**Krypton Wargame – Individual PoC Report**

Intern Name: Ishan Chowdhury

Intern ID: 159

Team: SkullFaced

Mode: Solo Player

# 🎯 Objective

This Proof of Concept (PoC) report demonstrates successful completion of all levels in the Krypton Wargame from OverTheWire. It showcases practical application of cryptographic techniques such as ROT13, Caesar cipher, Base64, and binary analysis.

# 🛠 Tools & Techniques

- Linux Terminal Utilities: `cat`, `tr`, `strings`, `objdump`, `hexdump`  
- Python scripting for decryption and brute-force logic  
- Static analysis tools for binaries  
- SSH-based remote access

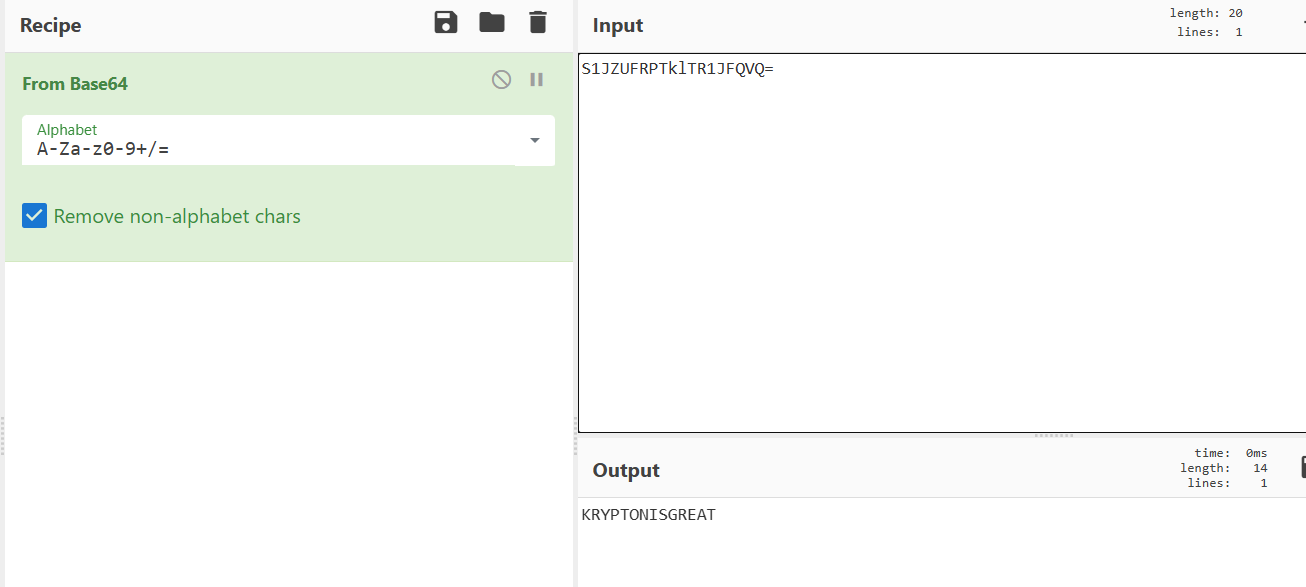
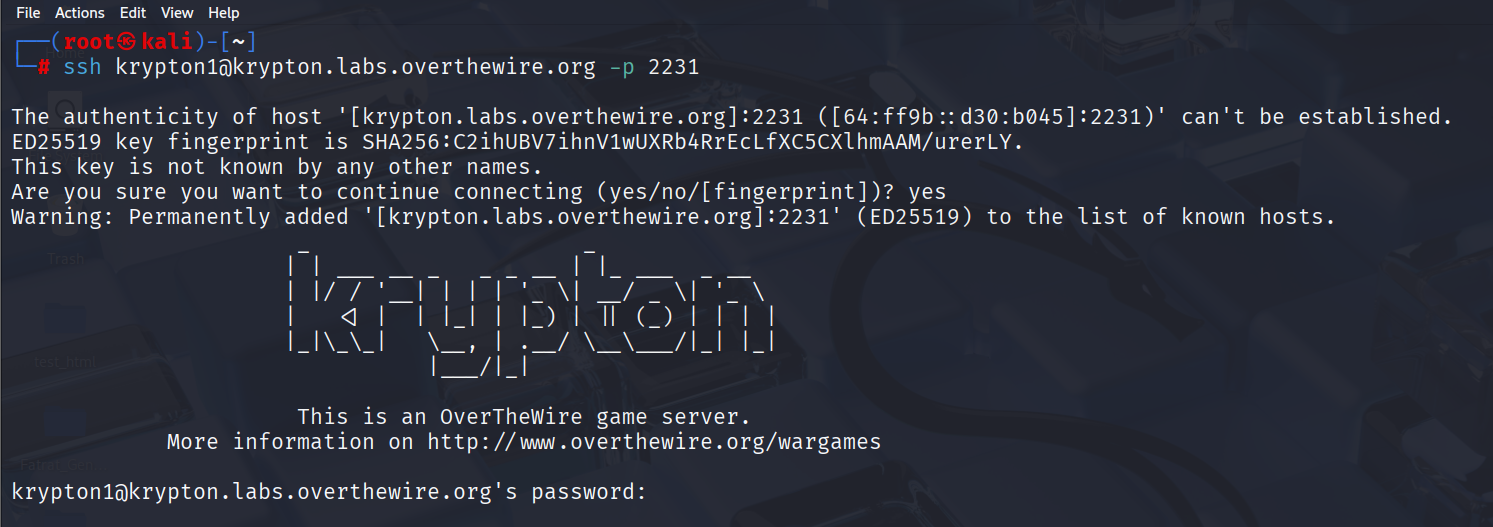
# 📘 Krypton Level Breakdown

