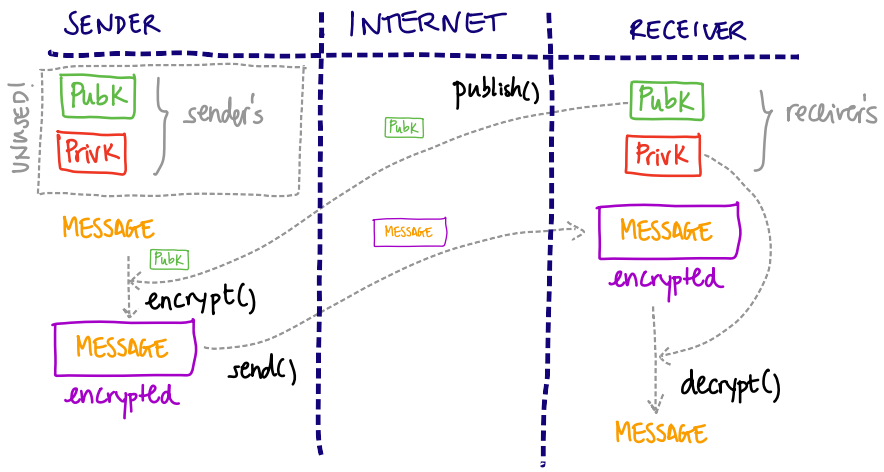
ASYMMETRIC CRYPTOGRAPHY: PRIVATE + PUBLIC KEYS

In asymmetric cryptography, each user has always 2 keys:

- Private key: never published, always kept secret. PrivK
- Public key: always published; it is obtained from the private key, but the private key cannot be obtained from the public key. PubK

① USE CASE: ENCRYPTION: Protect the content of a message from reading

Sender encrypts MESSAGE with PubK of the receiver. Receiver decrypts MESSAGE with their PrivK.



② USE CASE: DIGITAL SIGNATURES: Validate the authorship/authority of a message and the integrity of its content

Sender creates a signature of their MESSAGE using their PrivK

Receiver verifies that the MESSAGE comes unaltered from the sender with senders PubK