The Lewis Echo Theory: Final Manifesto (v4)

Author: Charles Lewis

Date: 2025-07-01

I. INTRODUCTION

The Lewis Echo Theory is a cryptographic chaining framework that explores echo-based transformations using SHA-256, ASCII-based logic, and Vigenère-style ciphering. It proposes that deterministic chaining can uncover predictable behavior and even expose structural collisions in cryptographic operations, such as salting patterns.

II. CORE CONCEPT

1. A base word is hashed using SHA-256.
2. The resulting hash becomes the key or input to the next operation (the "echo").
3. Variations include:
   - Reversing the word
   - Converting to ASCII and performing arithmetic shifts
   - Applying Vigenère cipher chaining using echoed keys
4. These chains are analyzed for deterministic repetition, clustering, and pseudo-salt behaviors.

This process is repeatable and supports:

- `--word` mode for single-word echo chaining

- `--wordlist` mode for batch echo testing

III. SMALL-SCALE TESTING

Example:

```
    $ python Echo_Theory_Engine.py --word awake
```

Result:

- The word "awake" is hashed
- The resulting hash is echoed through additional transformations
- Chain continues through multiple iterations with each hash becoming the key

---

IV. LARGE-SCALE TESTING: rockyou.txt

Example:

```
    $ python Echo_Theory_Engine.py --wordlist wordlist/rockyou.txt
```

Results:

- Echo chains from rockyou.txt showed early-stage convergence clusters
- Words reversed before hashing produced distinctly different paths
- Repeated patterns were found between unrelated words due to echo chaining

---

V. ASCII-BASED TRANSFORMATION TESTS

In this test, we:

- Converted words to ASCII ordinal values
- Applied modular transformations and shifts
- Converted ASCII sequences back to text and re-hashed them

Outcome:

- Echoing through ASCII preserved structure but revealed deterministic convergence
- Repeated patterns in ASCII shifts often returned to similar character sets
- When echoed into SHA-256, many converged back to previous hash states

---

VI. VIGENÈRE-STYLE CHAINING TESTS

In this variant, we:

- Used the SHA-256 hash of a word as a Vigenère cipher key
- Applied that key to subsequent words or characters
- Fed the resulting ciphertext back into the hashing loop

Findings:

- Deterministic key chaining produced tightly linked cryptographic chains
- Reuse of ciphertext as keys caused convergence in some paths
- Revealed pseudo-salt behavior that can be traced without external randomness

---

VII. SALT COLLISION DETECTION VIA ECHOES

- Echo chaining behaves like salt simulation
- Vigenère and ASCII transformations amplify this behavior
- Detected repeating hash chains that reveal internal structure of input influence

---

VIII. USE CASES

1. Echo-based password chaining & prediction
2. Salt resistance benchmarking
3. Cipher feedback chaining simulations
4. Input analysis under ASCII/Vigenère encoding and feedback

IX. CONCLUSION

The Lewis Echo Theory demonstrates that chaining hash inputs via echoes, ASCII logic, and Vigenère-style keys reveals consistent behaviors that are cryptographically significant. The framework provides a novel method to analyze deterministic cryptographic algorithms and simulate salt behavior under chaining loops.

Github Repository:

https://github.com/5p00k13/lewis-echo-theory