# Encryption Compendium for LabVIEW™

Datasheet

Lvs-tools.co.uk

## Features Overview

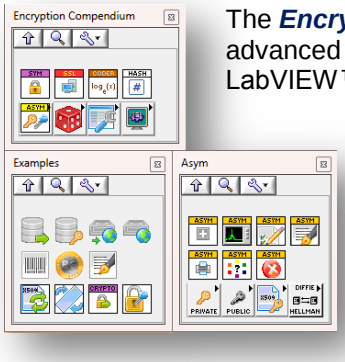
- Hashes.
- Symmetric encryption.
- SSL and TLS communications.
- SSH Client communications.
- Diffie-Hellman and Elliptic Curve key exchange.
- RSA, DSA and ECDSA signature generation, signing and verification.
- X509 certificate generation, signing and verification.
- PEM and DER certificate formats.
- Base 64 and Base 58 data encoding.
- Random numbers library.
- Bitcoin address library.
- Numerous examples.

## Platforms

- Windows® 7 or later

## LabVIEW™ Versions

- Windows® - 2012 or later


The ***Encryption Compendium for LabVIEW***™ offers developers advanced encryption, hashing and secure communication capabilities in LabVIEW™.

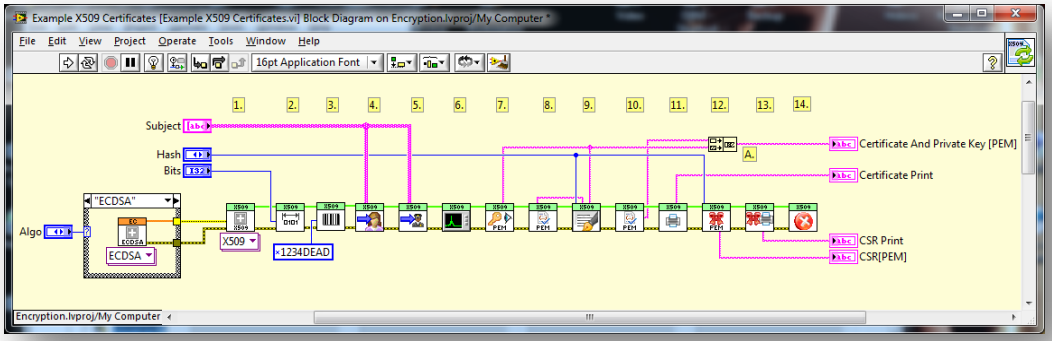
It is a comprehensive and feature rich API covering a multitude of technologies centred around securing data and communications. It comes complete with many symmetric and asymmetric encryption examples that can be used as a starting point to dramtically reduce the development time of your applications. Includes key generation, message signing, certificate generation and communications over Secure Sockets Layer (SSL), Transport Layer Security (TLS) and Secure Shell (SSH).

Data and information is valuable.

- *Prevent* it from being stolen.
- *Protect* it from competitors.
- *Preserve* ideas and intellectual property.
- *Provide* peace of mind.

Secure data and information with the ***Encryption Compendium for LabVIEW***™.

- *Safely* store it locally and in the cloud.
- *Shield* it from competitors.
- *Safeguard* ideas and intellectual property.
- *Sanctuary* for data and information.




The ***Encryption Compendium for LabVIEW***™ leverages the industry standard OpenSSL binaries* to provide LabVIEW developers with a complete suite of encryption capabilities for modern applications.

** OpenSSL binaries are supplied with the LabVIEW™ software installation and are maintained by National Instruments.*

# Encryption Compendium for LabVIEW™

Datasheet

Lvs-tools.co.uk

## Hashes

- MD4
- MD5
- SHA 1/256/384/512
- RIPEMD160
- WHIRLPOOL
- HMAC

## Symmetric Encryption

- AES 128/192/256
  *ECB/CBC/CFB/OFB*
- Blowfish
  *ECB/CBC/CFB/OFB*
- Cast-cbc
- Des
  *ECB/CBC/CFB/OFB*
- Des-ede
  *CBC/CFB/OFB*
- Des-ede3
  *CBC/CFB/OFB*
- Desx
- Idea
  *ECB/CBC/CFB/OFB*
- RC2
  *ECB/CBC/CFB/OFB*
- RC4-40
- RC4

