

L13 - Digital Signatures for Protection of Assets

Running command line sig-test - <https://youtu.be/mEK1HXEwZ14>

Part 1 - client server - <https://youtu.be/rESaFYrFWJ8>

Part 2 - client server - <https://youtu.be/4MKBQ-0OGTk>

From Amazon S3 - for download (same as youtube videos)

Running command line sig-test

Part 1 - client server

Part 2 - client server

If you want the details of how the ECDSA signature works (the actual math) rather than my 5 min quick overview <https://cryptobook.nakov.com/digital-signatures/ecdsa-sign-verify-messages>

Outline

Command line generation of and verification of a ECDSA signature.

What a keyfile looks like.

Code in Assignment 4.

Server - and end points.

Client and "GET" calls.