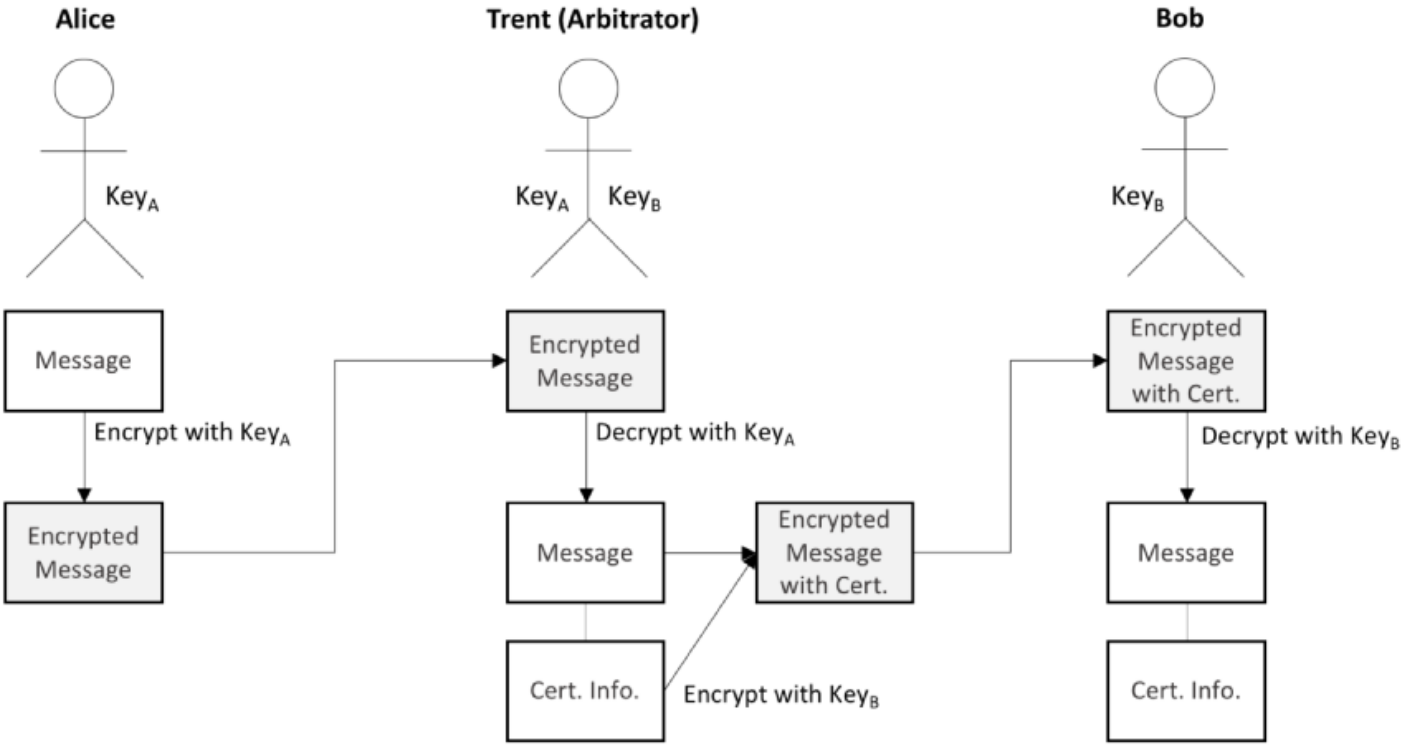
Digital Signatures

an ideal *physical* signature is:
- authentic: the signer deliberately signed the document
- unforgeable: someone should not be able to forge someone else's signature
- non-reusable: if one document is signed, that same signature cannot be used in another document
- unalterable: once signed, the document cannot be altered
- non-repudiated: the signer cannot deny signing the document

do physical signatures actually offer these features?
- to some extent

digital signatures
- a systematic, mathematical way to prove the authenticity and integrity of digital messages

digital signatures using symmetric cryptography
- messages can be digitally signed by involving a trusted arbitrator