## Level 0 → 1

**Method:** **Base64 decoding**

**Details:** Decode the provided Base64-encoded string to reveal the password, then SSH into the next level.

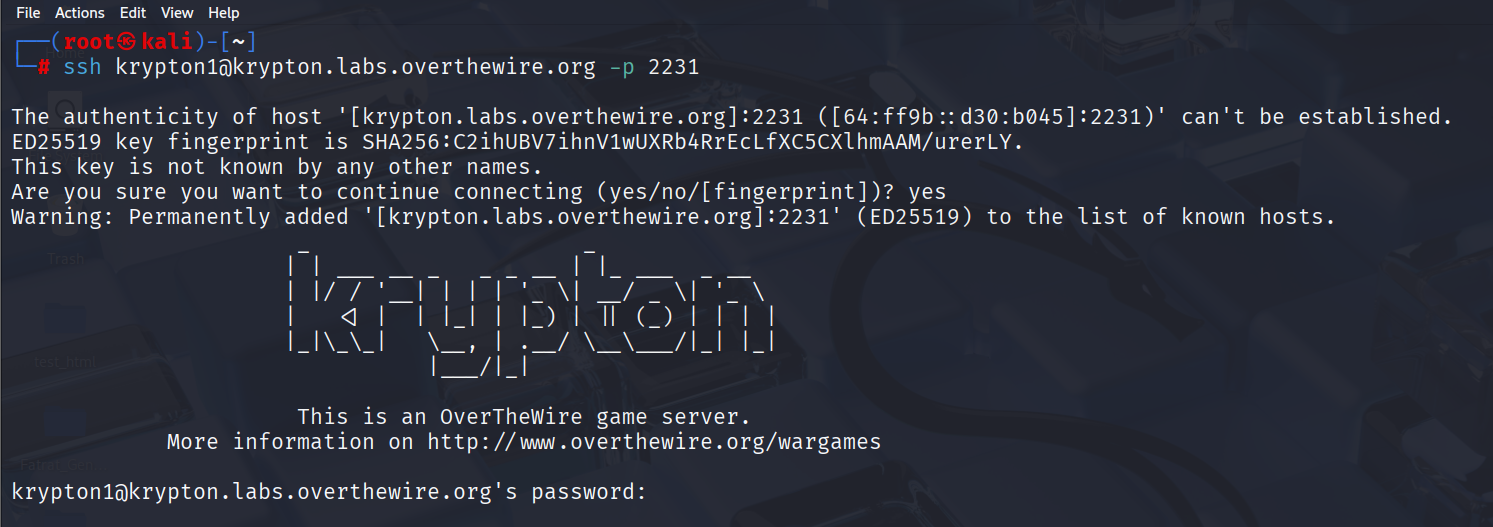
**Screenshot:**

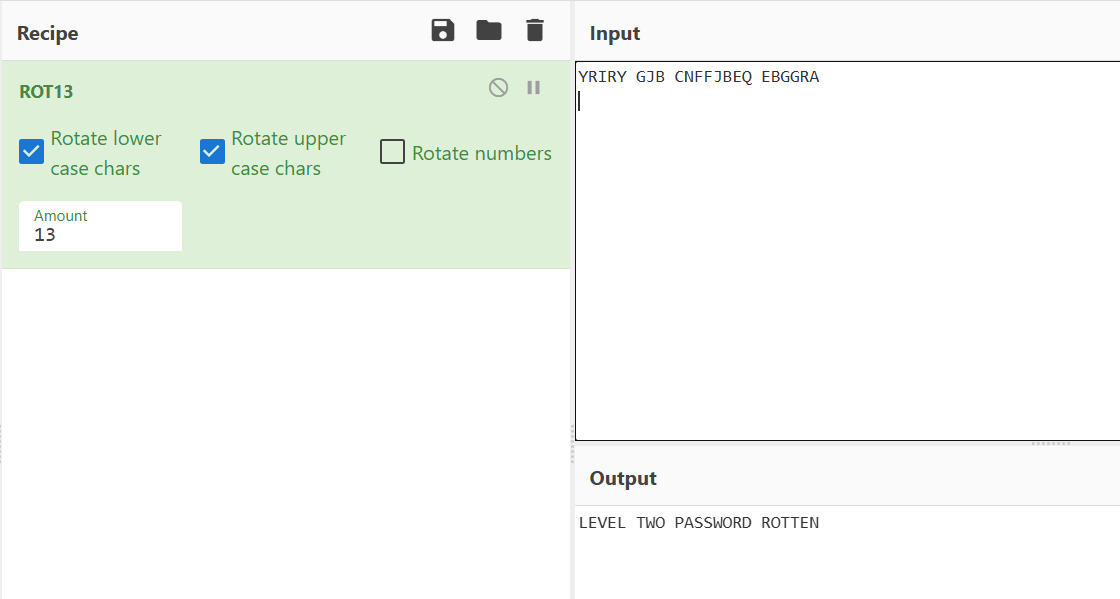
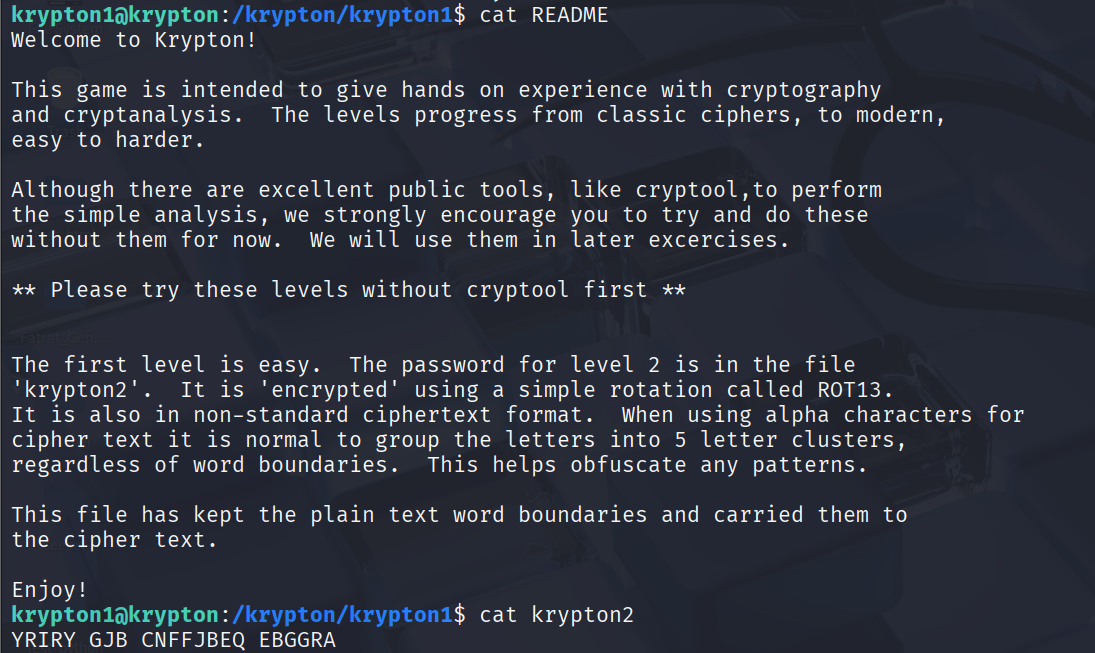


