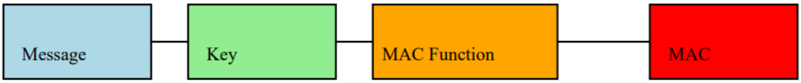
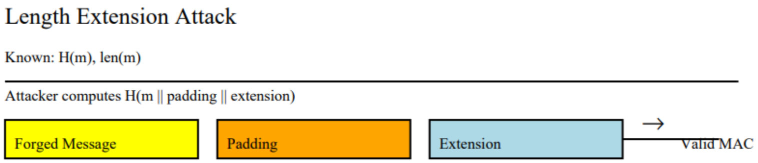
Below are diagrams illustrating various cryptographic concepts, including Message Authentication Codes (MAC), length extension attacks, and the SHA-1 hashing algorithm,MD5, HMAC. Each diagram is clearly labeled to reflect its corresponding topic.

Below is an illustration of how a MAC is generated and verified

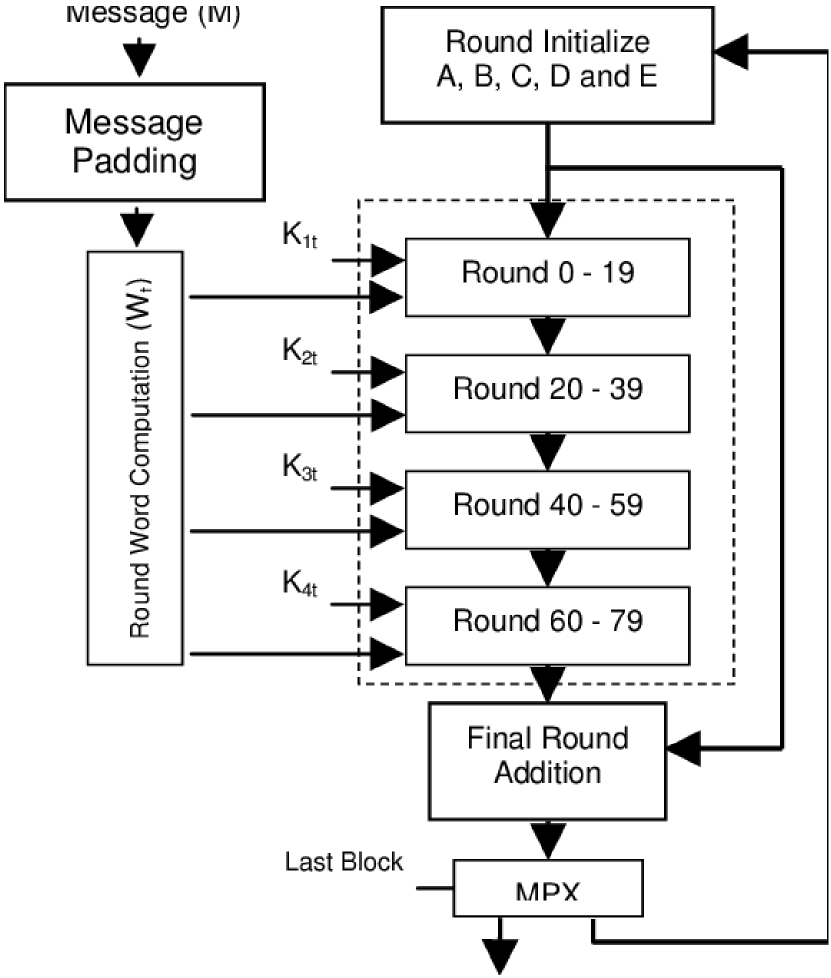



Length Extension Attack

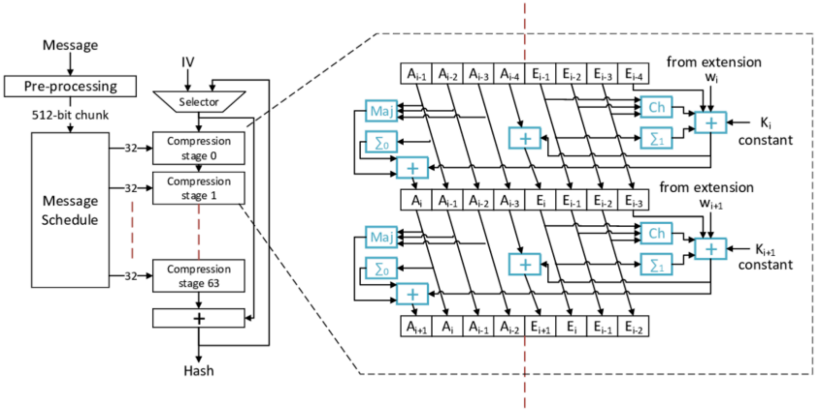
Known: H(m), len(m)

