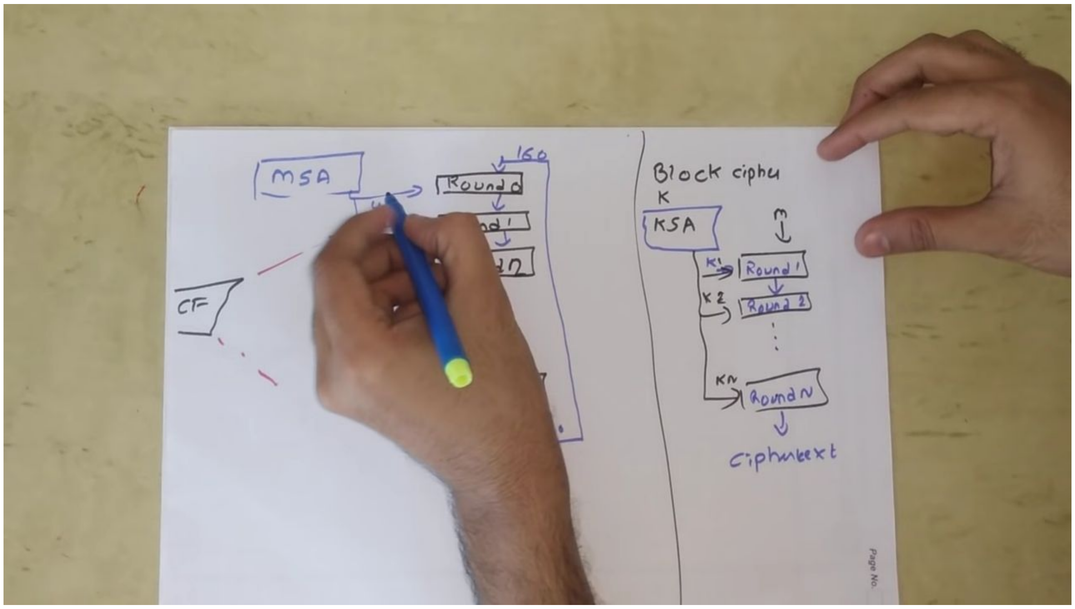
▷ 0:14


Block ciphu
K
KSA
m
K1
Round 1
K2
Round 2
Kn
Round N
ciphutext
CF
Page No.