## Level 1 → 2

**Method:** **ROT13 substitution cipher**

**Details:** The encrypted password (in cryptic, five-letter grouped format) is decoded using ROT13.

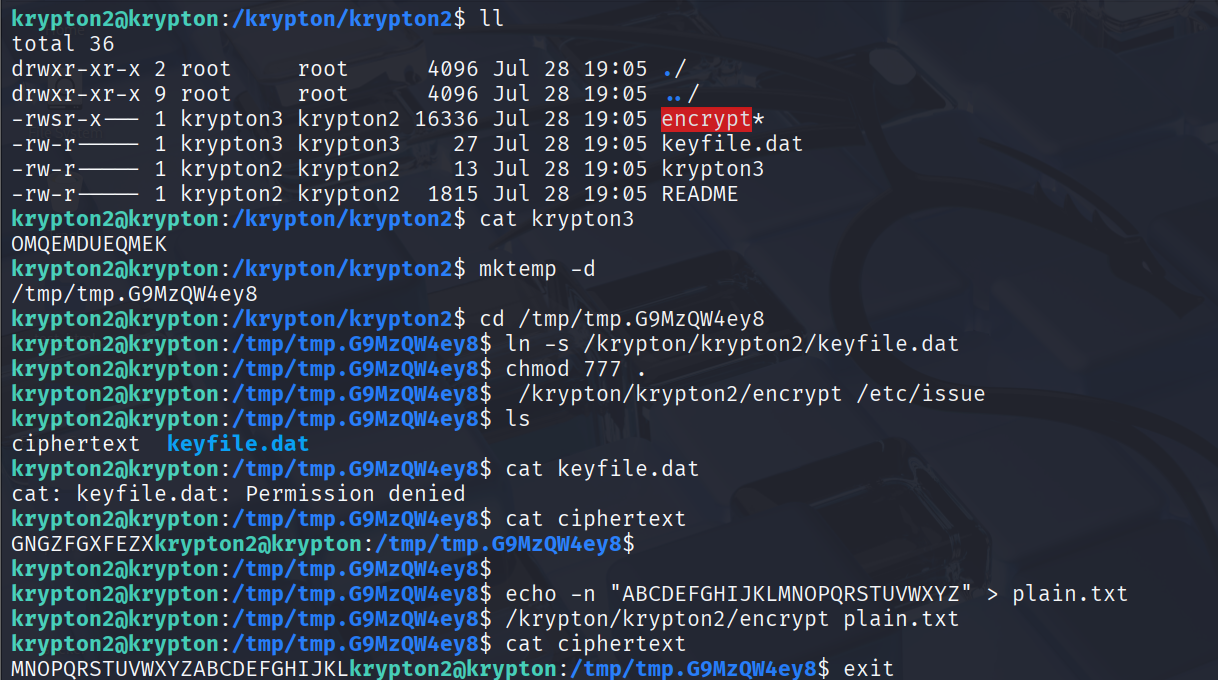
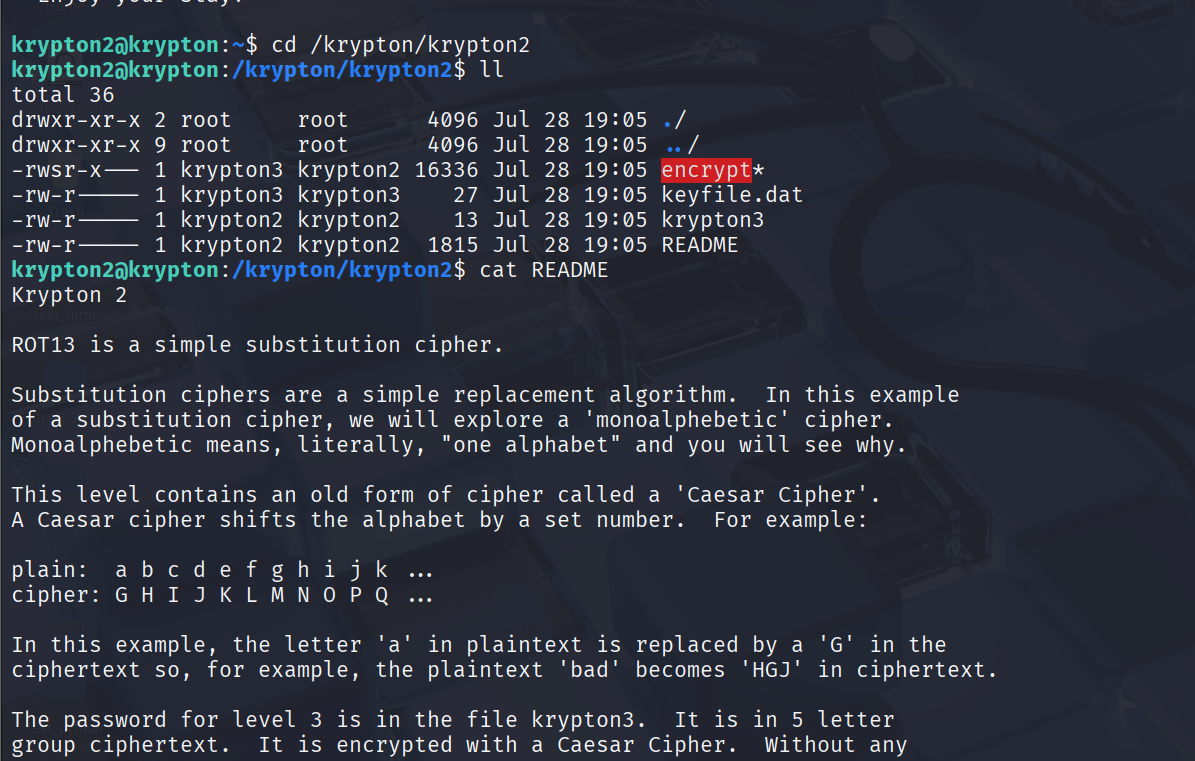
**Screenshot:**

