Tool Name: **Damage Ransom Decrypting Tool**

Description:
A ransomware decryption utility aimed at reversing file damage from "Damage" ransomware using static key libraries and cryptographic reversal techniques.

What Is This Tool About?
It is designed to analyze encrypted files, recognize the Damage ransomware pattern, and apply matching decryption strategies for file recovery.

Key Characteristics / Features:

- Identifies Damage ransomware variant
- Static and dynamic decryption methods
- Uses embedded or known decryption keys
- Works on most common file types
- Batch and selective decryption
- Lightweight and portable
- Error-handling and rollback support
- Provides decryption reports
- CLI tool with advanced options
- Available for Windows
- Recognizes signature-based patterns
- Updates decryption engine frequently
- Safe overwrite with original file backup
- Detects fake extensions
- Sandbox-compatible

Types / Modules Available:

- Damage Ransom Identifier
- Key Lookup & Mapping Engine
- Batch File Decryptor
- Decryption Validator
- Error & Log Reporter

How Will This Tool Help?
It assists in decrypting and restoring files targeted by Damage ransomware, enabling incident responders to avoid ransom payments and ensure continuity.

Liner Summary:

- Targets Damage ransomware
- Detects encrypted file structure
- Matches with known decryption keys
- Applies reversal logic
- Lightweight execution
- Logs every decryption attempt
- CLI-based flexible tool
- Reliable for common ransomware extensions
- Safe overwrite with backup
- Fast processing
- Error report generation
- Works on offline systems
- Helps law enforcement analysis
- Batch processing capable
- Supports encrypted doc, pdf, media files

Time to Use / Best Case Scenarios:

- Once Damage infection is confirmed
- When encrypted samples are collected
- After forensic snapshot
- While assessing scope of data damage

When to Use During Investigation:

- After compromise confirmation
- Before paying ransom
- For testing decrypted files
- As part of incident response planning

Best Person to Use This Tool & Required Skills:
Best User: Malware Analyst / Security Response Engineer
Required Skills:

- Understanding of ransomware behavior
- CLI command usage
- Cryptographic concepts
- File format and metadata analysis

Flaws / Suggestions to Improve:

- Limited UI (CLI only)
- Not effective on unknown variants
- No GUI for general users
- Dependency on latest key sets
- Needs offline validation tool

Good About the Tool:

- Focused and fast
- Reliable on supported variants
- Small footprint
- Maintains logs and integrity checks
- Ideal for forensic use