

A collection of small, colorful triangles in yellow, teal, and grey, some pointing towards the title and others away from it.

Digital Signature Algorithm

Jiang Aiqing

2017.10.19

Two clusters of four triangles each, arranged in a pinwheel pattern. The triangles are colored yellow, teal, light blue, and green.A large blue curved shape at the bottom of the slide, decorated with several small triangles in white, light blue, yellow, and grey.

What is digital signature ?

- A **digital signature** is a mathematical scheme for demonstrating the authenticity of digital messages or documents.
- A valid digital signature gives a recipient reason to believe that the message was created by a known sender, that the sender cannot deny having sent the message, and that the message was not altered in transit (integrity).
- **Applications:** software distribution, financial transactions, data storage etc.

Digital Signature Algorithm

- The **Digital Signature Algorithm (DSA)** is a Federal Information Processing Standard for digital signatures. In August 1991 the National Institute of Standards and Technology (NIST) proposed DSA for use in their **Digital Signature Standard (DSS)** and adopted it as FIPS 186 in 1993.

Steps of Digital Signature Algorithm

- Key generation

Key generation has two phases. The first phase is a choice of *algorithm parameters* which may be shared between different users of the system, while the second phase computes public and private keys for a single user.

- Signing

- Verifying