

DSA (DIGITAL SIGNATURE ALGORITHM)

Reporter: Xiumei Wang

Instructor: Wolfgang Härdle

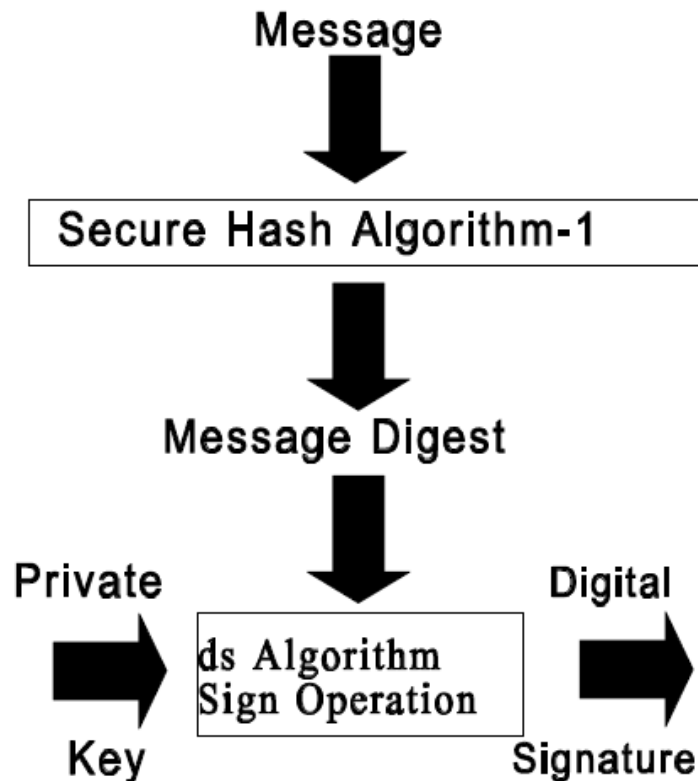
WHAT IS DSA (DIGITAL SIGNATURE ALGORITHM)?

- Digital signatures are essential to **verify the sender of a document's identity**. The signature is computer using a set of rules and algorithm such that the identity of the person can be verified.
- The signature is generated by the use of **a private key** that known only to **the user**. The signature is verified when a public key is corresponds to the private key. With every user having a public/private key pair, this is an example of public-key cryptography.
- **Public keys**, which are known by everyone, can be used to verify the signature of a user. **The private key**, which is never shared, is used in signature generation, which can only be done by the user.

WHAT CAN DSA DO?

- Digital signatures are used to detect unauthorized modifications to data. Also, the recipient of a digitally signed document is proving to a third party that the document was indeed signed by the person who it is claimed to be signed by. This is known as nonrepudiation, because the person who signed the document cannot repudiate the signature at a later time.
- Digital signature algorithms can be used in e-mails, electronic funds transfer, electronic data interchange, software distribution, data storage, and just about any application that would need to assure the integrity and originality of data.

Signature Generation



Signature Verification

