

Public / Private Key Encryption

- Bob wants to send a message to Alice
- He wants Alice to know it came from him
- The message contents can be read by others
- Bob gives away copies of his seal and signature
- Bob signs and seals messages before sending to Alice



```
// Bob generates a key pair and publishes his public key
let { publicKey, privateKey } = crypto_sign_keypair()

// Bob composes an important message
let message = 'Tonight is the meetup at 7pm'

// And signs it using his private key
let signature = crypto_sign_detached(message, privateKey)

// Alice gets the signed message and wants to verify it
let isVerified = crypto_sign_verify_detached(signature, message, publicKey)

console.log({message: message, isVerified: isVerified})
```