**1. Introduction**

**1.1 What is Mango?**

**Mango** is a next-generation cryptographic system that reimagines how encryption sequences are developed, optimized, and applied. At its core lies a robust **cryptographic library**—a high-performance, fully reversible engine capable of adaptive encryption using composable atomic transforms. Developers can use Mango out of the box to secure data using pre-optimized, high-scoring sequences—no tuning or configuration required.

Complementing this library is the **Mango Workbench**: a modular research toolchain used to discover and validate new encryption sequences. The Workbench includes tools like *Munge*, a sequence discovery engine that evaluates millions of permutations to find the best fit for specific data types (e.g., Natural, Random, Structured). These discoveries form the foundation for Mango’s default sequences.

In short:

* **The Cryptographic Library** is production-ready and secure by default.
* **The Workbench** is an optional toolkit for researchers, analysts, and developers seeking domain-specific or experimental encryption sequences.

This dual-architecture allows Mango to serve both practical encryption needs and academic exploration.

**1.1.1 Mango: Cryptographic Library vs. Workbench**

This chart outlines the distinction between Mango's production-ready cryptographic engine and its research-oriented workbench used for sequence discovery and optimization.

|  |  |  |
| --- | --- | --- |
| Feature | 🧱 Cryptographic Library | 🧪 Workbench (Research Suite) |
| Purpose | Secure data encryption in production | Discover and optimize sequences for different data types |
| Usage | Out-of-the-box with high-quality default sequences | Research-driven tuning of transform order and depth |
| Interface | Simple Encrypt() / Decrypt() APIs | Modular tools like Munge, BTR, and analysis modules |
| Transform Source | Uses pre-vetted, high-scoring sequences | Explores vast permutations using multi-metric scoring |
| Data Awareness | Auto-classifies input (e.g., Natural, Random, etc.) | Lets you target specific domains with focused tests |
| Developer Role | Drop-in encryption component | Researcher/analyst playground |
| Reversibility | Guaranteed (every sequence is invertible) | Verified during testing |
| Scoring Metrics | Optional, for audit/debug | Core to transform selection |
| Speed | Optimized for runtime | Optimized for discovery and insight |

**1.2 Philosophy & Goals**

Mango is guided by the belief that cryptography can be:

* 🔎 **Transparent** – All scoring, transform logic, and decision-making are explainable and inspectable.
* 🧩 **Modular** – Encryption is constructed from atomic, interchangeable building blocks.
* 🧠 **Adaptive** – Input is classified and profiled, enabling sequence selection based on actual data characteristics.
* 📈 **Provable** – Every sequence is scored with rigorous, multi-metric analysis to ensure objective comparison and repeatability.

The goal is a flexible, evolving encryption framework that offers both practical superiority and scientific accountability.

**1.3 Key Features**

* 🔐 **Atomic Transform Engine** – 40+ built-in transforms allow fine-grained encryption design. Custom transforms are easy to add.
* 🧠 **Munge: Sequence Discovery Engine** – Exhaustively searches for top-performing sequences across transform permutations and round variations.
* 📊 **Metric-Driven Scoring** – Evaluates encryption quality using up to 9 orthogonal metrics, including Avalanche, Entropy, Key Dependency, and more.
* 🧬 **Input-Aware Adaptation** – Automatically classifies input data and applies the most appropriate transform sequence.
* ♻️ **Fully Reversible Design** – All transforms and sequences are validated for round-trip integrity.
* 🚀 **AES Benchmarking** – Built-in tools compare Mango sequences against AES in terms of strength, diffusion, and runtime performance.