Lesson 4
Digital signatures

A. Sorokin (Input | Output)

Self paced course

July 31, 2025

What is Signing a Document?

Signing a document is the process of authenticating its origin and ensuring its integrity.

Signing helps to verify:

- **authenticity**: the signer is who they claim to be.
- **non-repudiation**: the signer cannot deny their involvement later.
- **integrity**: the document has not been altered after signing.

Types signatures

Signing a document can be done in two ways.

(i) **Traditional (real) signature**: handwritten on a physical document.

(ii) **Digital signature**: a cryptographic method for electronic documents.

Real vs digital signatures

Feature	**Real Signature**	**Digital Signature**
Medium	Physical (paper)	Digital (electronic)
Verification	Visual comparison	Cryptographic proof
Forging	Relatively easy	Hard to forge
Integrity	No, can be altered after signing	Yes, any change invalidates the signature

Real vs digital signatures

Feature	**Real Signature**	**Digital Signature**
Non-repudiation	Weak, hard to prove in court	Strong, mathematically verifiable
Process	Manual (pen and paper)	Automated (private and public keys)
Legal Acceptance	Widely accepted	Legally binding
Speed and Efficiency	Slow, requires physical handling	Instant, works globally

DSA

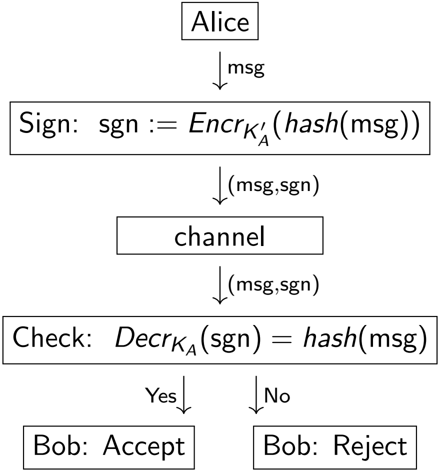
In general, the **digital signature algorithm (DSA)** has the following form.

(1) **Key generation**: Alice generates a public-private key pair.

(2) **Signing**: Alice encrypts a hash of her document with her private key and sends her **signature** to Bob together with a document.

(3) **Verification**: Bob decrypts the signature using Alice's public key and compares it to a hash of the received message. If they match, the signature is valid.

Digital signature scheme



Alice

msg

Sign: sgn $:= Encr_{K'_A}(hash(\text{msg}))$

(msg,sgn)

channel

(msg,sgn)

Check: $Decr_{K_A}(\text{sgn}) = hash(\text{msg})$

Yes

No

Bob: Accept

Bob: Reject

DSA benefits

Core properties and benefits of DSA are:

(i) **asymmetry**: only the private key holder can sign, but anyone can verify the signature with the public key;

(ii) **size independence**: signatures act on message digests (efficient for large files);

(iii) **authenticity**: altering a document invalidates its signature (unless the private key is compromised);

(iv) **uniqueness**: different documents will have different signatures.

Benefits and challenges of DSA

While DSA doesn't require any secret sharing and DSA systems are quite scalable, there are several limitations and challenges for digital signatures.

(1) **Private key security**: if a private key is lost, stolen, or compromised, all signatures made with it become untrustworthy.

(2) **Unsuitable for high-speed data**: signing every packet in real-time systems (e.g., video streaming) may introduce latency.

Benefits and challenges of DSA

(3) **Hash function dependence**: if the underlying hash is broken, signatures lose security.

(4) **Computational heaviness**: digital signatures based on public-key cryptosystems are slower than their symmetric alternatives like HMAC.

(5) **Storage overhead**: storing signatures for every transaction (e.g., blockchain) increases data size.

DSA examples

(1) DSA in RSA (RSA-DSA);

(2) Elliptic curve DSA (EDSA);

(3) Edwards-curve DSA (EdDSA).

DSA applications

(1) Secure messaging.

(2) Blockchain transactions.

(3) Software distribution.

(4) Legal documents.