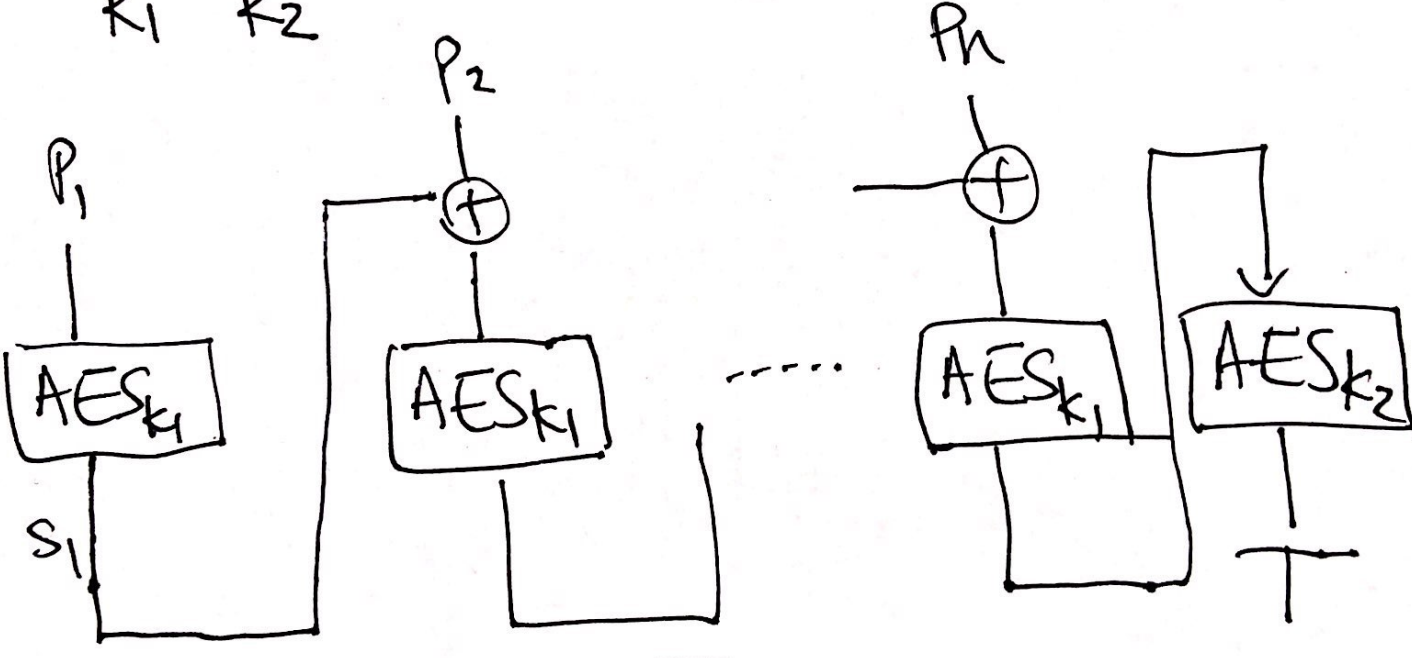
AES-EMAC

$MAC(K, M) = T$ $\quad M = P_1 \| \dots \| P_n$ (concat)

K_1 K_2



Consider $H(M) = \underbrace{MAC(\check{K}, M)}_{\text{hash definition}}$ known to attacker

$P_1 \| P_2 \| \dots P_n \to T$

$(S_1 \oplus P_2) \| \dots P_n \to T$

HMAC both a MAC and collision resistant when the attacker has key k

$$HMAC(K, M) = H\left(K \oplus opad \,||\, H(K \oplus ipad \,||\, M)\right)$$

assume H is a collision resistant hash

$0x5C...5C$ $0x36...36$

Why collision resistant? Because H is CR

Assume $HMAC(K, M_1) = HMAC(K, M_2)$

$\Rightarrow K \oplus opad \,||\, H(K \oplus ipad \,||\, M_1) =$

$= K \oplus opad \,||\, H(K \oplus ipad \,||\, M_2)$

$\Rightarrow K \oplus ipad \,||\, M_1 = K \oplus ipad \,||\, M_2$

$\Rightarrow M_1 = M_2$