1. MessageDigest
   1. Bouncy Castle

|  |
| --- |
| - BC  [1.0.10118.3.0.55, 1.2.804.2.1.1.1.1.2.2.1, 1.2.804.2.1.1.1.1.2.2.2, 1.2.804.2.1.1.1.1.2.2.3, 2.16.840.1.101.3.4.2.10, 2.16.840.1.101.3.4.2.7, 2.16.840.1.101.3.4.2.8, 2.16.840.1.101.3.4.2.9, BLAKE2B-160, BLAKE2B-256, BLAKE2B-384, BLAKE2B-512, BLAKE2S-128, BLAKE2S-160, BLAKE2S-224, BLAKE2S-256, DSTU7564-256, DSTU7564-384, DSTU7564-512, GOST3411, GOST3411-2012-256, GOST3411-2012-512, KECCAK-224, KECCAK-256, KECCAK-288, KECCAK-384, KECCAK-512, MD2, MD4, MD5, OID.1.0.10118.3.0.55, OID.1.2.804.2.1.1.1.1.2.2.1, OID.1.2.804.2.1.1.1.1.2.2.2, OID.1.2.804.2.1.1.1.1.2.2.3, OID.2.16.840.1.101.3.4.2.10, OID.2.16.840.1.101.3.4.2.7, OID.2.16.840.1.101.3.4.2.8, OID.2.16.840.1.101.3.4.2.9, RIPEMD128, RIPEMD160, RIPEMD256, RIPEMD320, SHA-1, SHA-224, SHA-256, SHA-384, SHA-512, SHA-512/224, SHA-512/256, SHA3-224, SHA3-256, SHA3-384, SHA3-512, SM3, Skein-1024-1024, Skein-1024-384, Skein-1024-512, Skein-256-128, Skein-256-160, Skein-256-224, Skein-256-256, Skein-512-128, Skein-512-160, Skein-512-224, Skein-512-256, Skein-512-384, Skein-512-512, TIGER, WHIRLPOOL]  - SUN  [MD2, MD5, SHA, SHA-224, SHA-256, SHA-384, SHA-512] |

1. Key Generator
   1. Algorithm

|  |
| --- |
| - BC  [1.2.392.200011.61.1.1.1.2, 1.2.392.200011.61.1.1.1.3, 1.2.392.200011.61.1.1.1.4, 1.2.392.200011.61.1.1.3.2, 1.2.392.200011.61.1.1.3.3, 1.2.392.200011.61.1.1.3.4, 1.2.410.200004.1.4, 1.2.410.200004.7.1.1.1, 1.2.410.200046.1.1.1, 1.2.410.200046.1.1.11, 1.2.410.200046.1.1.12, 1.2.410.200046.1.1.13, 1.2.410.200046.1.1.14, 1.2.410.200046.1.1.2, 1.2.410.200046.1.1.3, 1.2.410.200046.1.1.34, 1.2.410.200046.1.1.35, 1.2.410.200046.1.1.36, 1.2.410.200046.1.1.37, 1.2.410.200046.1.1.38, 1.2.410.200046.1.1.39, 1.2.410.200046.1.1.4, 1.2.410.200046.1.1.40, 1.2.410.200046.1.1.41, 1.2.410.200046.1.1.42, 1.2.410.200046.1.1.43, 1.2.410.200046.1.1.44, 1.2.410.200046.1.1.45, 1.2.410.200046.1.1.6, 1.2.410.200046.1.1.7, 1.2.410.200046.1.1.8, 1.2.410.200046.1.1.9, 1.2.804.2.1.1.1.1.1.3.1.1, 1.2.804.2.1.1.1.1.1.3.1.2, 1.2.804.2.1.1.1.1.1.3.1.3, 1.2.804.2.1.1.1.1.1.3.10.1, 1.2.804.2.1.1.1.1.1.3.10.2, 1.2.804.2.1.1.1.1.1.3.10.3, 1.2.804.2.1.1.1.1.1.3.2.1, 1.2.804.2.1.1.1.1.1.3.2.2, 1.2.804.2.1.1.1.1.1.3.2.3, 1.2.804.2.1.1.1.1.1.3.3.1, 1.2.804.2.1.1.1.1.1.3.3.2, 1.2.804.2.1.1.1.1.1.3.3.3, 1.2.804.2.1.1.1.1.1.3.5.1, 1.2.804.2.1.1.1.1.1.3.5.2, 1.2.804.2.1.1.1.1.1.3.5.3, 1.2.804.2.1.1.1.1.1.3.6.1, 1.2.804.2.1.1.1.1.1.3.6.2, 1.2.804.2.1.1.1.1.1.3.6.3, 