CSS322 – Message Authentication Codes Notes

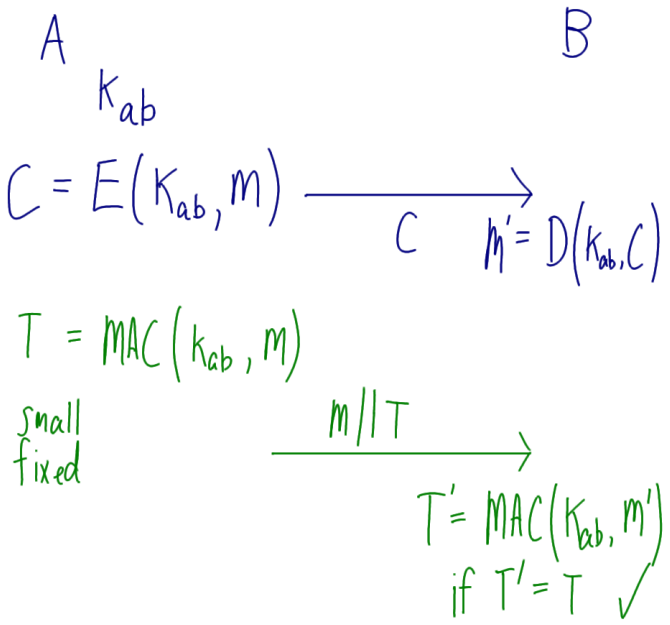

Figure 1: Symmetric Encryption vs MAC for Authentication; Lecture 14

$$T_1 = MAC(K_1, m_1)$$
$$T_2 = MAC(K_2, m_1)$$
$$T_3 = MAC(K_1, m_2)$$

Figure 2: Desired Properties of MAC Function; Lecture 14

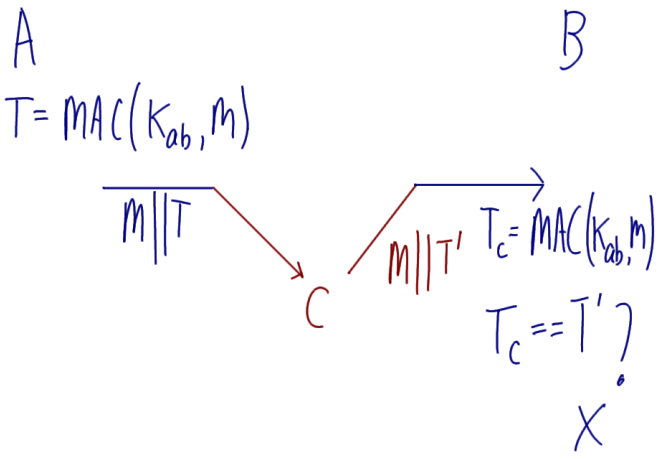

Figure 3: Attack on MAC: Change T; Lecture 14

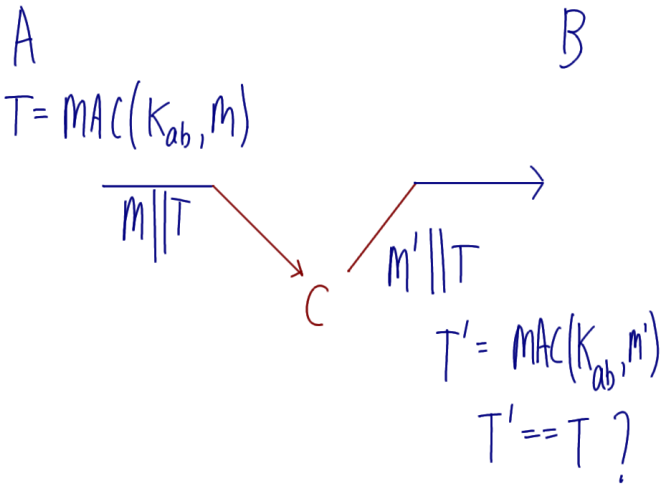

Figure 4: Attack on MAC: Change M; Lecture 14

