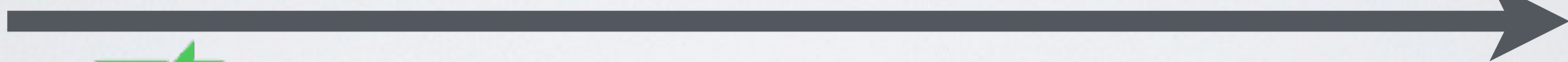


Digital Signature

K_{sa} Alice's Secret Key



K_{pa}, K_{pb} public keys





K_{sb}

➡ Use public cryptography to **sign and verify**

$$m \parallel \text{SIG}_{K_{sa}}(m)$$

$$\text{SIG}_{K_{sa}}(m) = E_{K_{sa}}(H(m))$$

Non-repudiation as a special case of integrity

	MAC	Digital Signature
Integrity		
Non-repudiation	