05\_AdaptiveTheory

## What Is Adaptive Cryptography?

Adaptive cryptography refers to encryption that tailors itself to the characteristics of the input data.

Rather than applying the same fixed sequence of operations regardless of structure—as traditional ciphers like AES do—adaptive systems respond dynamically to data patterns such as regularity, randomness, or predictability.

Mango’s adaptivity is deterministic, not random: the same input type will always result in the same transform sequence.

## Why Adaptivity Matters

In real-world applications, data is rarely uniform or truly random.

Static ciphers can underperform when applied to highly structured input, leaking small biases that may reduce overall diffusion or entropy.

Mango’s adaptive model helps close this gap by profiling input and selecting a pre-tuned transformation path designed to maximize disruption and cryptographic robustness for that type of data.

## Input Profiling

Mango classifies input into one of four InputTypes:

* • Natural — e.g., prose, source code, configuration files
* • Random — e.g., encrypted data, compressed archives
* • Sequence — e.g., incrementing counters, test harnesses
* • Combined — a fusion class optimized for hybrid/complex input

Combined is not a fallback. It is the most versatile and difficult to tune of the four, designed specifically for mixed-input environments.

## InputProfile: The Engine's Core

Once an InputType is detected, Mango loads the corresponding InputProfile.

Each InputProfile is a sequence of transforms, each with a specified transform round (TR) count, and a global round (GR) multiplier.

Mango Adaptive Cryptography uses these curated sequences to guarantee strong and reproducible encryption behavior.

All profiles are versioned, deterministic, and tuned for their respective data types.

## Workbench: The Profile Forge

The Mango Workbench allows developers to construct sequences manually or through automation (e.g., Munge).

When you build a custom sequence under a selected InputType, you are effectively proposing a new InputProfile.

This is exactly how the built-in profiles were discovered—Munge tested millions of sequences, evaluating them by cryptographic metrics such as entropy, avalanche, and bit variance.

Once a promising sequence is found, it can be exported and reused just like any other profile.

## Real-World Adaptivity: Custom InputTypes

Industries with unique data formats (e.g., genomic data, telemetry streams, logs) can create custom input datasets and run Munge over them to discover new god-sequences.

This workflow allows Mango to adapt to your data—not just ‘data in general’.

* 1. Capture representative input.

2. Run Workbench with the input and initiate Munge.

3. Promote the discovered sequence to a stable InputProfile.

## Are Custom InputProfiles Portable?

Yes. While input classification (InputProfiler) is customizable, the resulting InputProfile—a pipeline of transform IDs and round counts—is always portable.

It is completely deterministic and agnostic to platform.

The engine doesn’t care why a profile was selected—only what it is.

## Security Notes

Only Mango Adaptive Cryptography uses production-validated, high-quality sequences.

The Workbench, while powerful, does not enforce cryptographic safety—it is a sandbox.

For sensitive workloads, only use sequences derived from vetted Munge/BTR output with pass counts of 9/9 and strong cryptographic metric profiles.