





# Non-repudiation as a special case of integrity

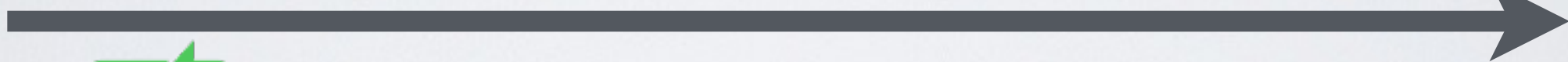
|                 | MAC   | Digital Signature   |
|-----------------|---|---|
| Integrity       |  |  |
| Non-repudiation |  |  |

# Digital Signatures and Confidentiality

$K_{sa}$  Alice's Secret Key



$K_{pa}, K_{pb}$  public keys



$K_{sb}$

1. Alice generates an asymmetric session key  $k$
2. Use both symmetric and asymmetric cryptography to **encrypt, sign and verify** the message and the key

$$E_{K_{pb}}(k) \parallel E_k(m \parallel E_{K_{sa}}(H(m)))$$