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 Alice 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 than manual (analog) signatures.

Simple Digital Signature Using Direct RSA Application

In its simplest form, the **RSA algorithm** can also be used for digital signatures.

The steps are as follows:

1. **Sign the document using your private key**.

2. In RSA, the roles of the private and public keys can be reversed: you can encrypt with either key, and the other key (and only that key) can decrypt the message.

3. If someone encrypts a message with their **private key**, it can be decrypted using their **public key**, thereby verifying the authenticity.

4. The entire document is encoded as part of the signature (the encoded document itself is the signature).

5. The signer cannot deny having signed the document because they are the only ones who know the

private key necessary to create the signature.

6. When using the RSA signing method, the document remains unreadable until the signature is verified.

However, this method can be **inconvenient** in certain cases:

- If the recipient does not have access to the **public key**.
- If there is not enough computational power available to decrypt the message.

This explanation outlines how RSA can be applied to digital signatures in a simple manner and highlights the potential limitations of this approach.