Tool Name: **Cyborg Ransomware Decryption Tool**

Description:
A specialized utility designed to decrypt files affected by Cyborg ransomware variants using known keys or algorithmic weaknesses.

What Is This Tool About?
This tool helps victims recover encrypted files without paying ransom by reversing Cyborg ransomware encryption using static or dynamic techniques.

Key Characteristics / Features:

- Supports known Cyborg variants (e.g., APT-CYBORG-007)
- Can detect and extract encryption keys from memory dumps
- Works on AES and RSA hybrid encryption used by Cyborg
- Portable executable, no installation required
- File format validation post-decryption
- GUI and CLI versions available
- Batch decryption mode
- Integrity check after decryption
- Windows OS support
- Encrypted file type identification
- Threat signature matching
- Generates decryption logs
- Offline decryption capability
- Tool auto-updates ransomware definitions
- Minimal system resource consumption

Types / Modules Available:

- Cyborg Decryptor Core Engine
- Memory Scanner for Key Extraction
- File Scanner & Identifier
- Batch Decryption Module
- Decryption Log Exporter

How Will This Tool Help?
Helps recover user data encrypted by Cyborg ransomware, prevents ransom payments, and aids forensic teams in understanding encryption flow.

Liner Summary:

- Detects Cyborg ransomware-encrypted files
- Identifies ransomware variant
- Attempts key extraction or known key match
- Decrypts files in bulk or one by one
- Cross-verifies output file integrity
- Works offline
- GUI and CLI support
- Portable utility
- Includes threat definition updates
- Uses secure overwrite during processing
- Good for enterprise or home use
- Supports logs and case file creation
- Memory dump compatible
- Operates in sandbox if needed
- Useful in law enforcement and DFIR cases

Time to Use / Best Case Scenarios:

- After detecting Cyborg infection
- Before ransom payment
- Post memory capture
- When file extensions are altered
- During ransomware variant analysis

When to Use During Investigation:

- Right after infection discovery
- During initial forensic triage

- After acquiring infected system image
- In digital recovery process
- As part of incident response

Best Person to Use This Tool & Required Skills:
Best User: DFIR Analyst / Malware Analyst
Required Skills:

- Knowledge of ransomware behavior
- Experience with encryption and key extraction
- Familiarity with system memory analysis
- Basic CLI/Git tools usage

Flaws / Suggestions to Improve:

- Limited to known Cyborg variants
- No real-time ransomware blocker
- Add cloud-based scanning for variants
- Improve UI for non-technical users
- Enhance key-finding heuristics

Good About the Tool:

- Effective against Cyborg variants
- Fast and accurate decryption
- Log-based documentation
- Works offline and securely
- Regular updates available