Digital Signature

To laypeople, a digital signature might suggest that an assistant scans their boss's signature into an image file, which can then be easily inserted into documents when needed. Unfortunately, this method could lead to serious legal consequences if used in such a way. In reality, a **digital signature** is entirely different.

Public key systems are also known as **asymmetric systems** because different keys are required for encryption and decryption. In **symmetric systems**, the same key is used for both encryption and decryption.

In asymmetric systems, anyone can send Anna a secret message. But how can we verify the identity of the sender? **Digital signature algorithms** are specialized asymmetric systems. There is a private key used for signing and a public key used to verify the authenticity of the signature.

Requirements for a Digital Signature:

1. **Authenticity**: The signature should convince the reader of the document that the signer deliberately signed the document.

2. **Non-falsifiable**: The signature must prove that the owner of the signature signed the document, and no one else.

3. **Cannot be reused on other documents**: The signature is an integral part of the document and cannot be transferred to another document.

4. **The signed document cannot be altered without detection**.

5. **Non-repudiation**: The signer cannot later deny having signed the document.

These requirements make digital signatures a much more secure solution compared to manual (analog) signatures.