ITS335 – Message Authentication Codes Notes

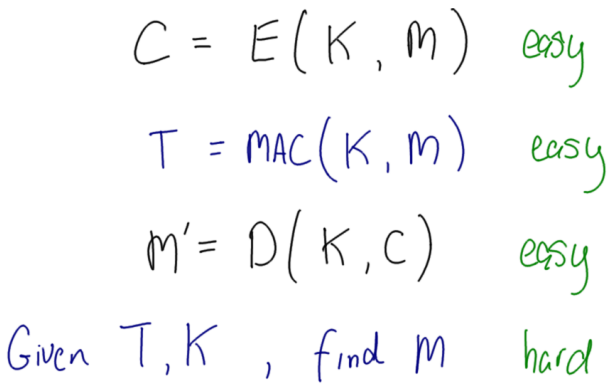

Figure 1: MAC function vs Encrypt function; Lecture 17

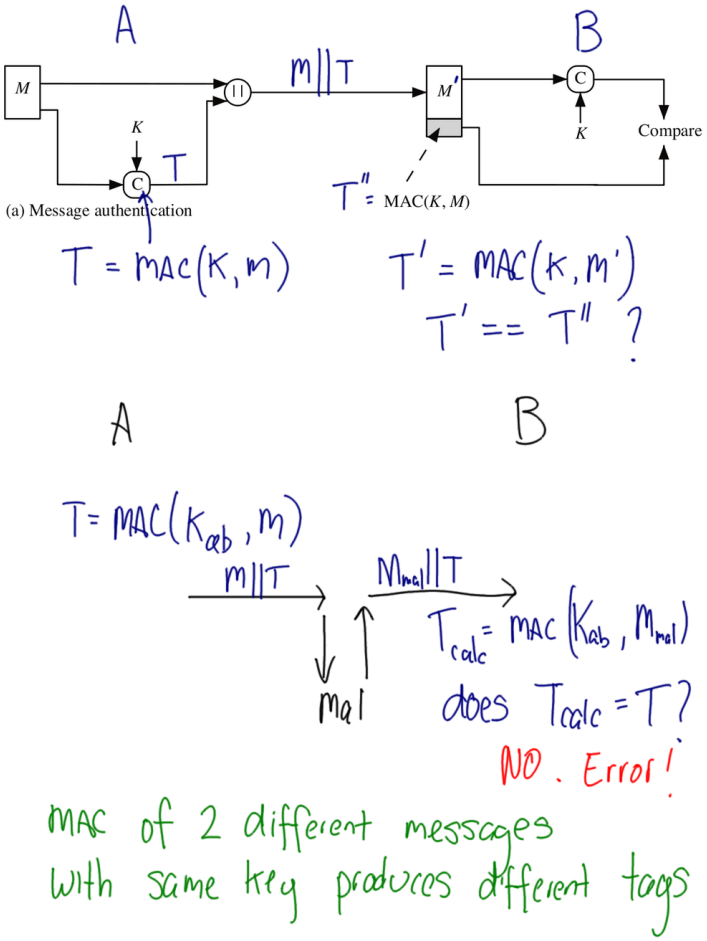

Figure 2: Authentication Attack on MAC by Changing Message; Lecture 17

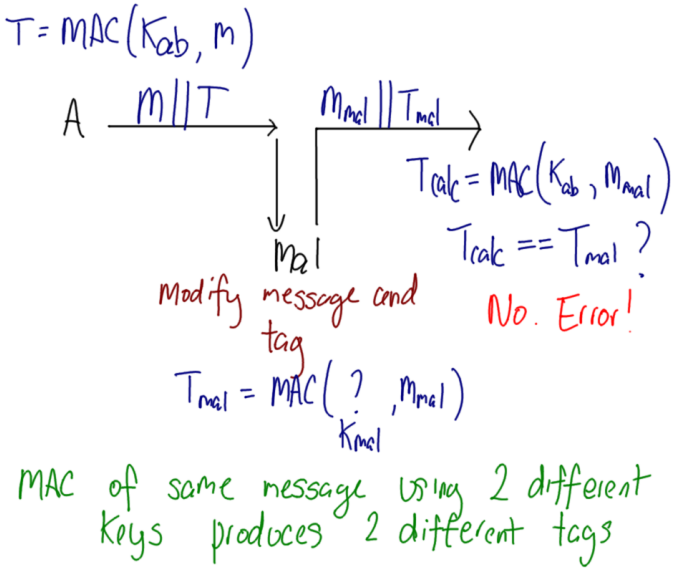

