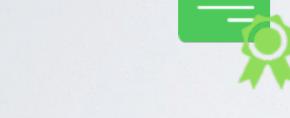
Digital Signature

Ksa Alice's Secret Key



Kpa, Kpb public keys





→ Use public cryptography to sign and verify

 $m \parallel SIG_{Ksa}(m)$

 $SIG_{Ksa}(m) = E_{Ksa}(H(m))$

Non-repudation as a special case of integrity

