

ECDSA: Digital Signature Workflow

SIGNING (Alice)

VERIFICATION (Anyone)

Message
 m

Hash
 $h = \text{SHA256}(m)$

Sign with
Private Key

Signature
 (r, s)

Send:
 $m + (r, s)$

CRITICAL: Never reuse nonce!

Properties:

- Authentication
- Integrity
- Non-repudiation

Received
 $m, (r, s)$

Compute
 $h = \text{SHA256}(m)$

Verify with
Public Key

Valid?