Attacker computes H(m || padding || extension)

ShA-1 :


Message (M)
Message Padding
Round Word Computation (W_t)
Round Initialize A, B, C, D and E
K_{1t}
Round 0 - 19
K_{2t}
Round 20 - 39
K_{3t}
Round 40 - 59
K_{4t}
Round 60 - 79
Final Round Addition
Last Block
MPX

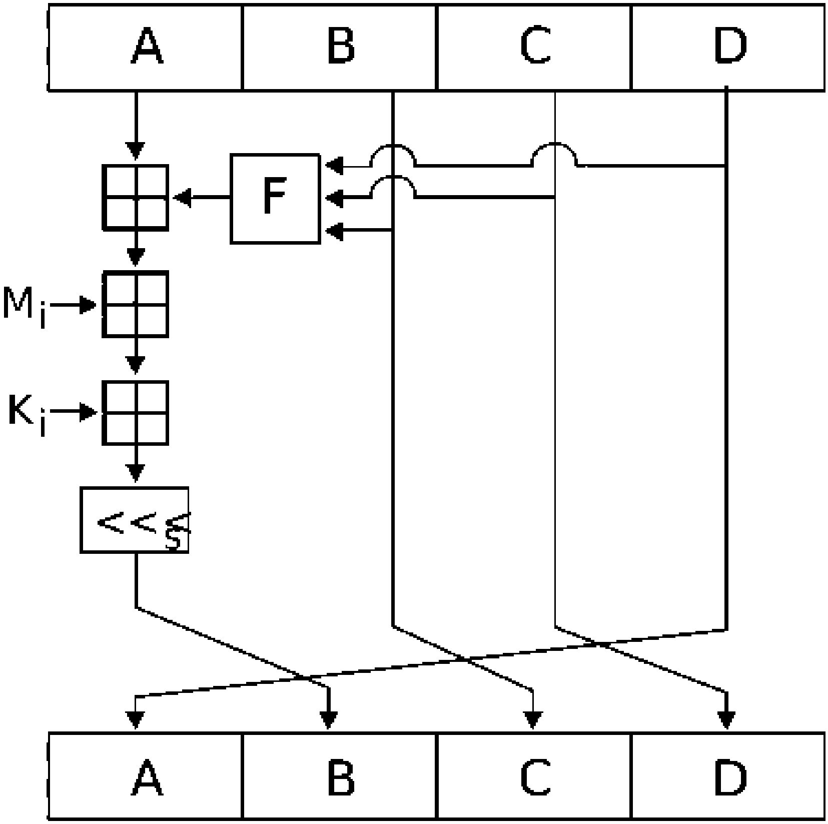
ShA-256 :



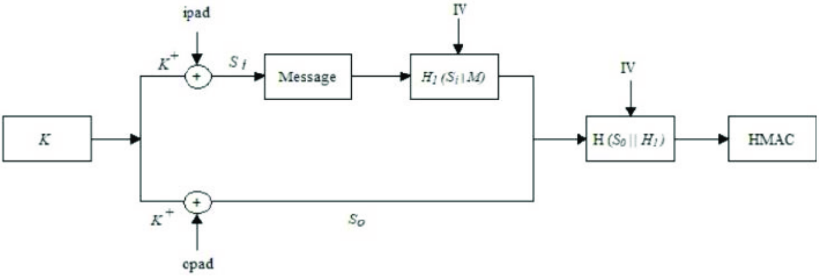
(a) SHA-256 Function

(b) Compression Stages

MD5 :



HMAC Algorithm :


ipad
IV
K^+
S_i
Message
$H_1 (S_i | M)$
IV
K
H (S_0 || H_1)
HMAC
K^+
S_o
opad