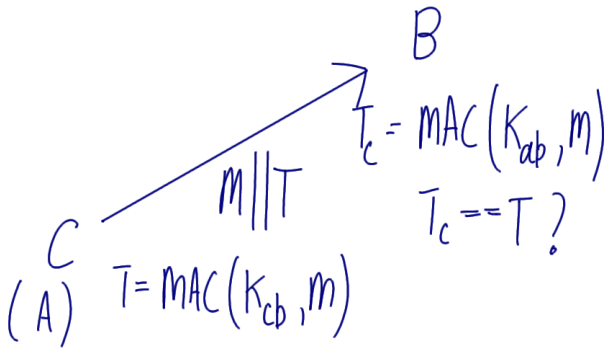

Figure 5: Attack on MAC: Masquerade; Lecture 14

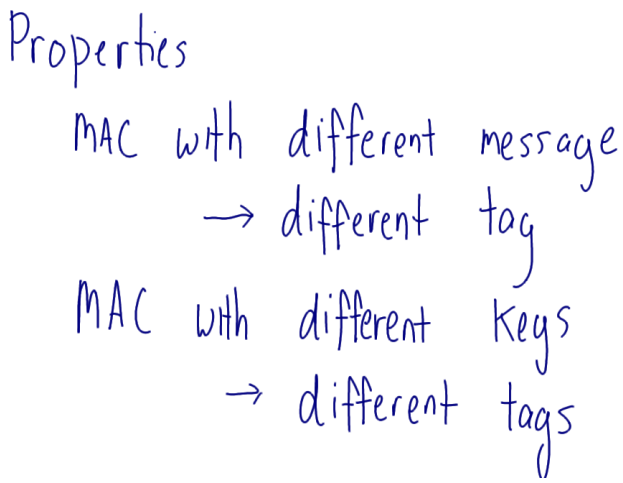

Figure 6: Required Properties of MAC Function; Lecture 15

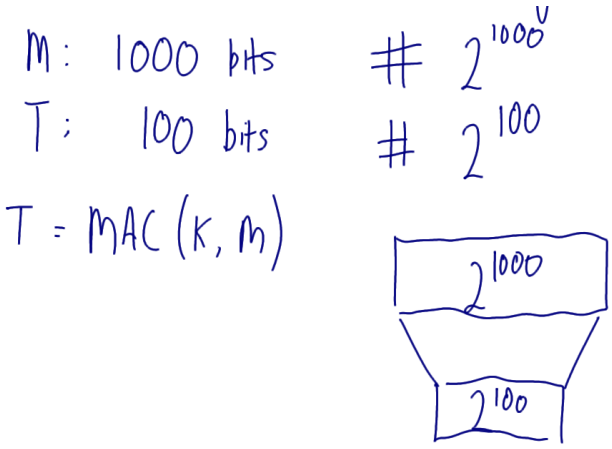

Figure 7: MAC Function: Many Messages Map to Same Tag; Lecture 15

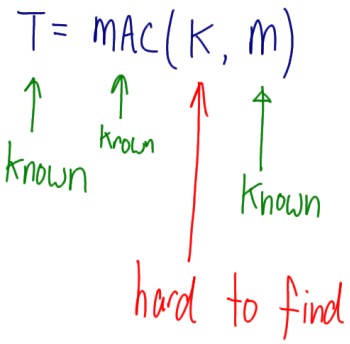

Figure 8: MAC Brute Force Attack; Lecture 15

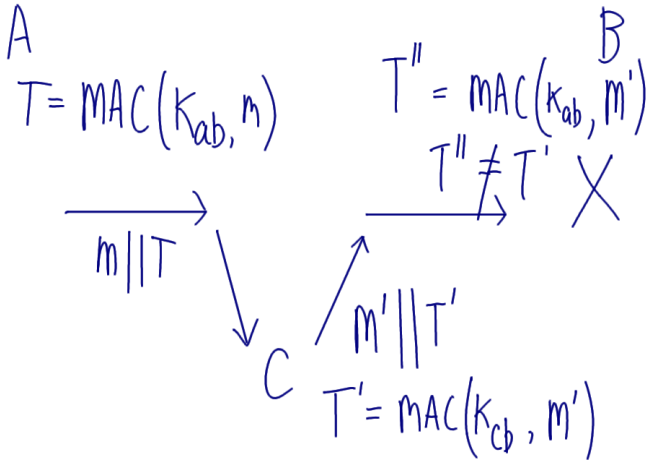

Figure 9: Attack on MAC: Change M and T; Lecture 15