B) 100 - 100 - 100

C(0) C(1) C(2) C(3)

111 100 110 101

C) 111 → 011 (⊗111 → 100) P(0)
000 (⊗100 → 100) P(2)
010 (⊗100 → 110) P(3)

m_0 m_1 m_2 m_3

111 - 100 - 100 - 110

100 ⊗111 → KS(011) → 100
100 ⊗100 → KS(000) → 110
100 ⊗110 → KS(010) → 101

6) $n = pq$ $z = (p-1)(q-1)$

a) $n = 55$ $z = 40$ $p = 5$, $q = 11$

b) 3 and z do not share common factors. In relation to p and q, they're prime. (e, & z) → (3, 40] Relatively Prime.

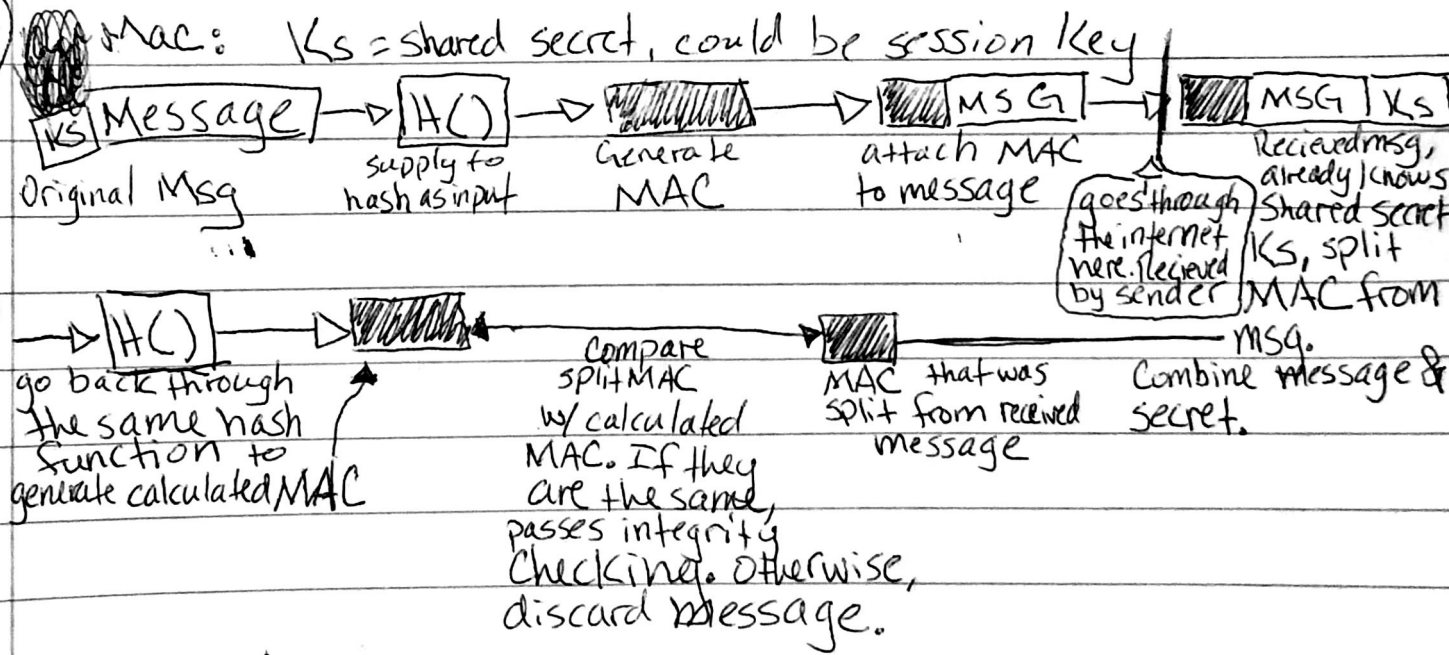
c) ed mod $z = 1$ → $ed = x \cdot z + 1$ → $3 \cdot d = x \cdot 40 + 1$ ⇒

$3d = 2 \cdot 40 + 1$ ⇒ **$d = 27$**, $x = 2$

d) Public = (55, 3) private = (55, 27) $m = 8$

$m^e \bmod n = 8^3 \bmod 55 = 17$ $C = 17$

7)



A message authentication code is a short piece of information used to authenticate/verify the sender aswell as message integrity.