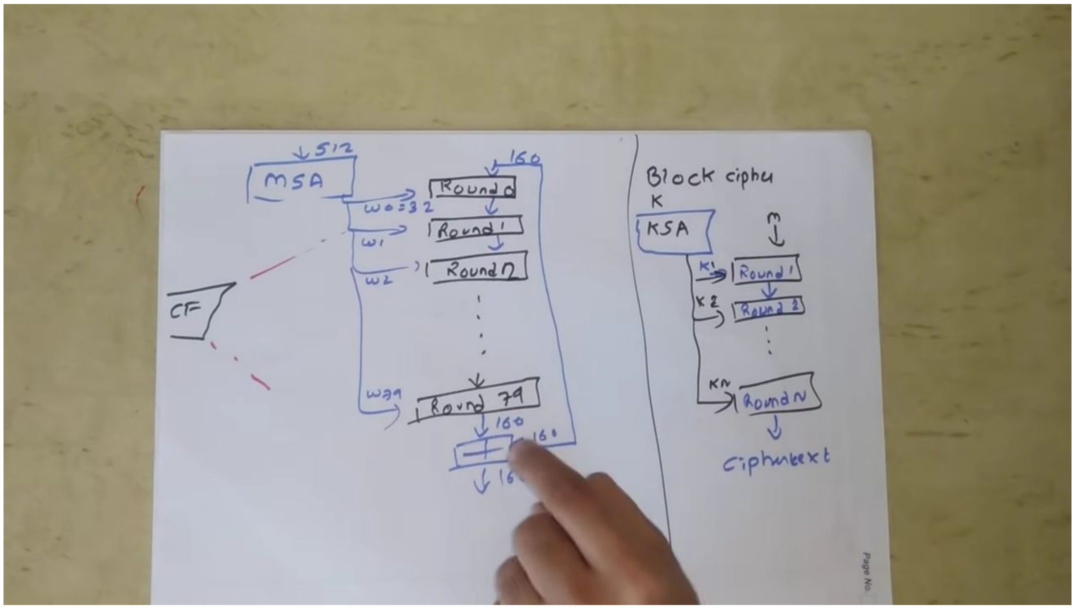
▷ 6:44


160
Round 0
Round 1
Round 2
Round 79
160
160
CF
Block ciphu
K
KSA
m
K1
Round 1
K2
Round 2
Kn
Round N
ciphutext

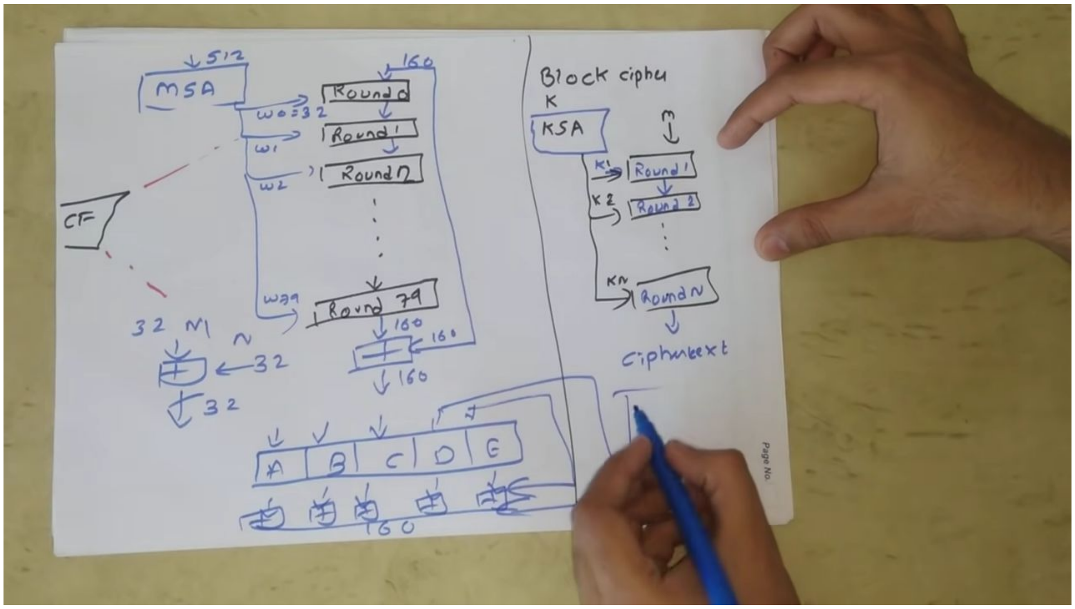
▷ 7:45


MSA
160
Round 0
Round 1
Round n
CF
Block ciphu
K
KSA
m
K1
Round 1
K2
Round 2
KN
Round N
ciphertext