1.2.804.2.1.1.1.1.1.3.7.1, 1.2.804.2.1.1.1.1.1.3.7.2, 1.2.804.2.1.1.1.1.1.3.7.3, 1.2.804.2.1.1.1.1.1.3.8.1, 1.2.804.2.1.1.1.1.1.3.8.2, 1.2.804.2.1.1.1.1.1.3.8.3, 1.2.840.113549.3.2, 1.2.840.113549.3.7, 1.3.6.1.4.1.188.7.1.1.2, 2.16.840.1.101.3.4.1.1, 2.16.840.1.101.3.4.1.2, 2.16.840.1.101.3.4.1.21, 2.16.840.1.101.3.4.1.22, 2.16.840.1.101.3.4.1.23, 2.16.840.1.101.3.4.1.24, 2.16.840.1.101.3.4.1.25, 2.16.840.1.101.3.4.1.26, 2.16.840.1.101.3.4.1.27, 2.16.840.1.101.3.4.1.28, 2.16.840.1.101.3.4.1.3, 2.16.840.1.101.3.4.1.4, 2.16.840.1.101.3.4.1.41, 2.16.840.1.101.3.4.1.42, 2.16.840.1.101.3.4.1.43, 2.16.840.1.101.3.4.1.44, 2.16.840.1.101.3.4.1.45, 2.16.840.1.101.3.4.1.46, 2.16.840.1.101.3.4.1.47, 2.16.840.1.101.3.4.1.48, 2.16.840.1.101.3.4.1.5, 2.16.840.1.101.3.4.1.6, 2.16.840.1.101.3.4.1.7, 2.16.840.1.101.3.4.1.8, 2.16.840.1.101.3.4.2, 2.16.840.1.101.3.4.22, 2.16.840.1.101.3.4.42, AES, AES-GMAC, AESWRAP, AESWRAPPAD, ARC4, ARIA, ARIA-GMAC, BLOWFISH, CAMELLIA, CAMELLIA-GMAC, CAST5, CAST6, CAST6-GMAC, CHACHA, CHACHA7539, DES, DESEDE, DESEDEWRAP, DSTU7624, GOST28147, GOST3412-2015, Grain128, Grainv1, HC128, HC256, HMACDSTU7564-256, HMACDSTU7564-384, HMACDSTU7564-512, HMACGOST3411, HMACGOST3411-2012-256, HMACGOST3411-2012-512, HMACKECCAK224, HMACKECCAK256, HMACKECCAK288, HMACKECCAK384, HMACKECCAK512, HMACMD2, HMACMD4, HMACMD5, HMACRIPEMD128, HMACRIPEMD160, HMACRIPEMD256, HMACRIPEMD320, HMACSHA1, HMACSHA224, HMACSHA256, HMACSHA3-224, HMACSHA3-256, HMACSHA3-384, HMACSHA3-512, HMACSHA384, HMACSHA512, HMACSHA512/224, HMACSHA512/256, HMACSkein-1024-1024, HMACSkein-1024-384, HMACSkein-1024-512, HMACSkein-256-128, HMACSkein-256-160, HMACSkein-256-224, HMACSkein-256-256, HMACSkein-512-128, HMACSkein-512-160, HMACSkein-512-224, HMACSkein-512-256, HMACSkein-512-384, HMACSkein-512-512, HMACTIGER, HMACWHIRLPOOL, IDEA, NOEKEON, NOEKEON-GMAC, OID.1.2.392.200011.61.1.1.1.2, OID.1.2.392.200011.61.1.1.1.3, OID.1.2.392.200011.61.1.1.1.4, OID.1.2.392.200011.61.1.1.3.2, OID.1.2.392.200011.61.1.1.3.3, OID.1.2.392.200011.61.1.1.3.4, OID.1.2.410.200004.1.4, OID.1.2.410.200004.7.1.1.1, OID.1.2.410.200046.1.1.1, OID.1.2.410.200046.1.1.11, OID.1.2.410.200046.1.1.12, OID.1.2.410.200046.1.1.13, OID.1.2.410.200046.1.1.14, OID.1.2.410.200046.1.1.2, OID.1.2.410.200046.1.1.3, OID.1.2.410.200046.1.1.34, OID.1.2.410.200046.1.1.35, OID.1.2.410.200046.1.1.36, OID.1.2.410.200046.1.1.37, OID.1.2.410.200046.1.1.38, OID.1.2.410.200046.1.1.39, OID.1.2.410.200046.