AES-EMAC

\[ \text{MAC}(K, M) = T \quad M = P_1 P_2 \ldots P_n \]

\[ K_1 \quad K_2 \]

\[ P_1 \]

\[ \text{AES}_{K_1} \]

\[ S_1 \]

\[ P_2 \]

\[ \text{AES}_{K_1} \]

\[ \ldots \]

\[ \text{AES}_{K_1} \]

\[ \text{AES}_{K_2} \]

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

\[ P_i \cup P_2 \cup \ldots \cup P_n \rightarrow T \]

\[ (S_1 \oplus P_2) \rightarrow P_n \rightarrow T \]
HMAC is both a MAC and collision resistant when the attacker has key $K$.

\[ \text{HMAC}(K, M) = H(K \oplus \text{pad} || H(K \oplus \text{ipad} || M)) \]

Assume $H$ is a collision resistant hash $0x5c...5c$ $0x36...3c$

Why collision resistant? Because $H$ is CR

Assume $H(\text{HMAC}(K, M_1)) = \text{HMAC}(K, M_2)$

\[ \Rightarrow K \oplus \text{pad} || H(K \oplus \text{ipad} || M_1) = K \oplus \text{pad} || H(K \oplus \text{ipad} || M_2) \]

\[ \Rightarrow K \oplus \text{ipad} || M_1 = K \oplus \text{ipad} || M_2 \]

\[ \Rightarrow M_1 = M_2 \]