

ITS335 – Message Authentication Codes Notes

$$\begin{aligned}C &= E(K, m) && \text{easy} \\T &= \text{MAC}(K, m) && \text{easy} \\m' &= D(K, C) && \text{easy} \\ \text{Given } T, K, & \text{ , find } m && \text{hard}\end{aligned}$$

Figure 1: MAC function vs Encrypt function; Lecture 17

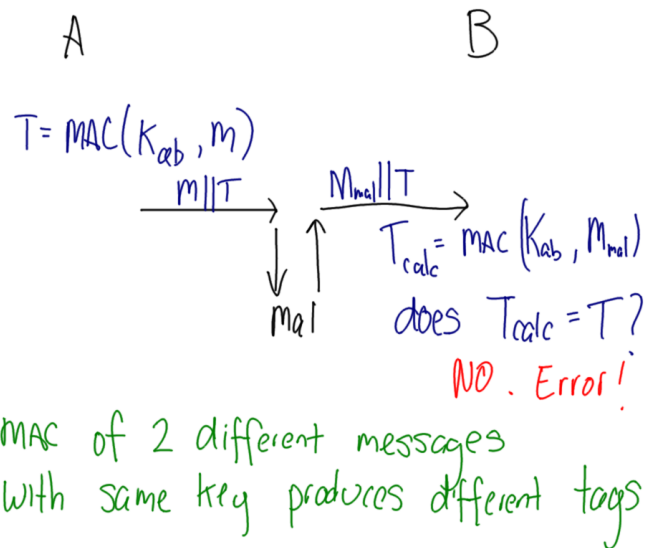
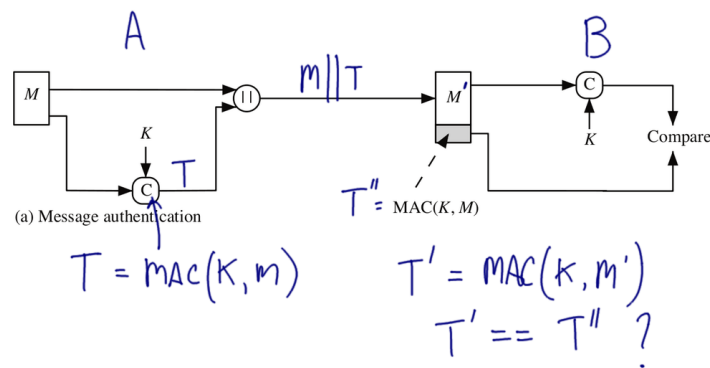


Figure 2: Authentication Attack on MAC by Changing Message; Lecture 17

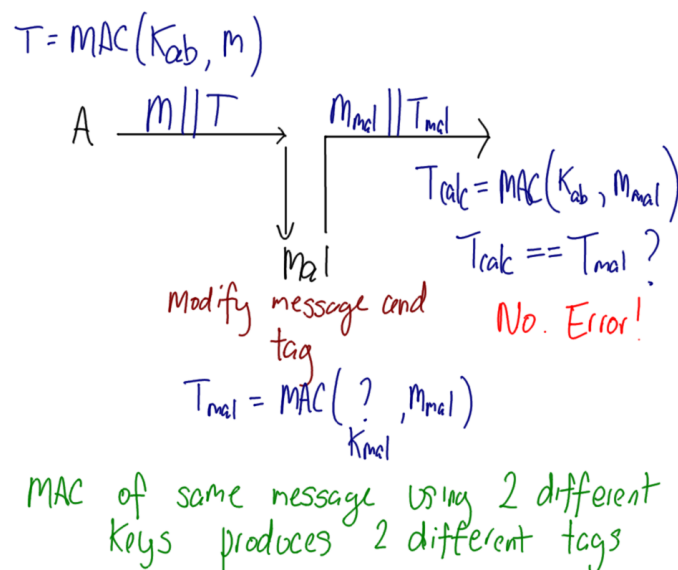


Figure 3: Authentication Attack on MAC by Changing Message and Tag; Lecture 17

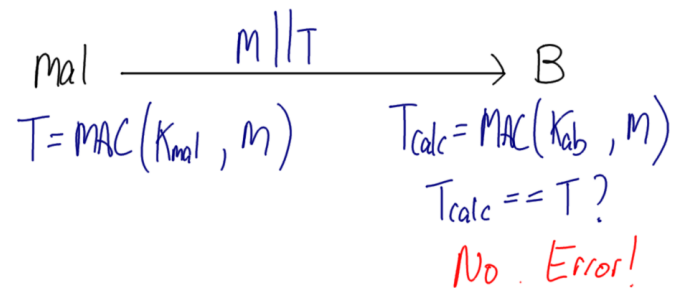


Figure 4: Authentication Attack on MAC by Masquerade; Lecture 17

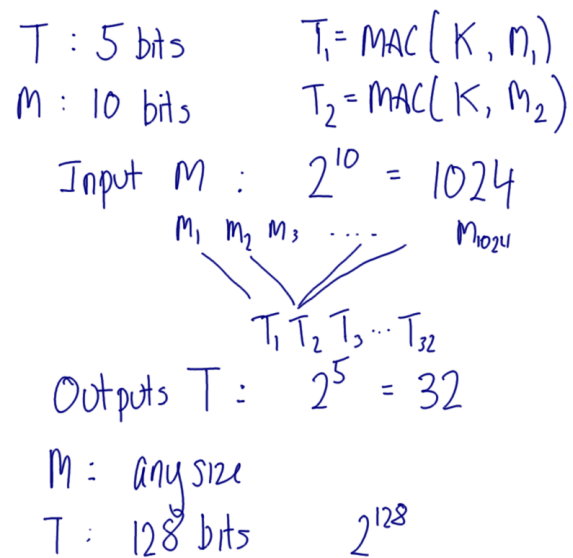


Figure 5: MAC collisions; Lecture 17

1. $K: 3 \text{ bits}$ $T: 4 \text{ bits}$ $M: 8 \text{ bits}$
 $T = \text{MAC}(K, m)$
 256 possible messages (input)

 16 possible tags (output)
 Attacker knows $T = 1110$ $M = 10110110$
 Find K ?
2. $K: 5 \text{ bits}$ $T: 4 \text{ bits}$ $M: 8 \text{ bits}$
 Attacker knows $T = 0101$
 $0101 = \text{MAC}(K, m)$

$\uparrow$ $\uparrow$
 secret find

 $\text{MAC} ;$ $K: 80 \text{ bits}$
 $T: 60 \text{ bits}$

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