

How to sign & encrypt



- If Alice wants to send a signed message to Bob
Alice ciphers with Alice's private key and Bob deciphers with Alice's public key
- If Alice wants to send an encrypted message to Bob
Alice ciphers with Bob's public key and Bob deciphers with Bob's private key
- What if we want to send a signed encrypted message?
Alice ciphers with Alice's private + Bob's public and Bob deciphers with Alice's public + Bob's private
- !!! How do I know Bob's public key came from Bob?