**Mango API Reference**

This document describes the core API functions provided by Mango's cryptographic engine (CryptoLib) and data profiler (InputProfiler).

**🔐 CryptoLib (Core Cryptographic Engine)**

CryptoLib(string password)

* **Description:** Creates a new cryptographic engine using the provided password.
* **Parameters:**
  + password *(string)* — Session password used to derive internal keys.
* **Returns:** CryptoLib instance

CryptoLib(string password, CryptoLibOptions options)

* **Description:** Creates a new cryptographic engine with optional advanced configuration.
* **Parameters:**
  + password *(string)* — Session password
  + options *(CryptoLibOptions)* — Optional settings such as round override or custom IV
* **Returns:** CryptoLib instance

**⚙️ CryptoLibOptions (Optional Configuration)**

CryptoLibOptions(int? rounds = null, byte[]? defaultIV = null)

* **Description:** Allows optional customization of the cryptographic engine.
* **Parameters:**
  + rounds *(int?)* — Optional override for global rounds; useful for experimentation
  + defaultIV *(byte[]?)* — Optional custom IV; if not provided, a secure default IV is used**Usage Example:**

CryptoLibOptions options = new CryptoLibOptions(

rounds: 6,

defaultIV: new byte[] { 0x1A, 0x2B, 0x3C, 0x4D, 0x5E, 0x6F, 0x70, 0x81, 0x92, 0xA3, 0xB4, 0xC5 }

);

CryptoLib crypto = new CryptoLib("my password", options);

**🔐 CryptoLib Methods**

byte[] Encrypt((byte ID, byte TR)[] sequence, byte rounds, byte[] input)

* **Description:** Encrypts input data using the specified transform sequence and round count.
* **Parameters:**
  + sequence — Transform sequence (ID and per-transform round count)
  + rounds — Number of global rounds to apply
  + input — The raw byte array to encrypt
* **Returns:** Encrypted byte array (includes header metadata)

byte[] Decrypt(byte[] encrypted)

* **Description:** Decrypts input data by extracting configuration from the header.
* **Parameters:**
  + encrypted — Encrypted data with header
* **Returns:** Decrypted original byte array

byte[] EncryptBlock(byte[] input)

* **Description:** Encrypts a block of data **without adding a header**. Assumes prior context has been cached from previous call to Encrypt().
* **Parameters:**
  + input — Raw input block (e.g., 1024 bytes)
* **Returns:** Headerless encrypted block

byte[] DecryptBlock(byte[] input)

* **Description:** Decrypts a headerless block of data. Assumes prior context has been cached from previous call to Decrypt().
* **Parameters:**
  + input — Encrypted block (headerless)
* **Returns:** Decrypted block

**🔍 InputProfiler (Input Analysis & Type Detection)**

InputProfile GetInputProfile(byte[] input)

* **Description:** Analyzes input data to determine its type (natural, random, etc.) and returns an optimized sequence + round configuration.
* **Parameters:**
  + input — Input data to classify
* **Returns:** InputProfile object containing:
  + Sequence — Recommended transform sequence
  + GlobalRounds — Recommended round count
  + InputType — Enum indicating data class (e.g., Natural, Random, Sequence)

This API reference represents the core surface area of Mango's runtime and adaptive encryption system. For higher-level use cases, see MangoAC or MangoBM.

For sequence design, transform customization, and metric testing, refer to the Mango Workbench documentation.