**Features[¶](https://pycryptodome.readthedocs.io/en/latest/src/features.html?highlight=hkdf%20hazmat" \l "features" \o "Permalink to this headline)**

This page lists the low-level primitives that PyCryptodome provides.

You are expected to have a solid understanding of cryptography and security engineering to successfully use them.

You must also be able to recognize that some primitives are obsolete (e.g. TDES) or even unsecure (RC4). They are provided only to enable backward compatibility where required by the applications.

A list of useful resources in that area can be found on [Matthew Green’s blog](http://blog.cryptographyengineering.com/p/useful-cryptography-resources.html).

* Symmetric ciphers:
  + AES
  + Single and Triple DES (legacy)
  + CAST-128 (legacy)
  + RC2 (legacy)
* Traditional modes of operations for symmetric ciphers:
  + ECB
  + CBC
  + CFB
  + OFB
  + CTR
  + OpenPGP (a variant of CFB, RFC4880)
* Authenticated Encryption:
  + CCM (AES only)
  + EAX
  + GCM (AES only)
  + SIV (AES only)
  + OCB (AES only)
  + ChaCha20-Poly1305
* Stream ciphers:
  + Salsa20
  + ChaCha20
  + RC4 (legacy)
* Cryptographic hashes:
  + SHA-1
  + SHA-2 hashes (224, 256, 384, 512, 512/224, 512/256)
  + SHA-3 hashes (224, 256, 384, 512) and XOFs (SHAKE128, SHAKE256)
  + Functions derived from SHA-3 (cSHAKE128, cSHAKE256, TupleHash128, TupleHash256)
  + KangarooTwelve (XOF)
  + Keccak (original submission to SHA-3)
  + BLAKE2b and BLAKE2s
  + RIPE-MD160 (legacy)
  + MD5 (legacy)
* Message Authentication Codes (MAC):
  + HMAC
  + CMAC
  + KMAC128 and KMAC256
  + Poly1305
* Asymmetric key generation:
  + RSA
  + ECC (NIST P-curves; Ed25519, Ed448)
  + DSA
  + ElGamal (legacy)
* Export and import format for asymmetric keys:
  + PEM (clear and encrypted)
  + PKCS#8 (clear and encrypted)
  + ASN.1 DER
* Asymmetric ciphers:
  + PKCS#1 (RSA)
    - RSAES-PKCS1-v1\_5
    - RSAES-OAEP
* Asymmetric digital signatures:
  + PKCS#1 (RSA)
    - RSASSA-PKCS1-v1\_5
    - RSASSA-PSS
  + (EC)DSA
    - Nonce-based (FIPS 186-3)
    - Deterministic (RFC6979)
  + EdDSA
* Key derivation:
  + PBKDF2
  + scrypt
  + **HKDF**
  + PBKDF1 (legacy)
* Other cryptographic protocols:
  + Shamir Secret Sharing
  + Padding
    - PKCS#7
    - ISO-7816
    - X.923

[Previous](https://pycryptodome.readthedocs.io/en/latest/src/introduction.html)[Next](https://pycryptodome.readthedocs.io/en/latest/src/installation.html)