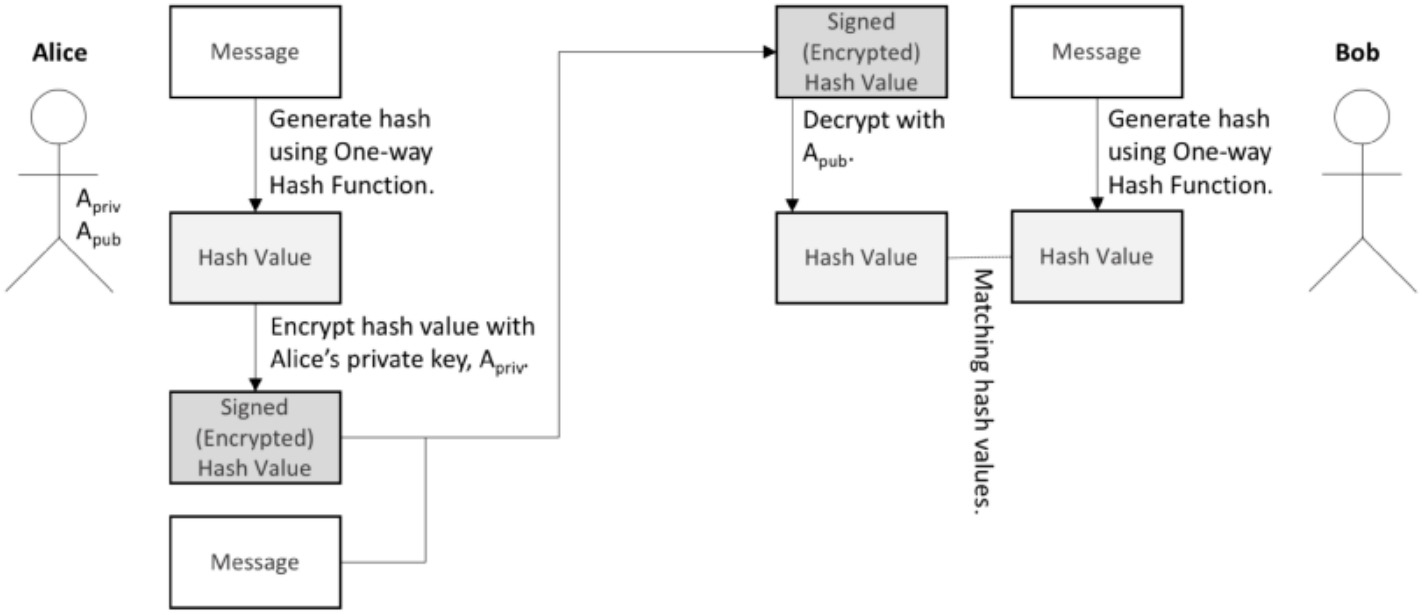
a trusted arbitrator shares two separate keys, K_A and K_B, with the sender and receiver respectively
the sender encrypts the document using the shared key, K_A, and sends it to the arbitrator
the arbitrator verifies that the document was encrypted using the key shared with the sender
the arbitrator adds some additional information certifying the signature (a bit like stamping)
- and encrypts the document and certification information with the shared key, K_B

the arbitrator sends this encrypted data to the receiver
the receiver decrypts the data and verifies the document and certification information

digital signatures using public-key cryptography
- a message can be digitally signed by encrypting it with the sender's private key
- the receiver can use the signer's public key to decrypt the message
- if the message is decrypted appropriately, then it must have been signed by the sender

also, the integrity of the message must have been preserved
since no one would be able to modify the message in transit without being able to decrypt it

digital signatures using one-way hash functions and public-key cryptography
some messages may be large
and signing them digitally using public-key cryptography may not be feasible
so generating a hash value of the message and signing the hash value is also valid
i.e., the hash of the message instead of the entire message is signed
using hash values to digitally sign a message is simpler and less-expensive
each party digitally signs their message with the hash value of the original message