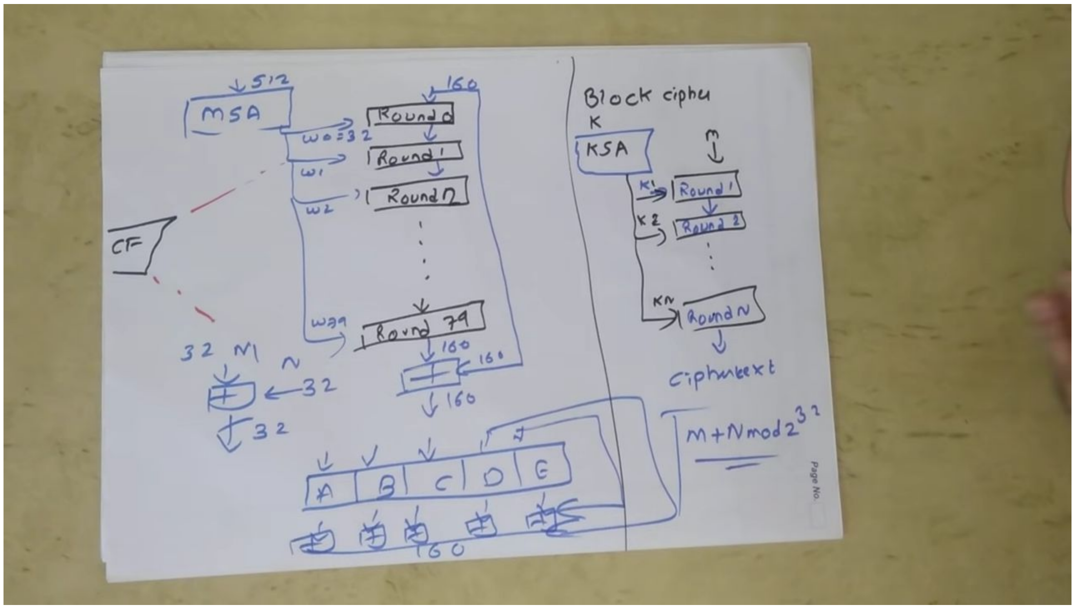
▷ 8:41


512
MSA
160
Round 0
W0=32
Round 1
W1
W2
Round n
W79
Round 79
160
160
160
CF
Block ciphu
K
KSA
m
K1
Round 1
K2
Round 2
KN
Round N
ciphertext

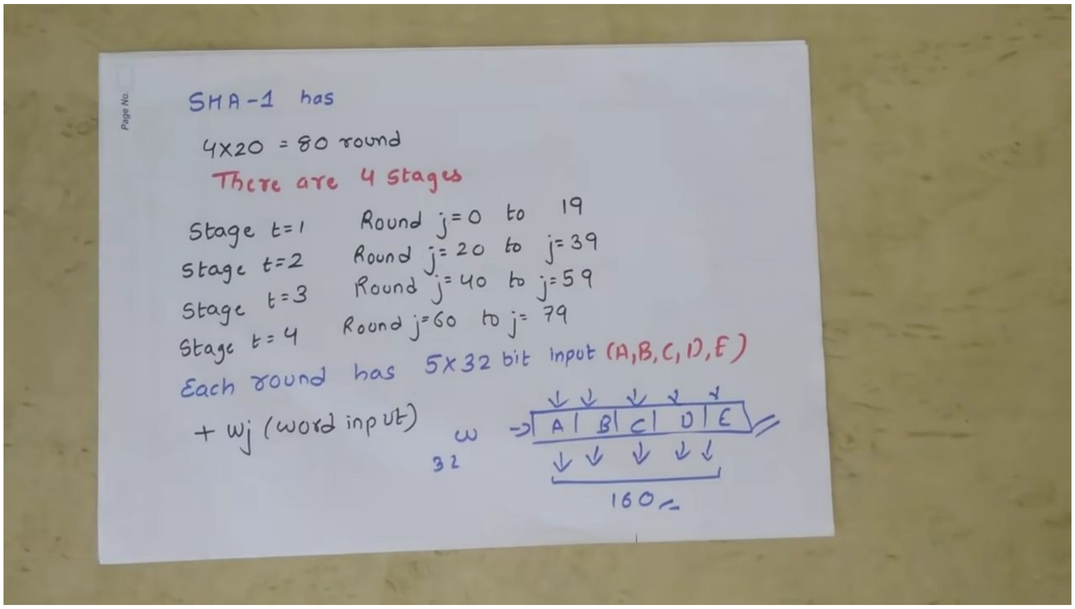
▷ 9:30


512
MSA
W0=32
W1
W2
W79
160
Round 0
Round 1
Round 2
Round 79
160
160
160
CF
32
M
N
32
32
A
B
C
D
E
160
Block cipher
K
KSA
m
K1
Round 1
K2
Round 2
Kn
Round N
ciphertext

▷ 12:16


512
MSA
W0=32
W1
W2
W79
160
Round 0
Round 1
Round 2
Round 79
160
160
160
CF
32
M
N
32
32
A
B
C
D
E
160
Block cipher
K
KSA
m
K1
Round 1
K2
Round 2
Kn
Round N
ciphertext
M+N mod 2^32

▷ 12:35



Page No.

