

# Forum:[Hack Forums](#)

Thread: [|| Free || Cipher Cracker |](#)

G\_Lock - February 9, 2026, 11:55 pm

## CIPHER CRACKER

An Educational Cybersecurity Suite for Learning Encryption, Cryptanalysis, and Password Security

Cipher Cracker is a Windows desktop application that teaches encryption and password security through hands-on, interactive demonstrations. It bridges the gap between classical cryptography (Caesar cipher) and modern encryption (AES-256), then shows exactly how and why passwords get cracked using real-world attack methodologies.

The core thesis of this tool: AES-256 encryption is mathematically unbreakable. But your password probably isn't. The weakest link in any encryption system is always the human element - the password you choose.

### What It Does

#### Classical Cryptography Module (Tabs 1-4)

- Encrypt/Decrypt: Apply Caesar cipher shifts (1-25) to plaintext and watch letter substitution in action
- Brute-Force Crack: Simultaneously try all 26 possible shifts - demonstrates why a 26-key keyspace is trivially insecure
- Frequency Analysis: Uses chi-squared statistical testing to compare letter distributions against English language patterns. Includes a visual bar chart showing observed vs. expected frequencies. Automatically identifies the correct shift without trying every possibility.
- Smart Crack: Hybrid approach combining frequency analysis with dictionary validation against 500 common English words. Ranks all 26 shifts by confidence score and provides CONFIRMED/LIKELY/POSSIBLE verdicts.

#### Modern Encryption Module (Tab 5 - File Encrypt)

- Encrypt any file with AES-256-CBC using PBKDF2 key derivation (100,000 iterations) with random salt and IV
- Decrypt files with the correct password
- File Forensics Engine: Analyzes files to detect encryption status using:
  - Shannon entropy calculation (measures randomness - encrypted data scores ~7.9/8.0)
  - Magic byte signature detection (identifies 30+ file formats: PNG, PDF, ZIP, EXE, MP4, SQLite, etc.)
  - Encryption method identification (detects ZIP encryption, PDF password protection, PGP/GPG, custom AES)
- Hex Viewer: Displays raw bytes in professional offset + hex + ASCII format

## Password Cracking Module (Tab 6 - Password Cracker)

A 5-phase attack pipeline that demonstrates real-world password cracking methodologies:

1. Phase 1 - Dictionary Attack: Tests 200 of the most common passwords from real breach databases (123456, password, dragon, qwerty, etc.). Cracks ~5% of all passwords instantly.
2. Phase 2 - Pattern Attack: Generates keyboard walks (qwerty, 1qaz2wsx), sequential runs (abcdef, 987654), repeated characters (aaaaaa), date patterns (01012024, 19901225), and symbol sequences (!@#\$%^). Catches "creative" passwords that are actually predictable patterns.
3. Phase 3 - Mutation Attack: Takes dictionary words and applies transformations: capitalization (Password), ALL CAPS (PASSWORD), leet speak (p@ssw0rd), number suffixes (password123, password2026), and reversal (drowssap). Catches the "I made it clever" passwords.
4. Phase 4 - Word Combiner Attack: Combines 80 common "power words" (shadow, dragon, phantom, krypton, phoenix, etc.) with 8 separators and 3 case patterns. Generates ~32,640 combinations. Catches passwords like "Krypton!Phantom" that password meters rate as "Excellent" but are actually just two predictable words joined together.
5. Phase 5 - Brute Force: Exhaustive search through every combination of 72 characters (a-z, A-Z, 0-9, symbols) at incrementing lengths. Guaranteed to find any password given enough time. Demonstrates exponential keyspace growth and why length is the most important factor in password strength.

Anti-false-positive validation: Uses PKCS7 padding checks combined with Shannon entropy analysis of decrypted output (real data < 7.5 entropy vs. garbage data ~7.99) to prevent false cracks.

## Live Demo Module (Tab 7)

Three automated scenarios that encrypt a classified intelligence document and attempt to crack it in real-time:

- WEAK ("dragon"): Cracked instantly by Phase 1. Demonstrates that common passwords provide zero protection regardless of the encryption algorithm.
- MEDIUM ("Shadow2026"): Survives the dictionary but falls to Phase 3 mutations. Demonstrates that "clever" variations of common words are predictable.
- MILITARY ("Krypton!Phantom"): Survives Phases 1-3, cracked by Phase 4 word combiner. Demonstrates that even 15-character passwords with mixed case and symbols can fall if they're composed of dictionary words.
- Each demo includes a lesson explaining exactly why the password failed and what the fix is.

A bonus scenario shows that a 20-character passphrase with truly random composition survives all 5 phases - proving that AES-256 itself is not the problem, your password is.

[Image: <https://imgur.com/cPWeJET>]

[Image: <https://imgur.com/hZk5XJF>]

[Image: <https://imgur.com/UerzOkt>]

[Image: <https://imgur.com/fnFRtXf>]

[Image: <https://imgur.com/yt6zxwV>]

[Image: <https://imgur.com/Wg5AMoE>]