Eric Altenburg CS-306 October 6, 2020

Lecture 6 - MACs & Hashing

6.2

1. Desired properties for MACs
   - efficiency: key gen & message transformations are fast
   - correctness: for all m and k, it holds that Vrf$_k$(m, Mac$_k$(m)) = ACCEPT
   - security: one cannot forge a fake verifiable pair m', t'
2. Conventions
   - Random key selection
     - typically, Gen selects key k uniformly at random from key space K
   - Canonical verification
     - when MAC is deterministic, Vrf typically amounts to re-computing the tag t
       - Vrf$_k$(m, t):
         1. t' := MAC$_k$(m)
         2. if t = t', output ACCEPT else output REJECT