## SSL/TLS**

- SSL2, SSL3
- TLS1, TLS1.2

## Digital Signatures

- RSA
- DSA
- ECDSA
- x509

## Key Exchange Algorithms

- Diffie-Hellman
- Elliptic Curve Diffie-Hellman

## Key and Certificate Formats

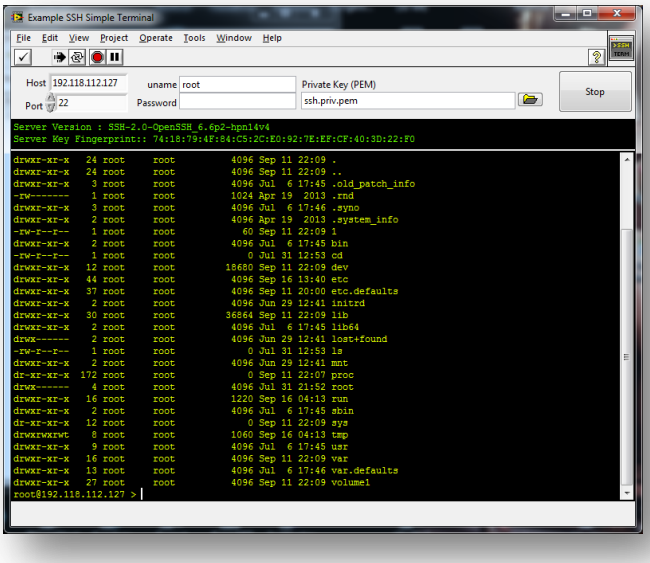
- PEM
- DER

## Encoding

- Base64
- Base58

## SSH

- SSH 1 Client
- SSH 2 Client
- Execute Command
- Interactive Shell Sessions
- Key Exchanges:
  - ecdh-sha2-nistp256.
  - diffie-hellman-group1-sha1.
  - diffie-hellman-group14-sha1
- Authentication:
  - Password.
  - Public-key.
- Ciphers:
  - aes256-ctr.
  - aes192-ctr.
  - aes128-ctr.
  - aes256-cbc.
  - aes192-cbc.
  - aes128-cbc.
  - 3des-cbc.
  - des-cbc-ssh1.
  - blowfish-cbc.




*** Over TCP. UDP is not currently supported.*

*NOTE:*
*Available features are dependent on the particular OpenSSL binaries installed with LabVIEW. For example, LabVIEW 2012 was originally deployed with OpenSSL binaries that do not support TLS 1.2.*

## Elliptic Curves

c2pnb163v1
c2pnb163v2
c2pnb163v3
c2pnb176v1
c2tnb191v1
c2tnb191v2
c2tnb191v3
c2onb191v4
c2onb191v5
c2pnb208w1
c2tnb239v1
c2tnb239v2
c2tnb239v3
c2onb239v4
c2onb239v5
c2pnb272w1
c2pnb304w1
c2tnb359v1
c2pnb368w1
c2tnb431r1
prime192v1
prime192v2
prime192v3
prime239v1
prime239v2
prime239v3
prime256v1
secp112r1
secp112r2
secp128r1
secp128r2
secp160k1
secp160r1
secp160r2
secp192k1
secp224k1
secp224r1
secp256k1
secp384r1
secp521r1
sect113r1
sect113r2
sect131r1
sect131r2
sect163k1
sect163r1
sect163r2
sect193r1
sect193r2
sect233k1
sect233r1
sect239k1
sect283k1
sect283r1
sect409k1
sect409r1
sect571k1
sect571r1

## Supplemental Libraries

- Bitcoin addresses
  - Private Key to Address
  - Private Key to WIF
  - Public Key from Private Key
  - Public Key to Address
  - Public Key from WIF
- Random number
  - Init
  - Bytes
  - Cleanup
  - Load File
  - Write File
  - Bytes