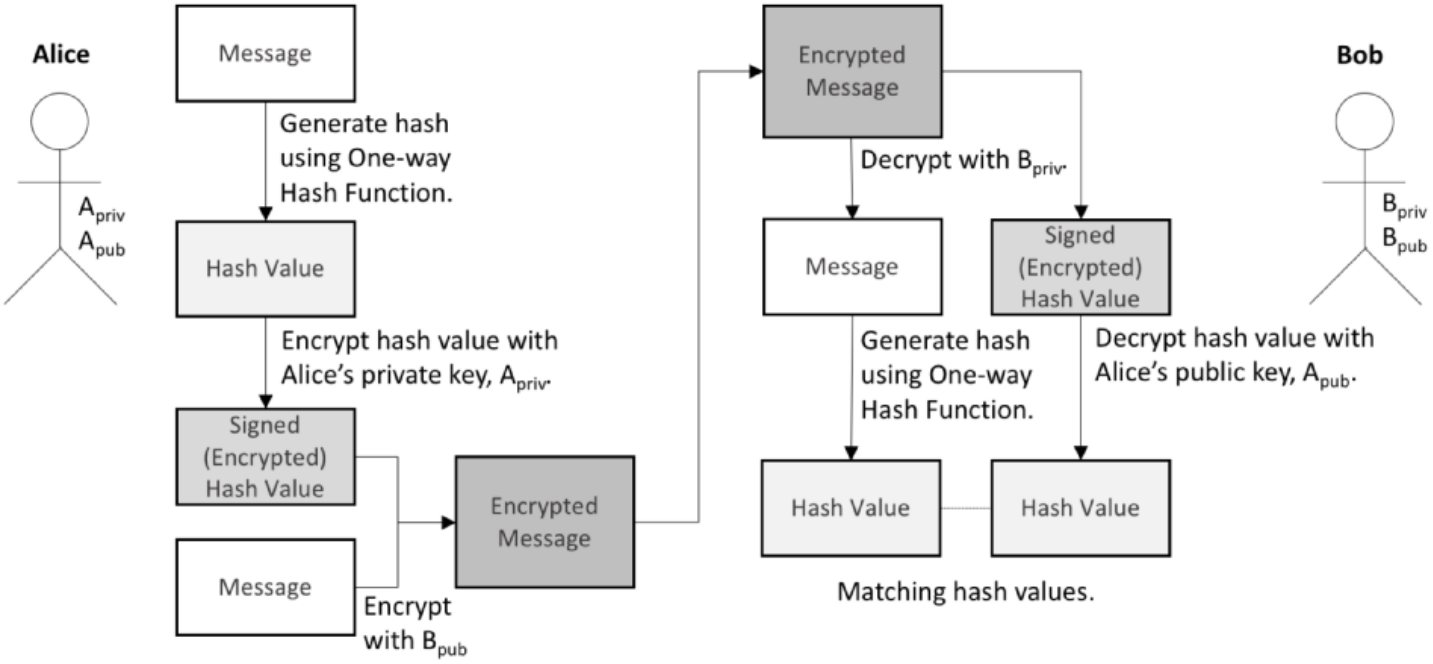


encrypted digital signatures

if the message must be signed and secured in transit

the signer can sign using a private key

they can then encrypt the message and signature with the recipient's public key



timestamps and digital signatures

every digital signature must have a timestamp embedded into it

correctly timestamping messages, including digital signatures, can be very challenging

the methods to timestamp data will be discussed later

undeniable digital signatures

these are the special type of digital signatures that can be verified only by the selected parties

e.g., using dongles and such

also, the signer cannot deny signing the document during verification

these signatures can be used to authenticate software products and other documents