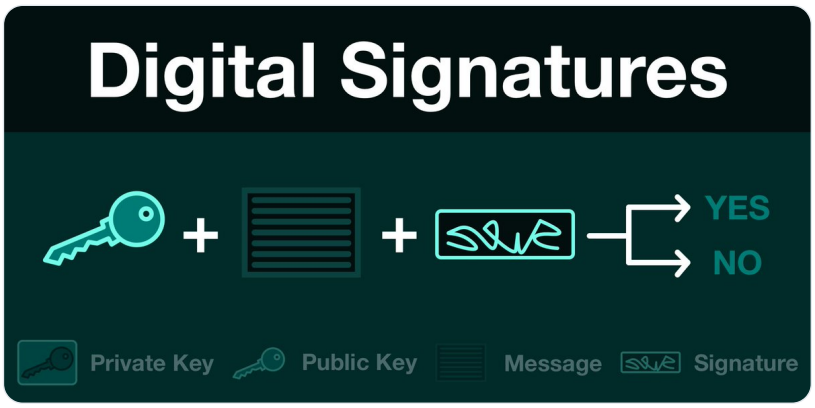
Haym @SalomonCrypto
Sep 28 · 8 tweets · SalomonCrypto/status/1575127511066824704

(1/7) Cryptography 101: Digital Signatures

The internet is the Wild West... how can we know who created a particular piece data? Can we be sure the data hasn't been altered? How can you create trust, trustlessly?

A primer on digital authenticity and integrity.

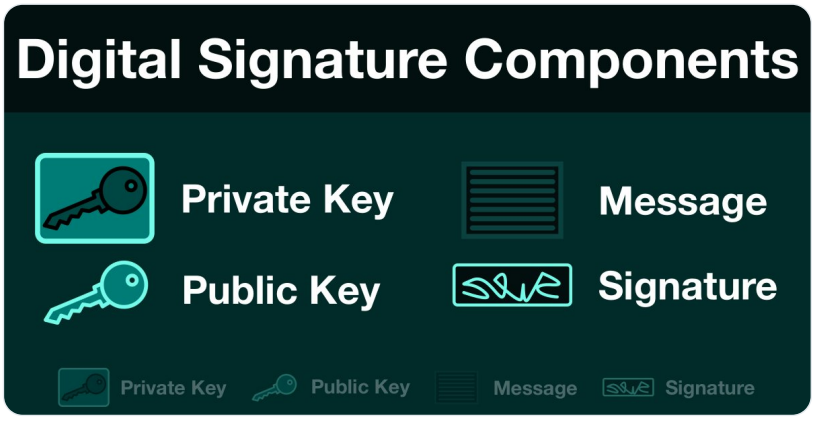


(2/7) A digital signature is a unique piece of information generated by one party to publicly confirm two things:

1) the message was really sent by the person claiming to send it (authenticity)
2) the message has not been tampered with (integrity)

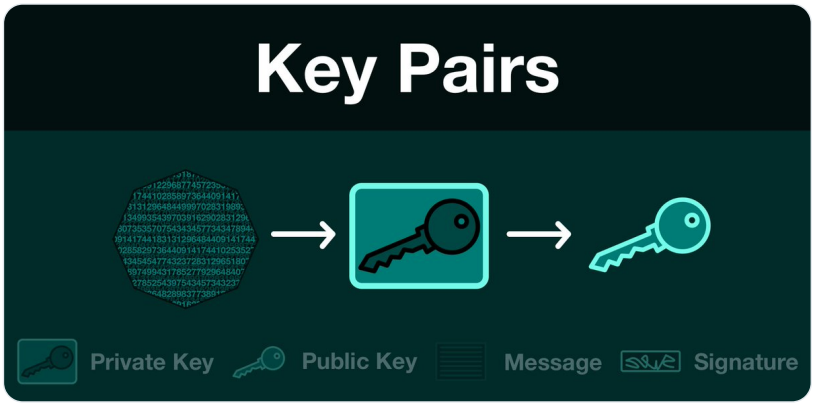
(3/7) There are 4 components to a digital signature:

Private Key - secret code used to create signatures
Public Key - public code used to verify signatures
Message - the data the signature is certifying
Signature - the cryptographically secure verification



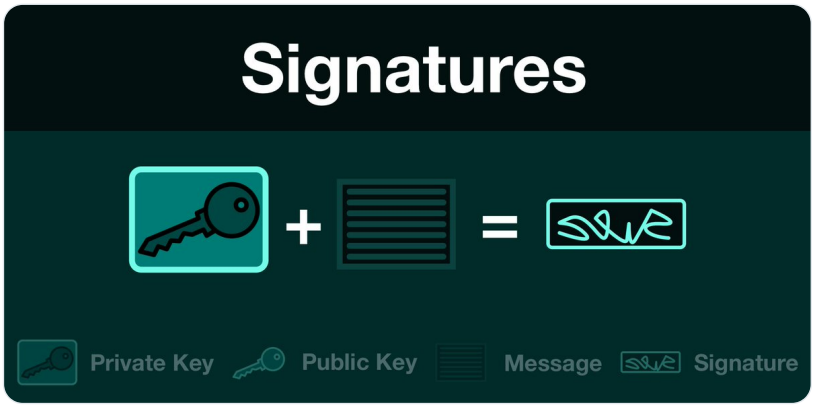
(4/7) The process begins by generating a private key (a big randomly generated number).

Using elliptic curve cryptography, the public key is derived from the private key. This is a one way operation; once finished, a private key cannot be recovered from a public key



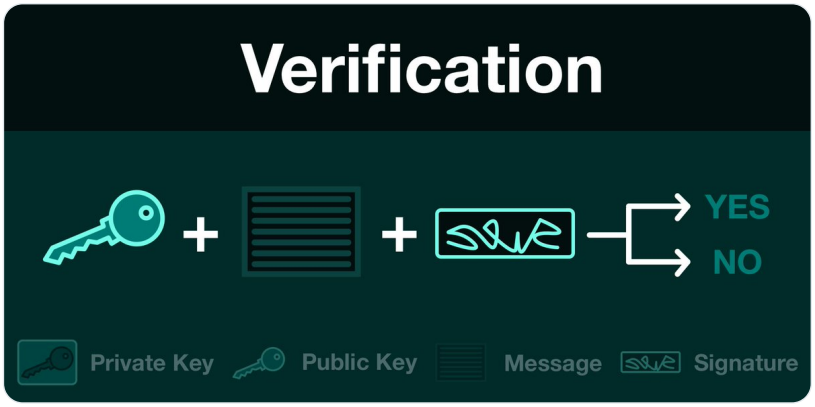
(5/7) A message is an arbitrary blob of data. Text, code, images... anything that can be represented as a string of data.

A signer applies their private key to a message, generate a signature. The signature is unique to both the private key (signer) and the message.



(6/7) A signature is verified by applying cryptographic magic to the signers public key, the message and the signature.

If they all match, the signature is declared valid; otherwise, there is a problem - either the message was changed or someone else generated the signature.



(7/7) There are many different types of digital signature schemes in use across computer science. Different schemes have different trade offs, but they all share the same core goals:

Proof of Authenticity - sent by a known sender
Proof of Integrity - unaltered message

Like what you read? Help me spread the word by retweeting the thread (linked below).

Follow me for more explainers and as much alpha as I can possibly serve.

• • •