SHA-1 has

4x20 = 80 round

There are 4 stages

Stage t=1 Round j=0 to 19

stage t=2 Round j=20 to j=39

stage t=3 Round j=40 to j=59

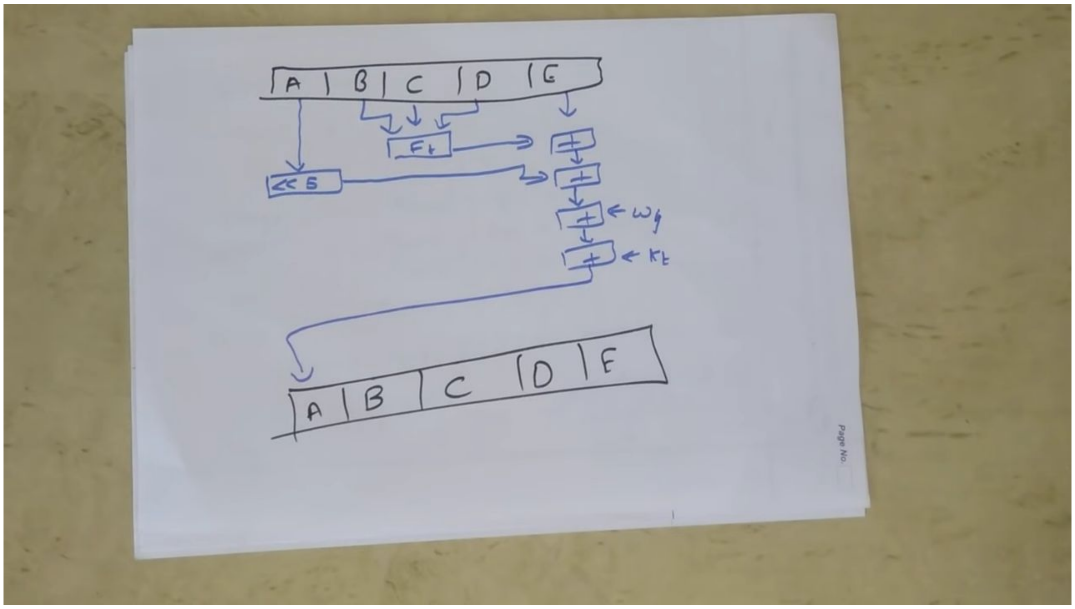
Stage t=4 Round j=60 to j=79

Each round has 5x32 bit input (A,B,C,D,E)

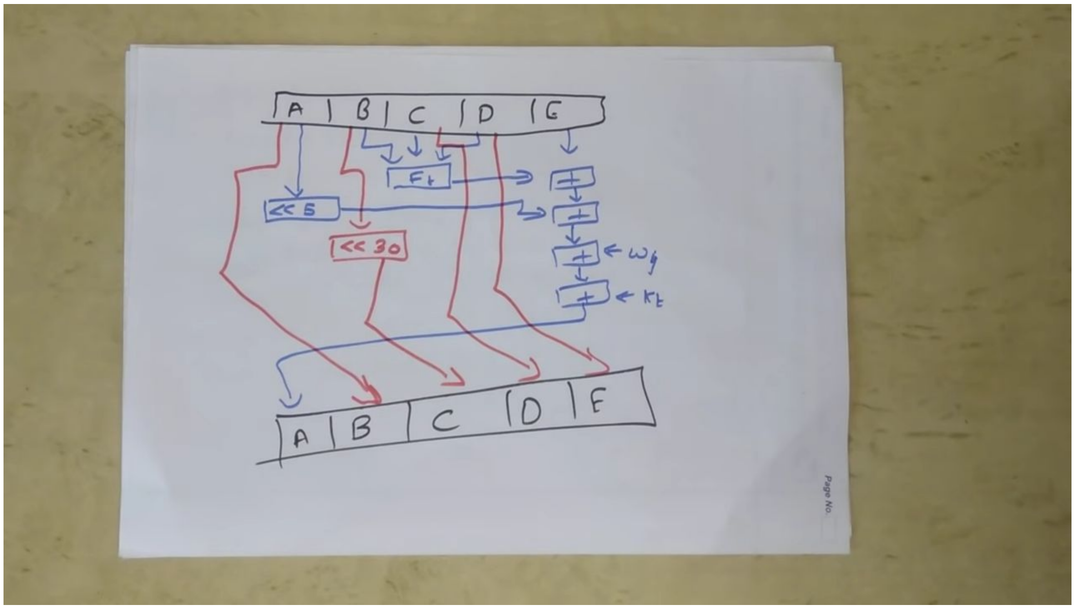
+ wj (word input)

