Digital Signatures Schemes in Practice

The precursors
- *ElGamal signature*
- *Schnorr signature*

The standards
- *DSA - Digital Signature Algorithm* (RSA-based)
- *ECDSA - Elliptic Curve Digital Signature Algorithm* (ECC-based)

The newcomer
- *EdDSA - Edwards-curve Digital Signature Algorithm* (ECC-based)

Non-repudation as a special case of integrity

	MAC	Digital Signature
Integrity	✅	✅
Non-repudiation	❌	✅