

B) $100 - 100 - 100$

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

$$\begin{array}{r} 100 \\ \otimes 111 \\ \hline K_S(011) \\ \downarrow \\ 100 \end{array} \quad \begin{array}{r} 100 \\ \otimes 100 \\ \hline K_S(000) \\ \downarrow \\ 110 \end{array} \quad \begin{array}{r} 100 \\ \otimes 110 \\ \hline K_S(010) \\ \downarrow \\ 101 \end{array}$$

C)

$$\begin{array}{r} 111 \\ \otimes 111 \\ \hline 100 \\ p(1) \end{array} \quad \begin{array}{r} 100 \\ \downarrow \\ 011 \\ \otimes 111 \\ \hline 100 \\ p(2) \end{array} \quad \begin{array}{r} 110 \\ \downarrow \\ 000 \\ \otimes 100 \\ \hline 100 \\ p(3) \end{array} \quad \begin{array}{r} 101 \\ \downarrow \\ 010 \\ \otimes 100 \\ \hline 110 \end{array}$$

$m_0 \ m_1 \ m_2 \ m_3$

$111 - 100 - 100 - 110$

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. $(e, z) \rightarrow (3, 40)$ Relatively Prime.

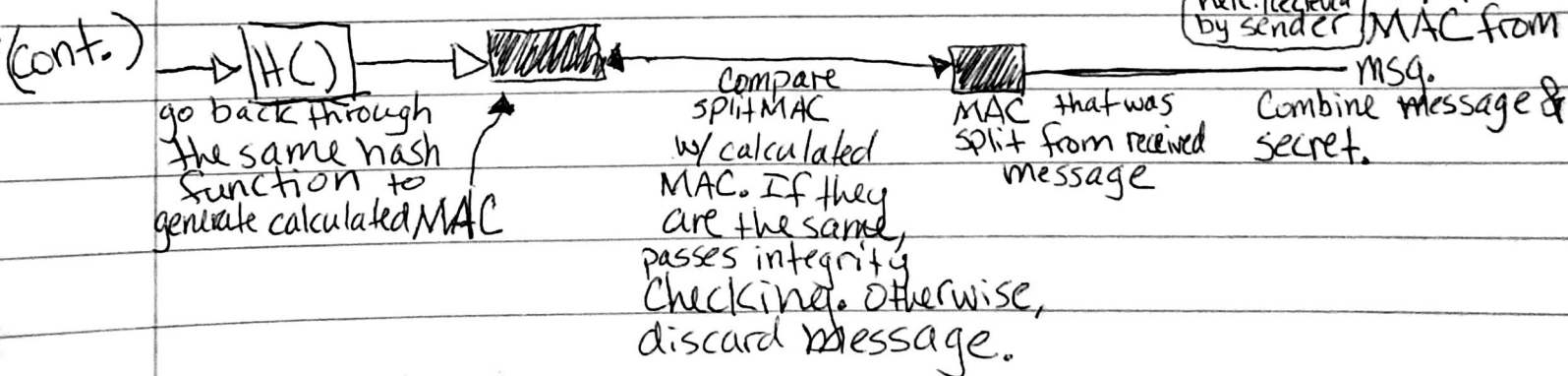
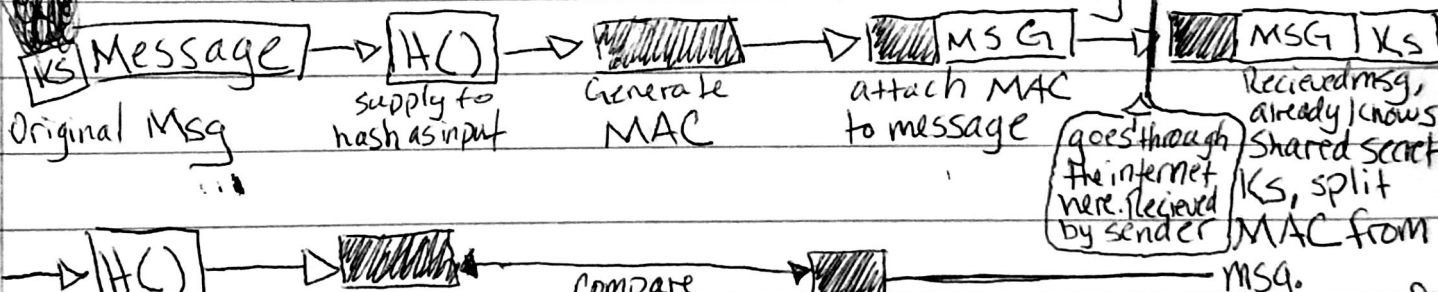
c) $ed \bmod z = 1 \rightarrow ed = x \cdot z + 1 \rightarrow 3 \cdot d = x \cdot 40 + 1 \Rightarrow$

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

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

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

7) Mac: $K_S =$ shared secret, could be session key



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