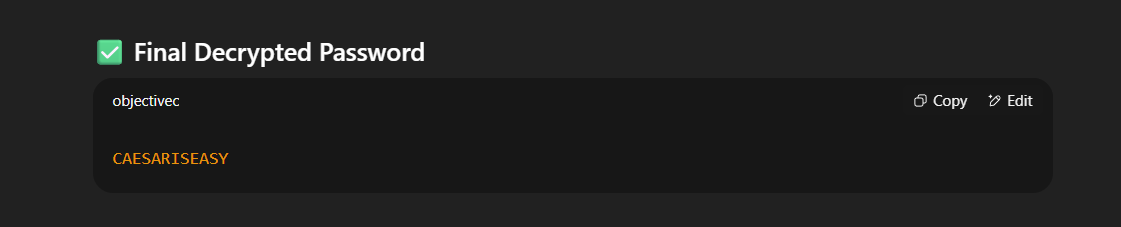


## Level 2 → 3

**Method:** **Caesar Cipher** (classic shift cipher)

**Details:** Use an encryption binary to determine the key shift, then apply Caesar decryption (using tr or brute force) to recover the actual password.

**Screenshot:**

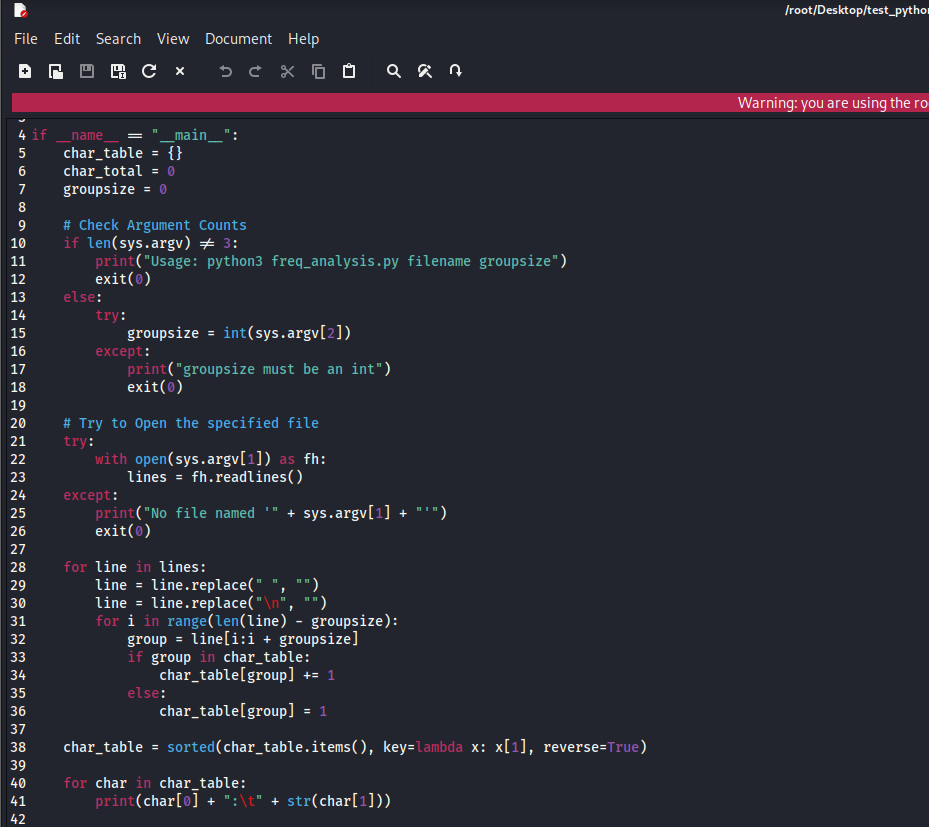
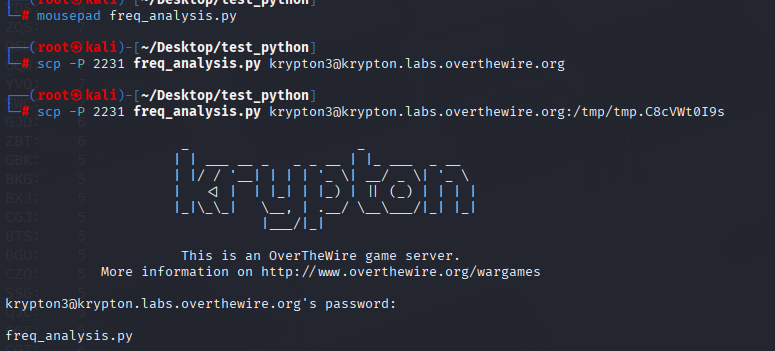
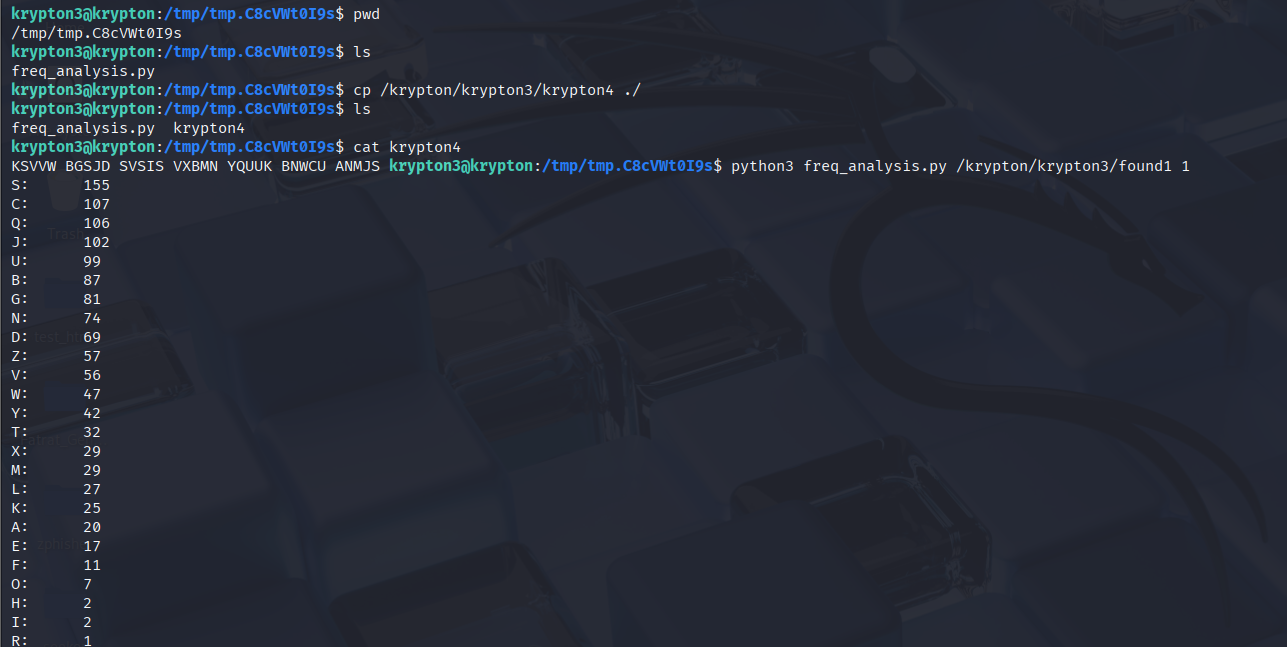


## Level 3 → 4

**Method:** **Frequency analysis + monoalphabetic substitution cipher**

**Details:** Analyze letter frequencies across multiple ciphertext files to map the most frequent letters to likely plaintext letters, then apply a custom tr translation to decode the password.

