3. Cryptography 2

Thursday, February 11, 2021 12:58 PM

Digital Signing:

- For **integrity** verification
- Message -> Hash function -> Meaningless data

Hash: one-way; unique fingerprint
MD5, SHA3

Client A			Web service B
PrivA	Encrypts data using PrivA	Sends original message + digital signature	Separates original message and digital signature

You can get digest from a message using hash function.
Digest of a text: cryptographic hash function with string of digits created by one-way hash formula.

- A tiny digital summary
- Two different messages will never have the same digest

Fingerprint: a tiny digital summary

- Only 2 identical messages give identical digests.

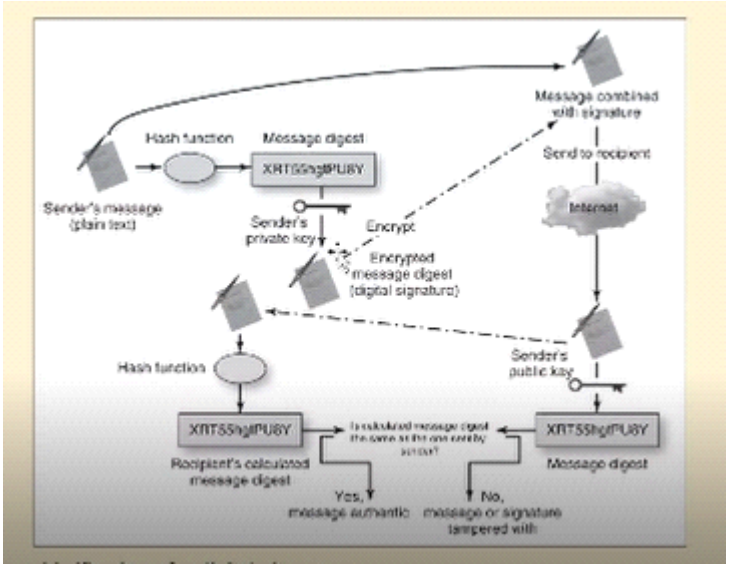
B decrypts digital signature using public key of A to get the digest appended by A for the original message.

- Digest and digital signature is meaningless. (encrypted or decrypted) (less likely to be tampered with)
- Digest -> encrypted -> digital signature
- **Digest must be encrypted** with a private key (even though it is meaningless)

B wants to verify the integrity of the message. If the digest computed by B (of the received message) does not match the digest sent by A (which is calculated by decrypting the digital signature of A by B), then the message has been tampered with.

Digital signature verification:

- Message is not tampered during transit
- Confirms the sender of the message



If I can decrypt successfully something using public key of A, then it would be encrypted using private key of A. It implies that the original message and signature originated from A only. A cannot deny that it has not sent the message.

Digital Certificate:

Mechanism to identify who a public key belongs to (along with expiry) + signature from a well-known authority = digital certificate

Certificate authority signs a digest and is appended to the data
Name, organization, validity, public key, signature

Developing a self-signed certificate