

(pure) encryption ensures confidentiality ...

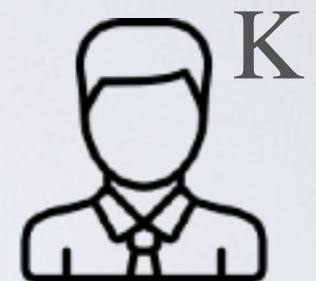
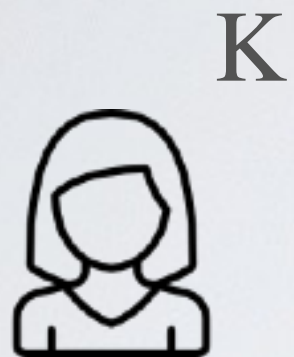


$E_k(m) = \text{tkS3bffBp} \dots$

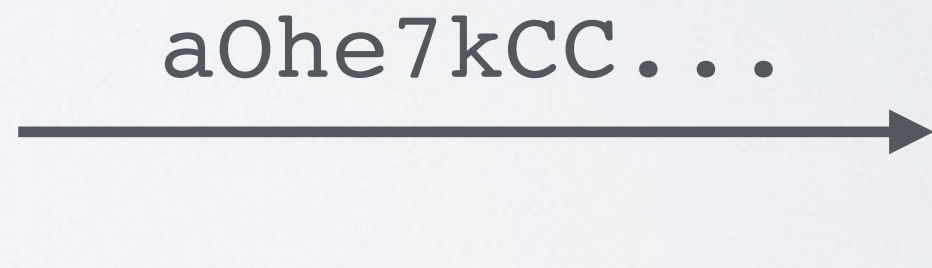
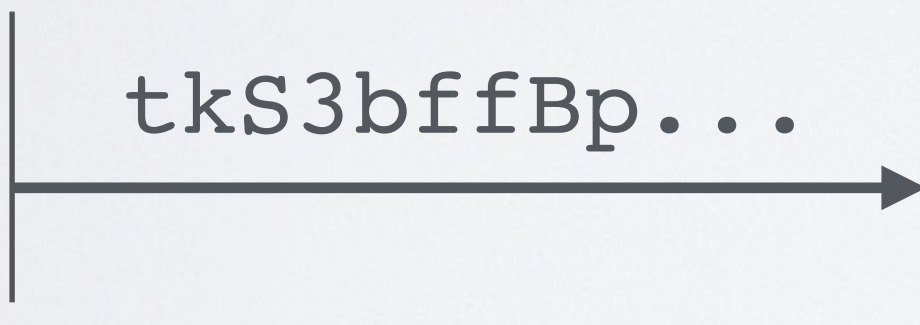


$D_k(\text{"tkS3bffBp} \dots \text{"}) = m$

... but does not ensure integrity !



$E_K(m) = \text{tkS3bffBp} \dots$



$D_K(\text{"a0he7kCC} \dots \text{"}) = m'$

⦿ Encrypting a message does not authenticate it