CS 346 Class Notes

Mark Lindberg

May 4, 2016

This Time:
LAST DAY.
Substitute prof.

- Gen: $(N, e, d) = \mathsf{GenRSA}(1^n)$. $pk = \langle N, e \rangle$, $sk = \langle N, d \rangle$.
- Sign: Compute $\sigma := [m^d \mod N]$.
- Vrfy: $m \stackrel{?}{=} [\sigma^e \mod N]$.

I cannot read what he's writing. That is an absolutely miserable marker.
He covered the secure version.
Exam stuffs.
12.7 and 12.8 are not on the final.