

DER-Encoded Hash Algorithm ID

30 31 30 0d 06 09 60 86 48 01
65 03 04 02 01 05 00 04 20

This is a
signature

Padding String

ff ff ff ... ff

Message

256-bit
SHA-2

0x00

0x01

PS

0x00

DER

Hash

Little-Endian Integer

Private Key

RSA
Decryption

PKCS #1 v1.5
RSA Signature