**Screenshot:**

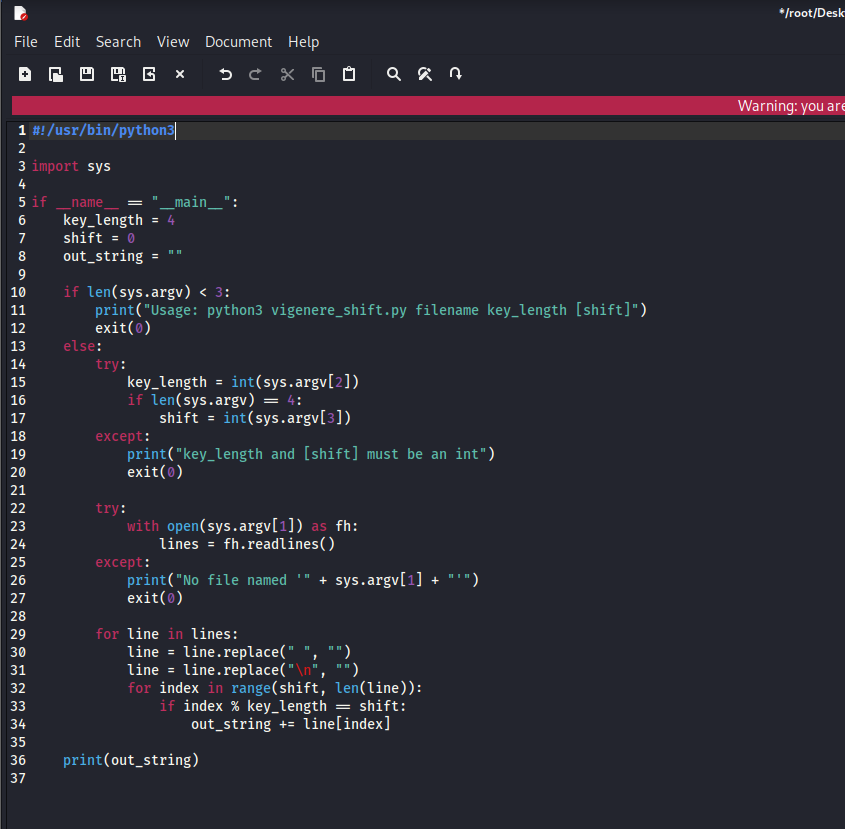
Screenshot 2025-08-07 141228Screenshot 2025-08-07 141344

