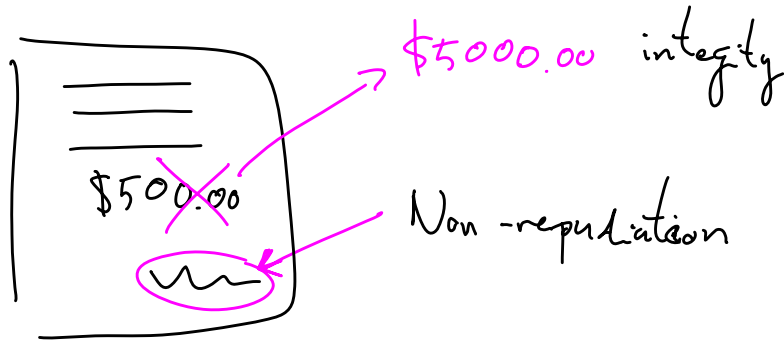


Lecture 26

Signatures



m : message

$$m \xrightarrow{K_A^+} K_A^+(m) \xrightarrow{K_A^-} K_A^-(K_A^+(m)) = m$$

B A

$$K_A^+(m, K_B^-(m)) \rightarrow m, K_B^+(K_B^-(m)) \quad \text{check} = ?$$

$$m, K_B^-(H(m)) \quad H(m) \quad K_B^+(K_B^-(H(m))) = ?$$

