

Security goals vs attacker's model

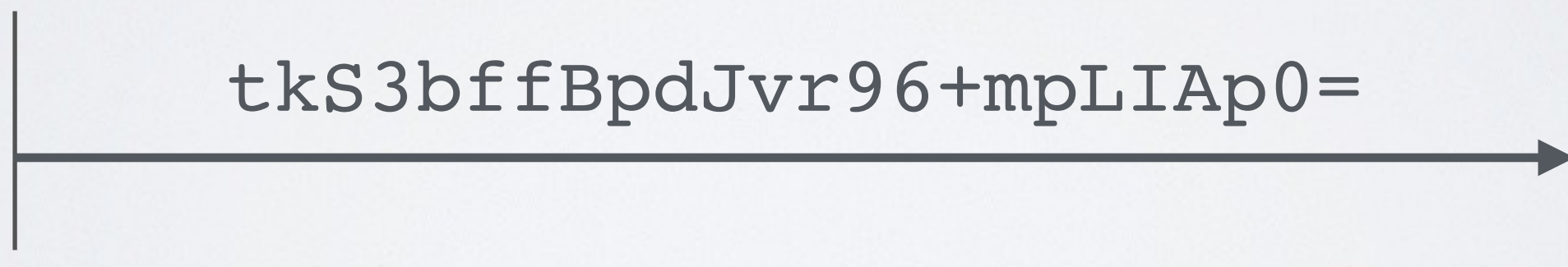


Let us consider **confidentiality, integrity and availability**

(pure) encryption ensures confidentiality ...



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



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