1.1.4, OID.1.2.410.200046.1.1.40, OID.1.2.410.200046.1.1.41, OID.1.2.410.200046.1.1.42, OID.1.2.410.200046.1.1.43, OID.1.2.410.200046.1.1.44, OID.1.2.410.200046.1.1.45, OID.1.2.410.200046.1.1.6, OID.1.2.410.200046.1.1.7, OID.1.2.410.200046.1.1.8, OID.1.2.410.200046.1.1.9, OID.1.2.804.2.1.1.1.1.1.3.1.1, OID.1.2.804.2.1.1.1.1.1.3.1.2, OID.1.2.804.2.1.1.1.1.1.3.1.3, OID.1.2.804.2.1.1.1.1.1.3.10.1, OID.1.2.804.2.1.1.1.1.1.3.10.2, OID.1.2.804.2.1.1.1.1.1.3.10.3, OID.1.2.804.2.1.1.1.1.1.3.2.1, OID.1.2.804.2.1.1.1.1.1.3.2.2, OID.1.2.804.2.1.1.1.1.1.3.2.3, OID.1.2.804.2.1.1.1.1.1.3.3.1, OID.1.2.804.2.1.1.1.1.1.3.3.2, OID.1.2.804.2.1.1.1.1.1.3.3.3, OID.1.2.804.2.1.1.1.1.1.3.5.1, OID.1.2.804.2.1.1.1.1.1.3.5.2, OID.1.2.804.2.1.1.1.1.1.3.5.3, OID.1.2.804.2.1.1.1.1.1.3.6.1, OID.1.2.804.2.1.1.1.1.1.3.6.2, OID.1.2.804.2.1.1.1.1.1.3.6.3, OID.1.2.804.2.1.1.1.1.1.3.7.1, OID.1.2.804.2.1.1.1.1.1.3.7.2, OID.1.2.804.2.1.1.1.1.1.3.7.3, OID.1.2.804.2.1.1.1.1.1.3.8.1, OID.1.2.804.2.1.1.1.1.1.3.8.2, OID.1.2.804.2.1.1.1.1.1.3.8.3, OID.1.3.6.1.4.1.188.7.1.1.2, OID.2.16.840.1.101.3.4.1.1, OID.2.16.840.1.101.3.4.1.2, OID.2.16.840.1.101.3.4.1.21, OID.2.16.840.1.101.3.4.1.22, OID.2.16.840.1.101.3.4.1.23, OID.2.16.840.1.101.3.4.1.24, OID.2.16.840.1.101.3.4.1.25, OID.2.16.840.1.101.3.4.1.26, OID.2.16.840.1.101.3.4.1.27, OID.2.16.840.1.101.3.4.1.28, OID.2.16.840.1.101.3.4.1.3, OID.2.16.840.1.101.3.4.1.4, OID.2.16.840.1.101.3.4.1.41, OID.2.16.840.1.101.3.4.1.42, OID.2.16.840.1.101.3.4.1.43, OID.2.16.840.1.101.3.4.1.44, OID.2.16.840.1.101.3.4.1.45, OID.2.16.840.1.101.3.4.1.46, OID.2.16.840.1.101.3.4.1.47, OID.2.16.840.1.101.3.4.1.48, OID.2.16.840.1.101.3.4.1.5, OID.2.16.840.1.101.3.4.1.6, OID.2.16.840.1.101.3.4.1.7, OID.2.16.840.1.101.3.4.1.8, POLY1305, POLY1305-AES, POLY1305-ARIA, POLY1305-CAMELLIA, POLY1305-CAST6, POLY1305-NOEKEON, POLY1305-RC6, POLY1305-SEED, POLY1305-SERPENT, POLY1305-SM4, POLY1305-Twofish, RC2, RC5, RC5-64, RC6, RC6-GMAC, RIJNDAEL, SALSA20, SEED, SEED-CMAC, SEED-GMAC, SERPENT-GMAC, SHACAL-2, SIPHASH, SKIPJACK, SM4, SM4-CMAC, SM4-GMAC, Serpent, Shacal2, Skein-MAC-1024-1024, Skein-MAC-1024-384, Skein-MAC-1024-512, Skein-MAC-256-128, Skein-MAC-256-160, Skein-MAC-256-224, Skein-MAC-256-256, Skein-MAC-512-128, Skein-MAC-512-160, Skein-MAC-512-224, Skein-MAC-512-256, Skein-MAC-512-384, Skein-MAC-512-512, TEA, TNEPRES-GMAC, Threefish-1024, Threefish-256, Threefish-512, Tnepres, Twofish, Twofish-GMAC, VMPC, VMPC-KSA3, XSALSA20, XTEA]  - SunJCE  [AES, ARCFOUR, Blowfish, DES, DESede, HmacMD5, HmacSHA1, HmacSHA224, HmacSHA256, HmacSHA384, HmacSHA512, RC2, SunTls12Prf, SunTlsKeyMaterial, SunTlsMasterSecret, SunTlsPrf, SunTlsRsaPremasterSecret] |