ω
32
A
B
C
D
E
160

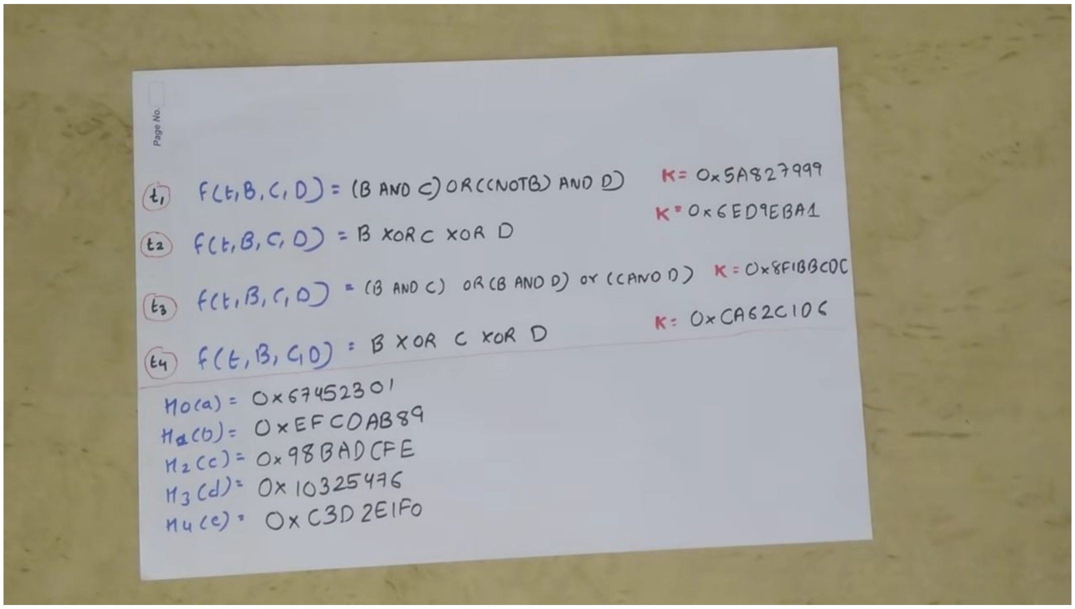
▷ 13:06



▷ 17:42



▷ 18:40



t1 F(t, B, C, D) = (B AND C) OR ((NOT B) AND D) K = 0x5A827999

t2 F(t, B, C, D) = B XOR C XOR D K = 0x6ED9EBA1

t3 F(t, B, C, D) = (B AND C) OR (B AND D) or (C AND D) K = 0x8F1BBCDC

t4 F(t, B, C, D) = B XOR C XOR D K = 0xCA62C1D6

H_0(a) = 0x67452301
H_1(b) = 0xEFCDAB89
H_2(c) = 0x98BADCFE
H_3(d) = 0x10325476
H_4(e) = 0xC3D2E1F0

▷ 19:05