Digital Signature

Integrity, Authen

User 1 msg: "Hello, I am here"

↓ hash function (SHA-256)

Produce a message digest

(1579811 7 ——)

User 2

↓

Encrypt the message digest (Digital Signature)

(by using private key of user1)

↓

"Hello I am here"

Encrypted (1579811 7 ——)

↓

User 2

"Hello I am here" → SHA 256 → digest

(1579811 7 ——)

Decrypt it using public key of sender

(1579811 7 ——)

Compare (if both match then integrity is maintained)