1. Key Pair Generator
   1. Asdf

|  |
| --- |
| - BC  [DH, DSA, DSTU4145, EC, ECDH, ECDHC, ECDHWITHSHA1KDF, ECDSA, ECGOST3410, ECGOST3410-2012, ECIES, ECMQV, ELGAMAL, GOST3410, RSA]  - SunEC  [EC]  - SunRsaSign  [RSA]  - SunMSCAPI  [RSA]  - SunJCE  [DiffieHellman]  - SunJSSE  [RSA]  - SUN  [DSA] |

1. Message Authentication Code
   1. Asdf

|  |
| --- |
| - BC  [AES-GMAC, AESCCMMAC, AESCMAC, ARIA-GMAC, BLOWFISHCMAC, CAMELLIA-GMAC, CAST6-GMAC, DESCMAC, DESEDECMAC, DESEDEMAC, DESEDEMAC/CFB8, DESEDEMAC64, DESEDEMAC64WITHISO7816-4PADDING, DESMAC, DESMAC/CFB8, DESMAC64, DESMAC64WITHISO7816-4PADDING, DESWITHISO9797, DSTU7624-128GMAC, DSTU7624-256GMAC, DSTU7624-512GMAC, DSTU7624GMAC, GOST28147MAC, GOST3412MAC, HMACDSTU7564-256, HMACDSTU7564-384, HMACDSTU7564-512, HMACGOST3411, HMACGOST3411-2012-256, HMACGOST3411-2012-512, HMACKECCAK224, HMACKECCAK256, HMACKECCAK288, HMACKECCAK384, HMACKECCAK512, HMACMD2, HMACMD4, HMACMD5, HMACRIPEMD128, HMACRIPEMD160, HMACRIPEMD256, HMACRIPEMD320, HMACSHA1, HMACSHA224, HMACSHA256, HMACSHA3-224, HMACSHA3-256, HMACSHA3-384, HMACSHA3-512, HMACSHA384, HMACSHA512, HMACSHA512/224, HMACSHA512/256, HMACSkein-1024-1024, HMACSkein-1024-384, HMACSkein-1024-512, HMACSkein-256-128, HMACSkein-256-160, HMACSkein-256-224, HMACSkein-256-256, HMACSkein-512-128, HMACSkein-512-160, HMACSkein-512-224, HMACSkein-512-256, HMACSkein-512-384, HMACSkein-512-512, HMACTIGER, HMACWHIRLPOOL, IDEAMAC, IDEAMAC/CFB8, ISO9797ALG3MAC, ISO9797ALG3WITHISO7816-4PADDING, NOEKEON-GMAC, OLDHMACSHA384, OLDHMACSHA512, PBEWITHHMACRIPEMD160, PBEWITHHMACSHA, PBEWITHHMACSHA1, PBEWITHHMACSHA224, PBEWITHHMACSHA256, PBEWITHHMACSHA384, PBEWITHHMACSHA512, POLY1305, POLY1305-AES, POLY1305-ARIA, POLY1305-CAMELLIA, POLY1305-CAST6, POLY1305-NOEKEON, POLY1305-RC6, POLY1305-SEED, POLY1305-SERPENT, POLY1305-SM4, POLY1305-Twofish, RC2MAC, RC2MAC/CFB8, RC5MAC, RC5MAC/CFB8, RC6-GMAC, SEED-CMAC, SEED-GMAC, SERPENT-GMAC, SIPHASH-2-4, SIPHASH-4-8, SKIPJACKMAC, SKIPJACKMAC/CFB8, SM4-CMAC, SM4-GMAC, Shacal-2CMAC, Skein-MAC-1024-1024, Skein-MAC-1024-384, Skein-MAC-1024-512, Skein-MAC-256-128, Skein-MAC-256-160, Skein-MAC-256-224, Skein-MAC-256-256, Skein-MAC-512-128, Skein-MAC-512-160, Skein-MAC-512-224, Skein-MAC-512-256, Skein-MAC-512-384, Skein-MAC-512-512, TNEPRES-GMAC, Threefish-1024CMAC, Threefish-256CMAC, Threefish-512CMAC, Twofish-GMAC, VMPCMAC]  - SunJCE  [HmacMD5, HmacPBESHA1, HmacSHA1, HmacSHA224, HmacSHA256, HmacSHA384, HmacSHA512, PBEWithHmacSHA1, PBEWithHmacSHA224, PBEWithHmacSHA256, PBEWithHmacSHA384, PBEWithHmacSHA512, SslMacMD5, SslMacSHA1] |

