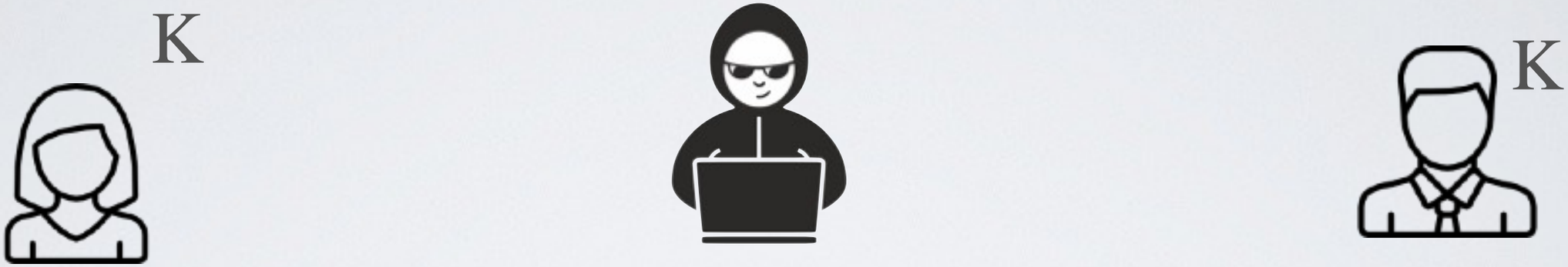
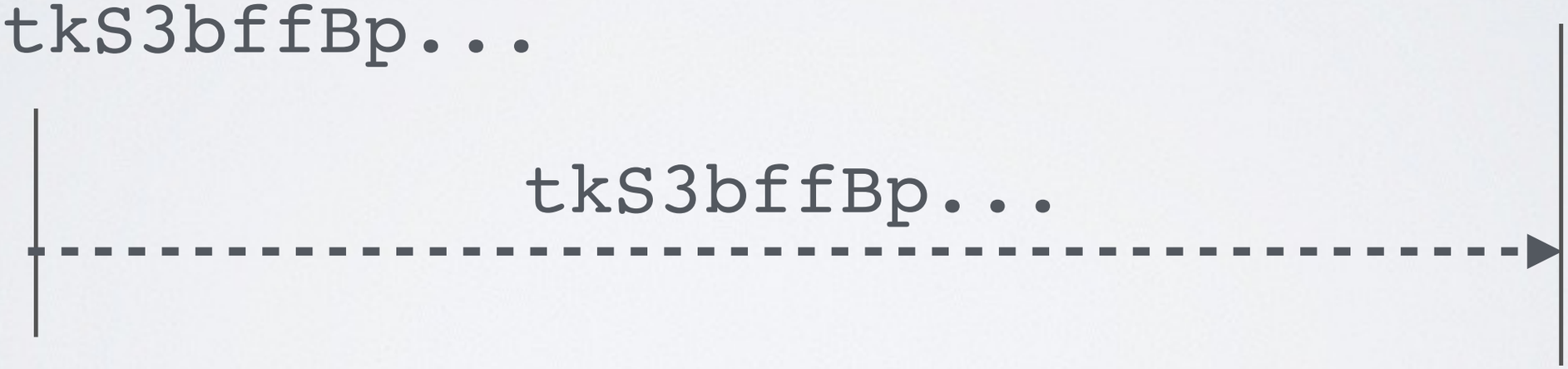
... but does not ensure integrity !



- Encrypting a message does not authenticate it

One more issue ...

$E_k(m)$ = `tkS3bffBp...`



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