Quiz/Attendance 7F

Total:

Firstname Lastname **ID#**

1. Adversary A attacks the MAC $F : \mathcal{K} \times \mathcal{M} \to \{0,1\}^t$. It asks a query M_1 and gets back a tag $T_1 = F_K(M_1)$; then it asks a query M_2 and gets back a tag $T_2 = F_K(M_2)$. Adversary A then outputs a pair (M_3, T_3) and halts. Adversary A is said to *forge* (or *win*) if the following conditions hold:

Be succinct and precise. Your answer is the AND of some Boolean conditions. Use the named variables and not English.

2. From MT.1: How many possible *cycles* are there on $\{0,1\}^8$, the space of 1-byte strings?

A cycle $C : S \to S$ on a finite set S is a permutation C for which $S = \{x, C(x), C(C(x)), \ldots\}$ for any $x \in S$.