1. Cipher
   1. Asdf

|  |
| --- |
| - BC  [1.2.392.200011.61.1.1.1.2, 1.2.392.200011.61.1.1.1.3, 1.2.392.200011.61.1.1.1.4, 1.2.410.200004.1.4, 1.2.410.200046.1.1.1, 1.2.410.200046.1.1.11, 1.2.410.200046.1.1.12, 1.2.410.200046.1.1.13, 1.2.410.200046.1.1.14, 1.2.410.200046.1.1.2, 1.2.410.200046.1.1.3, 1.2.410.200046.1.1.4, 1.2.410.200046.1.1.6, 1.2.410.200046.1.1.7, 1.2.410.200046.1.1.8, 1.2.410.200046.1.1.9, 1.2.643.2.2.13.0, 1.2.643.2.2.13.1, 1.2.643.2.2.21, 1.2.804.2.1.1.1.1.1.3.1.1, 1.2.804.2.1.1.1.1.1.3.1.2, 1.2.804.2.1.1.1.1.1.3.1.3, 1.2.804.2.1.1.1.1.1.3.2.1, 1.2.804.2.1.1.1.1.1.3.2.2, 1.2.804.2.1.1.1.1.1.3.2.3, 1.2.804.2.1.1.1.1.1.3.3.1, 1.2.804.2.1.1.1.1.1.3.3.2, 1.2.804.2.1.1.1.1.1.3.3.3, 1.2.804.2.1.1.1.1.1.3.5.1, 1.2.804.2.1.1.1.1.1.3.5.2, 1.2.804.2.1.1.1.1.1.3.5.3, 1.2.804.2.1.1.1.1.1.3.6.1, 1.2.804.2.1.1.1.1.1.3.6.2, 1.2.804.2.1.1.1.1.1.3.6.3, 1.2.804.2.1.1.1.1.1.3.8.1, 1.2.804.2.1.1.1.1.1.3.8.2, 1.2.804.2.1.1.1.1.1.3.8.3, 1.2.840.113533.7.66.10, 1.2.840.113549.1.1.1, 1.2.840.113549.1.1.7, 1.2.840.113549.1.9.16.3.6, 1.2.840.113549.3.2, 1.2.840.113549.3.7, 1.3.14.3.2.7, 1.3.6.1.4.1.11591.13.2.1, 1.3.6.1.4.1.11591.13.2.2, 1.3.6.1.4.1.11591.13.2.21, 1.3.6.1.4.1.11591.13.2.22, 1.3.6.1.4.1.11591.13.2.23, 1.3.6.1.4.1.11591.13.2.24, 1.3.6.1.4.1.11591.13.2.3, 1.3.6.1.4.1.11591.13.2.4, 1.3.6.1.4.1.11591.13.2.41, 1.3.6.1.4.1.11591.13.2.42, 1.3.6.1.4.1.11591.13.2.43, 1.3.6.1.4.1.11591.13.2.44, 1.3.6.1.4.1.188.7.1.1.2, 1.3.6.1.4.1.3029.1.1.2, 2.16.840.1.101.3.4.1.1, 2.16.840.1.101.3.4.1.2, 2.16.840.1.101.3.4.1.21, 2.16.840.1.101.3.4.1.22, 2.16.840.1.101.3.4.1.23, 2.16.840.1.101.3.4.1.24, 2.16.840.1.101.3.4.1.3, 2.16.840.1.101.3.4.1.4, 2.16.840.1.101.3.4.1.41, 2.16.840.1.101.3.4.1.42, 2.16.840.1.101.3.4.1.43, 2.16.840.1.101.3.4.1.44, 2.5.8.1.1, AES, AESRFC3211WRAP, AESRFC5649WRAP, AESWRAP, AESWRAPPAD, ARC4, ARIA, ARIARFC3211WRAP, ARIAWRAP, ARIAWRAPPAD, BLOWFISH, BROKENPBEWITHMD5ANDDES, BROKENPBEWITHSHA1ANDDES, BROKENPBEWITHSHAAND2-KEYTRIPLEDES-CBC, BROKENPBEWITHSHAAND3-KEYTRIPLEDES-CBC, CAMELLIA, CAMELLIARFC3211WRAP, CAMELLIAWRAP, CAST5, CAST6, CCM, CHACHA, CHACHA7539, DES, DESEDE, DESEDERFC3211WRAP, DESEDEWRAP, DESRFC3211WRAP, DHIES, DHIESWITHDESEDE-CBC, DHIESwithAES-CBC, DSTU7624, DSTU7624-128, DSTU7624-128KW, DSTU7624-256, DSTU7624-256KW, DSTU7624-512, DSTU7624-512KW, DSTU7624KW, ECIES, ECIESwithAES-CBC, ECIESwithDESEDE-CBC, ELGAMAL, ELGAMAL/PKCS1, GCM, GOST28147, GOST3412-2015, GOST3412-2015/CBC, GOST3412-2015/CFB, GOST3412-2015/CFB8, GOST3412-2015/CTR, GOST3412-2015/OFB, Grain128, Grainv1, HC128, HC256, IDEA, IES, IESWITHDESEDE-CBC, IESwithAES-CBC, NOEKEON, OID.1.2.392.200011.61.1.1.1.2, OID.1.2.392.200011.61.1.1.1.3, OID.1.2.392.200011.61.1.1.1.4, OID.1.2.410.200004.1.4, OID.1.2.410.200046.1.1.1, OID.1.2.410.200046.1.1.11, OID.1.2.410.200046.1.1.12, OID.1.2.410.200046.1.1.13, OID.1.2.410.200046.1.1.14, OID.1.2.410.200046.1.1.2, OID.1.2.410.200046.1.1.3, OID.1.2.410.200046.1.1.4, OID.1.2.410.200046.1.1.6, OID.1.2.410.200046.1.1.7, OID.1.2.410.200046.1.1.8, OID.1.2.410.200046.1.1.9, OID.1.2.804.2.1.1.1.1.1.3.1.1, OID.1.2.804.2.1.1.1.1.1.3.1.2, OID.1.2.804.2.1.1.1.1.1.3.1.3, OID.1.2.804.2.1.1.1.1.1.3.2.1, OID.1.2.804.2.1.1.1.1.1.3.2.2, OID.1.2.804.2.1.1.1.1.1.3.2.3, OID.1.2.804.2.1.1.1.1.1.3.3.1, OID.1.2.804.2.1.1.1.1.1.3.3.2, OID.1.2.804.2.1.1.1.1.1.3.3.3, OID.1.2.804.2.1.1.1.1.1.3.5.1, OID.1.2.804.2.1.1.1.1.1.3.5.2, OID.1.2.804.2.1.1.1.1.1.3.5.3, OID.1.2.804.2.1.1.1.1.1.3.6.1, OID.1.2.804.2.1.1.1.1.1.3.6.2, OID.1.2.804.2.1.1.1.1.1.3.6.3, OID.1.2.804.2.1.1.1.1.1.3.8.1, OID.1.2.804.2.1.1.1.1.1.3.8.2, OID.1.2.804.2.1.1.1.1.1.3.8.3, OID.1.2.840.113533.7.66.10, OID.1.2.840.113549.1.1.1, OID.1.2.840.113549.1.1.7, OID.1.2.840.113549.1.9.16.3.6, OID.1.2.840.113549.3.2, OID.1.2.840.113549.3.7, OID.1.3.14.3.2.7, OID.1.3.6.1.4.1.11591.13.2.1, OID.1.3.6.1.4.1.11591.13.2.2, OID.1.3.6.1.4.1.11591.13.2.21, OID.1.3.6.1.4.1.11591.13.2.22, OID.1.3.6.1.4.1.11591.13.2.23, OID.1.3.6.1.4.1.11591.13.2.24, OID.1.3.6.1.4.1.11591.13.2.3, OID.1.3.6.1.4.1.11591.13.2.4, OID.1.3.6.1.4.1.11591.13.2.41, OID.1.3.6.1.4.1.11591.13.2.42, OID.1.3.6.1.4.1.11591.13.2.43, OID.1.3.6.1.4.1.11591.13.2.44, OID.1.3.6.1.4.1.188.7.1.1.2, OID.1.3.6.1.4.1.3029.1.1.2, OID.2.16.840.1.101.3.4.1.1, OID.2.16.840.1.101.3.4.1.2, OID.2.16.840.1.101.3.4.1.21, OID.2.16.840.1.101.3.4.1.22, OID.2.16.840.1.101.3.4.1.23, OID.2.16.840.1.101.3.4.1.24, OID.2.16.840.1.101.3.4.1.3, OID.2.16.840.1.101.3.4.1.4, OID.2.16.840.1.101.3.4.1.41, OID.2.16.840.1.101.3.4.1.42, OID.2.16.840.1.101.3.4.1.43, OID.2.16.840.1.101.3.4.1.44, OID.2.5.8.1.1, OLDPBEWITHSHAAND3-KEYTRIPLEDES-CBC, OLDPBEWITHSHAANDTWOFISH-CBC, PBEWITHMD2ANDDES, PBEWITHMD5AND128BITAES-CBC-OPENSSL, PBEWITHMD5AND192BITAES-CBC-OPENSSL, PBEWITHMD5AND256BITAES-CBC-OPENSSL, PBEWITHMD5ANDDES, PBEWITHMD5ANDRC2, PBEWITHSHA1ANDDES, PBEWITHSHA1ANDRC2, PBEWITHSHA256AND128BITAES-CBC-BC, PBEWITHSHA256AND192BITAES-CBC-BC, PBEWITHSHA256AND256BITAES-CBC-BC, PBEWITHSHAAND128BITAES-CBC-BC, PBEWITHSHAAND128BITRC2-CBC, PBEWITHSHAAND128BITRC4, PBEWITHSHAAND192BITAES-CBC-BC, PBEWITHSHAAND2-KEYTRIPLEDES-CBC, PBEWITHSHAAND256BITAES-CBC-BC, PBEWITHSHAAND3-KEYTRIPLEDES-CBC, PBEWITHSHAAND40BITRC2-CBC, PBEWITHSHAAND40BITRC4, PBEWITHSHAANDIDEA-CBC, PBEWITHSHAANDTWOFISH-CBC, RC2, RC2WRAP, RC5, RC5-64, RC6, RIJNDAEL, RSA, RSA/1, RSA/2, RSA/ISO9796-1, RSA/OAEP, RSA/PKCS1, RSA/RAW, SALSA20, SEED, SEEDWRAP, SHACAL-2, SKIPJACK, SM4, Serpent, Shacal2, TEA, Threefish-1024, Threefish-256, Threefish-512, Tnepres, Twofish, VMPC, VMPC-KSA3, XSALSA20, XTEA]  - SunMSCAPI  [RSA, RSA/ECB/PKCS1Padding]  - SunJCE  [AES, AESWrap, AESWrap\_128, AESWrap\_192, AESWrap\_256, AES\_128/CBC/NoPadding, AES\_128/CFB/NoPadding, AES\_128/ECB/NoPadding, AES\_128/GCM/NoPadding, AES\_128/OFB/NoPadding, AES\_192/CBC/NoPadding, AES\_192/CFB/NoPadding, AES\_192/ECB/NoPadding, AES\_192/GCM/NoPadding, AES\_192/OFB/NoPadding, AES\_256/CBC/NoPadding, AES\_256/CFB/NoPadding, AES\_256/ECB/NoPadding, AES\_256/GCM/NoPadding, AES\_256/OFB/NoPadding, ARCFOUR, Blowfish, DES, DESede, DESedeWrap, PBEWithHmacSHA1AndAES\_128, PBEWithHmacSHA1AndAES\_256, PBEWithHmacSHA224AndAES\_128, PBEWithHmacSHA224AndAES\_256, PBEWithHmacSHA256AndAES\_128, PBEWithHmacSHA256AndAES\_256, PBEWithHmacSHA384AndAES\_128, PBEWithHmacSHA384AndAES\_256, PBEWithHmacSHA512AndAES\_128, PBEWithHmacSHA512AndAES\_256, PBEWithMD5AndDES, PBEWithMD5AndTripleDES, PBEWithSHA1AndDESede, PBEWithSHA1AndRC2\_128, PBEWithSHA1AndRC2\_40, PBEWithSHA1AndRC4\_128, PBEWithSHA1AndRC4\_40, RC2, RSA] |

1. Signature
   1. Signature algorithm

|  |
| --- |
| - BC  [1.2.840.113549.1.1.10, DDSA, DETDSA, DSA, DSTU4145, ECDDSA, ECDSA, ECGOST3410, ECGOST3410-2012-256, ECGOST3410-2012-512, GOST3410, GOST3411-2012-256WITHECGOST3410-2012-256, GOST3411-2012-512WITHECGOST3410-2012-512, GOST3411WITHDSTU4145, GOST3411WITHDSTU4145LE, GOST3411WITHECGOST3410, MD2WITHRSA, MD4WITHRSA, MD5WITHRSA, MD5WITHRSA/ISO9796-2, NONEWITHDSA, NONEwithECDSA, OID.1.2.840.113549.1.1.10, RAWRSASSA-PSS, RIPEMD128WITHRSA, RIPEMD128WITHRSA/X9.31, RIPEMD160WITHECDSA, RIPEMD160WITHPLAIN-ECDSA, RIPEMD160WITHRSA, RIPEMD160