Asymmetric:

Privacy: Always encrypt with the receiver’s PUBLIC key. Receiver decrypts with receiver’s PRIVATE key which only that receiver has.

Authenticity: Sender will encrypt “something” with the sender’s PRIVATE key. When the receiver is able to successfully decrypt that “something” with that sender’s PUBLIC key, that proves it was encrypted with the sender’s PRIVATE key, which only the sender has.

Integrity: Create a message digest (hash) with a hashing algorithm (MD5, SHA-1, SHA 256)

Non-Repudiation. Sender encrypts hash with the sender’s private key. Receiver decrypts hash with sender’s public key. Receiver hashes document—if hashes match, receiver gets a guarantee that message has not been modified. This is called a digital signature.