AlgosToSecFuns

- AsymKeyPair-DomPar
  - DSA PQGGen (FIPS186-4)
  - DSA PQGVer (FIPS186-4)
- AsymKeyPair-KeyGen
  - DSA KeyGen (FIPS186-4)
  - ECDSA KeyGen (FIPS186-4)
  - ECDSA KeyGen (FIPS186-5)
  - EDDSA KeyGen
  - LMS KeyGen
  - RSA KeyGen (FIPS186-4)
  - RSA KeyGen (FIPS186-5)
  - Safe Primes Key Generation
- AsymKeyPair-KeyVer
  - ECDSA KeyVer (FIPS186-4)
  - ECDSA KeyVer (FIPS186-5)
  - EDDSA KeyVer
  - Safe Primes Key Verification
- BC-Auth
  - AES-CCM
  - AES-GCM
  - AES-GCM-SIV
  - AES-KW
  - AES-KWP
  - TDES-KW
- BC-UnAuth
  - AES-CBC
  - AES-CBC-CS1
  - AES-CBC-CS2
  - AES-CBC-CS3
  - AES-CFB1
  - AES-CFB128
  - AES-CFB8
  - AES-CTR
  - AES-ECB

- AES-FF1
- AES-FF3-1
- AES-OFB
- AES-XPN
- AES-XTS
- AES-XTS Testing Revision 2.0
- TDES-CBC
- TDES-CBCI
- TDES-CFB1
- TDES-CFB64
- TDES-CFB8
- TDES-CFBP1
- TDES-CFBP64
- TDES-CFBP8
- TDES-CTR
- TDES-ECB
- TDES-OFB
- TDES-OFBI

DigSig-SigGen

- Deterministic ECDSA SigGen (FIPS186-5)
- DSA SigGen (FIPS186-4)
- ECDSA SigGen (FIPS186-4)
- ECDSA SigGen (FIPS186-5)
- EDDSA SigGen
- LMS SigGen
- RSA SigGen (FIPS186-4)
- RSA SigGen (FIPS186-5)
- RSA Signature Primitive

DigSig-SigVer

- DSA SigVer (FIPS186-4)
- ECDSA SigVer (FIPS186-4)
- ECDSA SigVer (FIPS186-5)
- EDDSA SigVer
- LMS SigVer
- RSA SigVer (FIPS186-2)
- RSA SigVer (FIPS186-4)
- RSA SigVer (FIPS186-5)

- DRBG
  - Counter DRBG
  - Hash DRBG
  - HMAC DRBG
- ENT-Cond
  - Conditioning Component AES-CBC-MAC SP800-90B
  - Conditioning Component Block Cipher Derivation Function SP800-90B
  - Conditioning Component Hash Derivation Function SP800-90B
- KAS-135KDF
  - KDF ANS 9.42
  - KDF ANS 9.63
  - KDF IKEv1
  - KDF IKEv2
  - KDF SNMP
  - KDF SRTP
  - KDF SSH
  - KDF TLS
  - KDF TPM
  - TLS v1.2 KDF RFC7627
  - TLS v1.3 KDF
- KAS-Full
  - KAS-ECC
  - KAS-ECC Sp800-56Ar3
  - KAS-FFC
  - KAS-FFC Sp800-56Ar3
  - KAS-IFC
- KAS-KC
  - KAS-KC SP800-56
- KAS-SSC
  - KAS-ECC CDH-Component
  - KAS-ECC CDH-Component SP800-56Ar3
  - KAS-ECC Component
  - KAS-ECC-SSC Sp800-56Ar3
  - KAS-FFC Component
  - KAS-FFC-SSC Sp800-56Ar3
  - KAS-IFC-SSC
- KBKDF

- KDF KMAC Sp800-108r1
- KDF SP800-108
- KTS-Encap
  - KTS-IFC
  - RSA Decryption Primitive
  - RSA Decryption Primitive Sp800-56Br2
- MAC
  - AES-CMAC
  - AES-GMAC
  - HMAC-SHA-1
  - HMAC-SHA2-224
  - HMAC-SHA2-256
  - HMAC-SHA2-384
  - HMAC-SHA2-512
  - HMAC-SHA2-512/224
  - HMAC-SHA2-512/256
  - HMAC-SHA3-224
  - HMAC-SHA3-256
  - HMAC-SHA3-384
  - HMAC-SHA3-512
  - TDES-CMAC
- PBKDF
  - PBKDF
- SHA
  - SHA-1
  - SHA2-224
  - SHA2-256
  - SHA2-384
  - SHA2-512
  - SHA2-512/224
  - SHA2-512/256
  - SHA3-224
  - SHA3-256
  - SHA3-384
  - SHA3-512
- XOF
  - cSHAKE-128

cSHAKE-256
KMAC-128
KMAC-256
ParallelHash-128
ParallelHash-256
SHAKE-128
SHAKE-256
TupleHash-128
TupleHash-256