WITHRSA/X9.31, RIPEMD160withRSA/ISO9796-2, RIPEMD256WITHRSA, RMD128WITHRSA, RMD128WITHRSA/X9.31, RMD160WITHRSA, RMD160WITHRSA/X9.31, RMD256WITHRSA, RSA, RSASSA-PSS, SHA1WITHCVC-ECDSA, SHA1WITHDDSA, SHA1WITHDETDSA, SHA1WITHECDDSA, SHA1WITHECNR, SHA1WITHPLAIN-ECDSA, SHA1WITHRSA, SHA1WITHRSA/ISO9796-2, SHA1WITHRSA/X9.31, SHA1WITHRSAANDMGF1, SHA224WITHCVC-ECDSA, SHA224WITHDDSA, SHA224WITHDETDSA, SHA224WITHDSA, SHA224WITHECDDSA, SHA224WITHECDSA, SHA224WITHECNR, SHA224WITHPLAIN-ECDSA, SHA224WITHRSA, SHA224WITHRSA/ISO9796-2, SHA224WITHRSA/X9.31, SHA224WITHRSAANDMGF1, SHA256WITHCVC-ECDSA, SHA256WITHDDSA, SHA256WITHDETDSA, SHA256WITHDSA, SHA256WITHECDDSA, SHA256WITHECDSA, SHA256WITHECNR, SHA256WITHPLAIN-ECDSA, SHA256WITHRSA, SHA256WITHRSA/ISO9796-2, SHA256WITHRSA/X9.31, SHA256WITHRSAANDMGF1, SHA3-224WITHDDSA, SHA3-224WITHDSA, SHA3-224WITHECDDSA, SHA3-224WITHECDSA, SHA3-224WITHRSA, SHA3-224WITHRSAANDMGF1, SHA3-256WITHDDSA, SHA3-256WITHDSA, SHA3-256WITHECDDSA, SHA3-256WITHECDSA, SHA3-256WITHRSA, SHA3-256WITHRSAANDMGF1, SHA3-384WITHDDSA, SHA3-384WITHDSA, SHA3-384WITHECDDSA, SHA3-384WITHECDSA, SHA3-384WITHRSA, SHA3-384WITHRSAANDMGF1, SHA3-512WITHDDSA, SHA3-512WITHDSA, SHA3-512WITHECDDSA, SHA3-512WITHECDSA, SHA3-512WITHRSA, SHA3-512WITHRSAANDMGF1, SHA384WITHCVC-ECDSA, SHA384WITHDDSA, SHA384WITHDETDSA, SHA384WITHDSA, SHA384WITHECDDSA, SHA384WITHECDSA, SHA384WITHECNR, SHA384WITHPLAIN-ECDSA, SHA384WITHRSA, SHA384WITHRSA/ISO9796-2, SHA384WITHRSA/X9.31, SHA384WITHRSAANDMGF1, SHA512(224)WITHRSA, SHA512(224)WITHRSA/ISO9796-2, SHA512(224)WITHRSA/X9.31, SHA512(224)WITHRSAANDMGF1, SHA512(256)WITHRSA, SHA512(256)WITHRSA/ISO9796-2, SHA512(256)WITHRSA/X9.31, SHA512(256)WITHRSAANDMGF1, SHA512WITHCVC-ECDSA, SHA512WITHDDSA, SHA512WITHDETDSA, SHA512WITHDSA, SHA512WITHECDDSA, SHA512WITHECDSA, SHA512WITHECNR, SHA512WITHPLAIN-ECDSA, SHA512WITHRSA, SHA512WITHRSA/ISO9796-2, SHA512WITHRSA/X9.31, SHA512WITHRSAANDMGF1, SM3WITHSM2, WhirlpoolWITHRSA/ISO9796-2, WhirlpoolWITHRSA/X9.31]  - SunEC  [NONEwithECDSA, SHA1withECDSA, SHA224withECDSA, SHA256withECDSA, SHA384withECDSA, SHA512withECDSA]  - SunRsaSign  [MD2withRSA, MD5withRSA, SHA1withRSA, SHA224withRSA, SHA256withRSA, SHA384withRSA, SHA512withRSA]  - SunMSCAPI  [MD2withRSA, MD5withRSA, NONEwithRSA, SHA1withRSA, SHA256withRSA, SHA384withRSA, SHA512withRSA]  - SunJSSE  [MD2withRSA, MD5andSHA1withRSA, MD5withRSA, SHA1withRSA]  - SUN  [NONEwithDSA, SHA1withDSA, SHA224withDSA, SHA256withDSA] |

1. Asdf
2. asdf