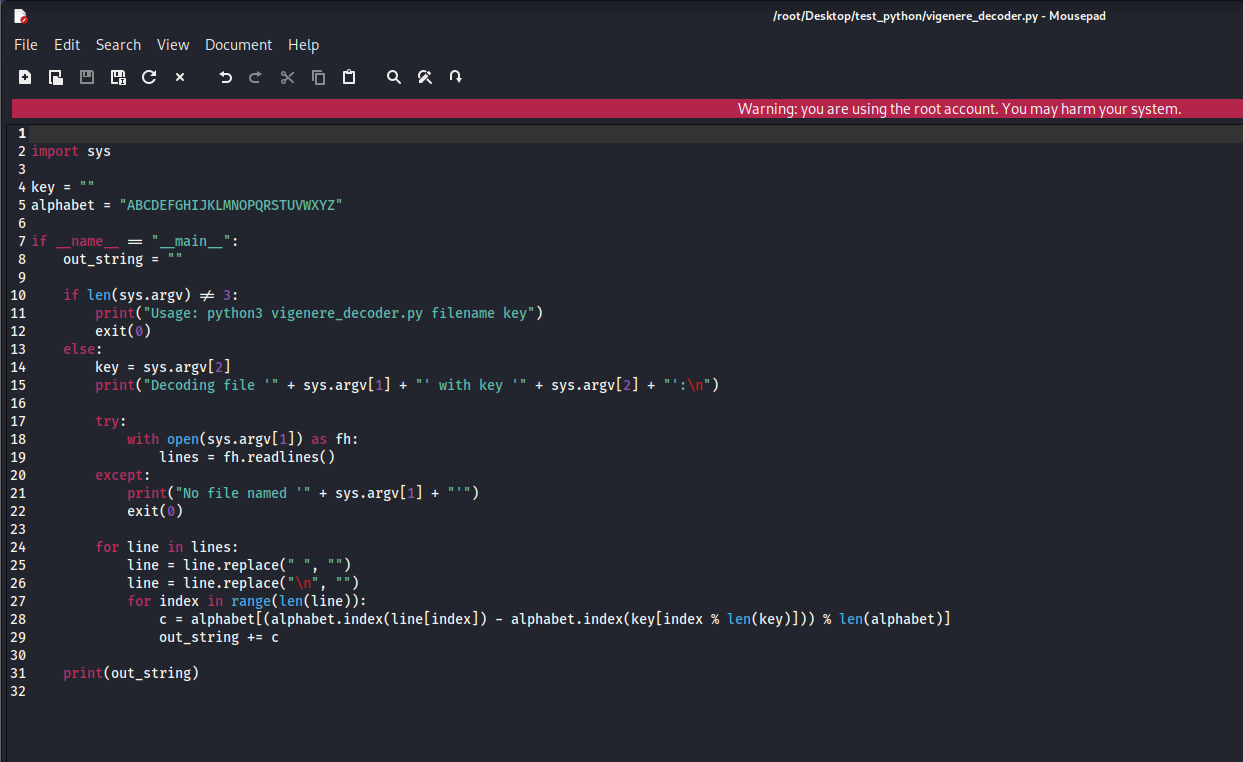
## Level 4 → 5

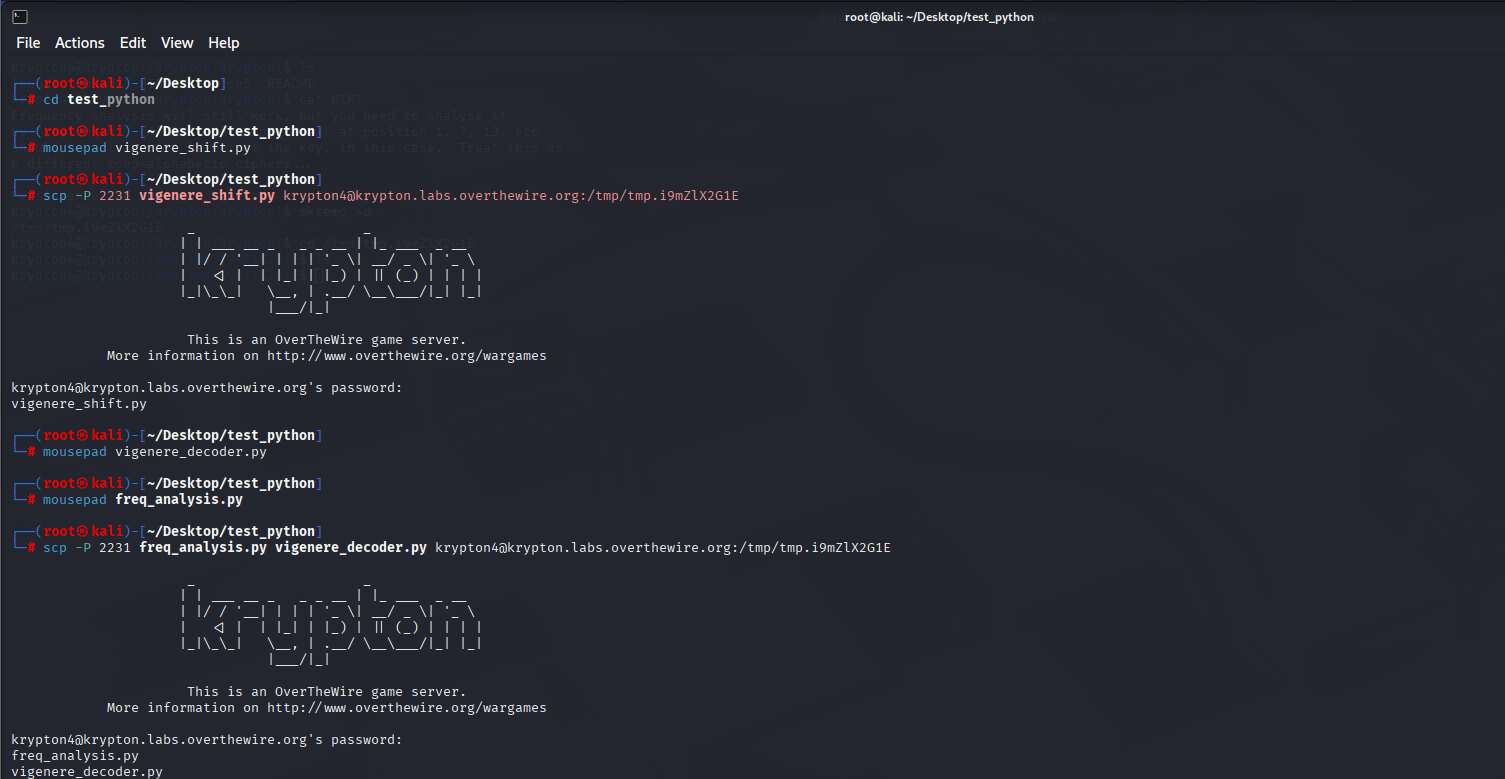
**Method:** **Vigenère Cipher** (polyalphabetic cipher) with a known key length

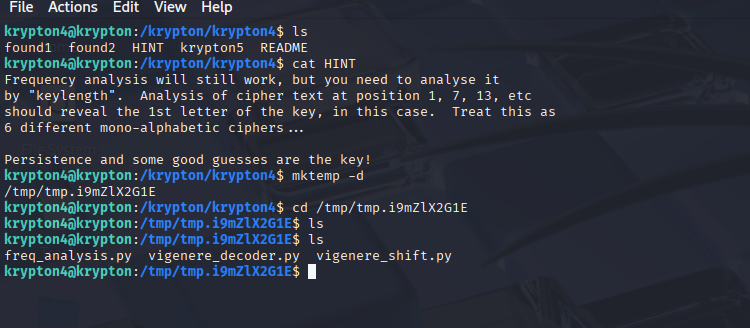
**Details:** Knowing the key length (6), use online tools (like dCode) to break the cipher and reveal the password.

