ENEE/CMSC/MATH 456: Introduction to Cryptology
CRHF Class Exercise 3/25/19

Let (Gen, H) be a collision-resistant hash function and let F be a PRF. For each of the following, state whether $\widehat{H}$ is necessarily collision resistant. Justify your answer.

1. $\widehat{H}^s(x_1||x_2) = H^s(x_1 \oplus F_s(x_2))$

2. $\widehat{H}^s(x_1||x_2) = H^s(H^s(x_1)||x_2)$