

# Practice Exercise - Blockchain Cryptography

We have understood the working of both the Asymmetric Key Cryptography and Digital Signatures in Blockchain.

In this exercise we will combine the knowledge of both Asymmetric Key Cryptography and Digital Signature to provide a double layer of security, privacy, integrity and authenticity.

A combined use case is, Alice sends a signed message to Bob, she also protects this message from being read by anyone else. In this case, Alice will do the following activities...

- a. Alice encrypts the message using Bob's public key. Then sign the message using her private key. Finally sends this to Bob.
- b. Bob decrypts the message using Alice's public key. Then uses his private key to verify the message. Finally retrieve the original message.

Note: you need the package **cryptography** to work in this exercise