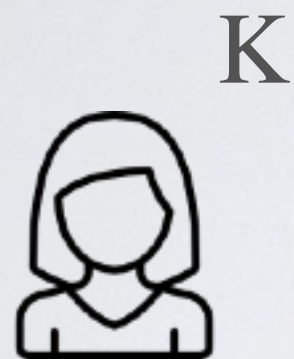
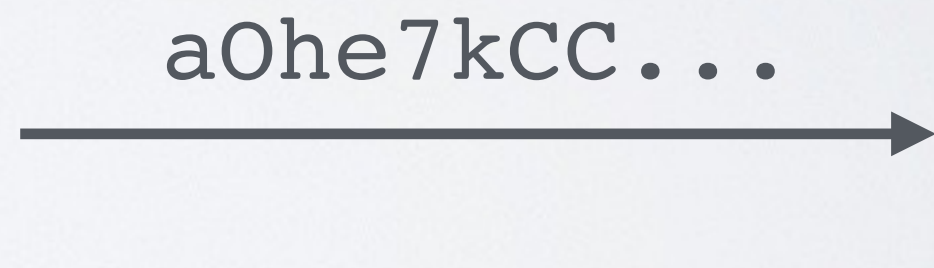
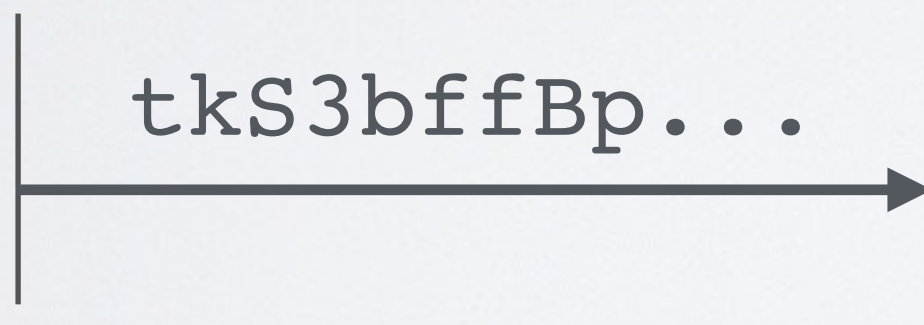


(pure) encryption ensures confidentiality ...



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



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

⦿ Encrypting a message does not authenticate it

One more issue ...



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



● How does Alice and Bob agree on a symmetric key?