Figure 3: Authentication Attack on MAC by Changing Message and Tag; Lecture 17

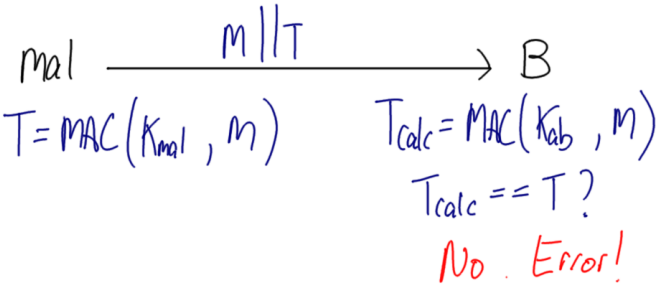

Figure 4: Authentication Attack on MAC by Masquerade; Lecture 17

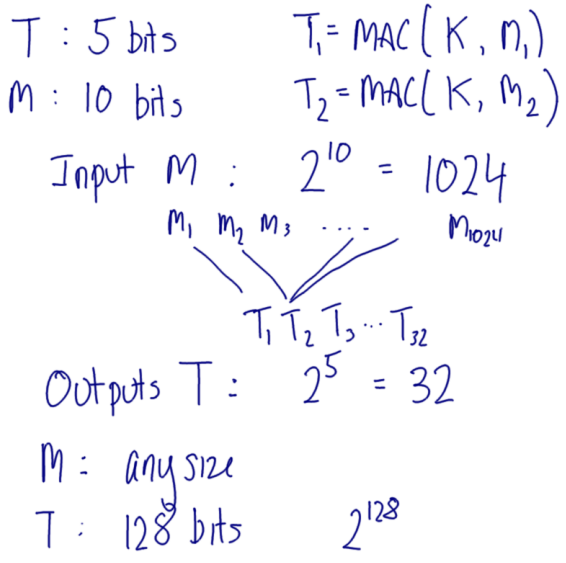

Figure 5: MAC collisions; Lecture 17

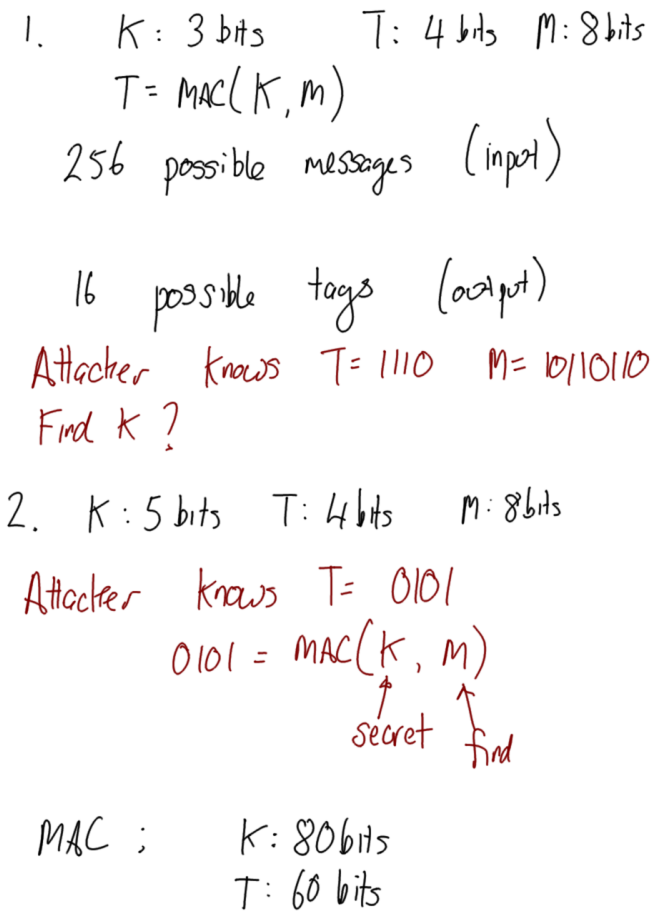

Figure 6: Brute Force Attack on MAC Key and Tag; Lecture 18