**Screenshot:**

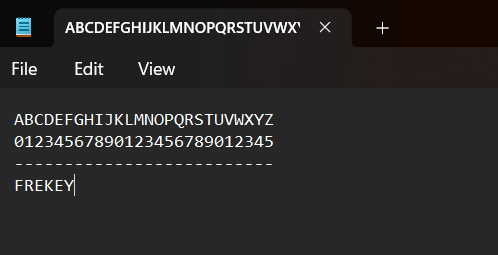


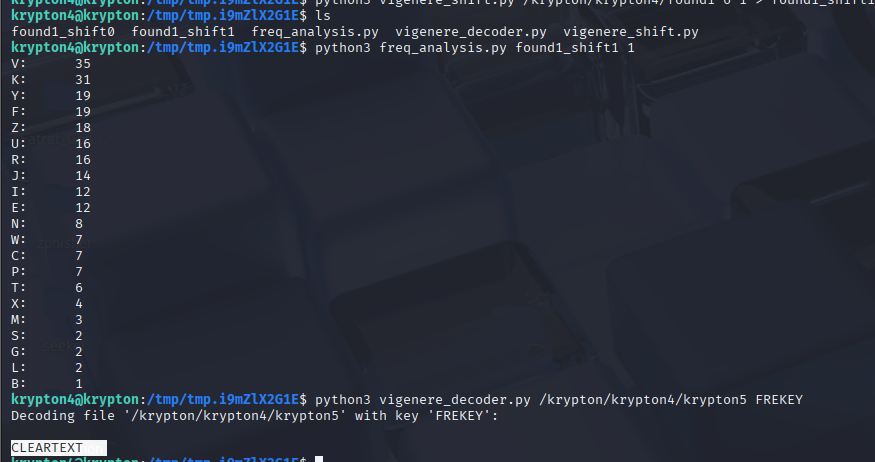










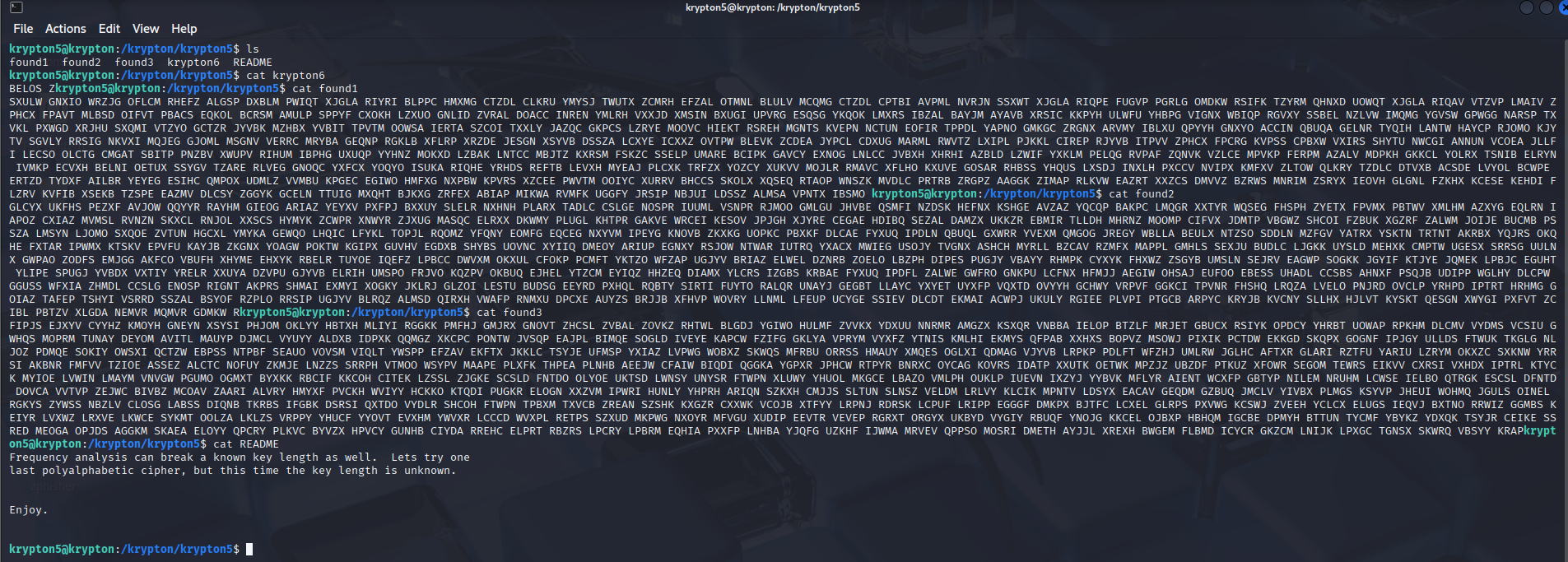


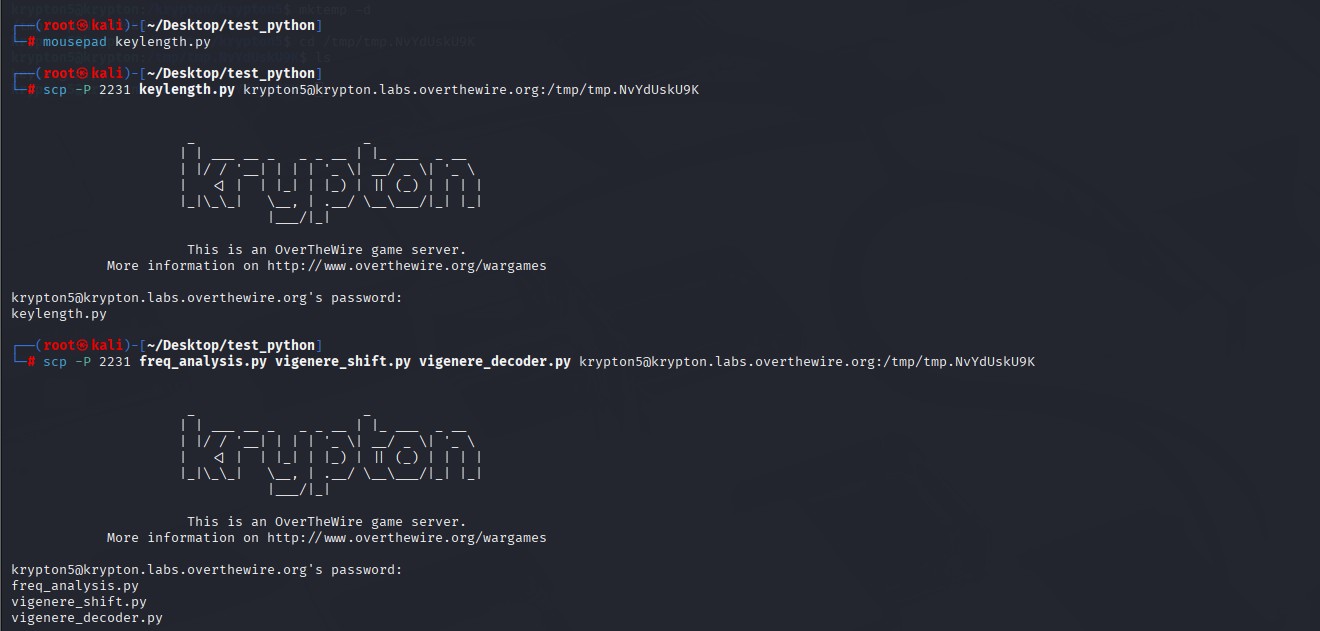
## Level 5 → 6

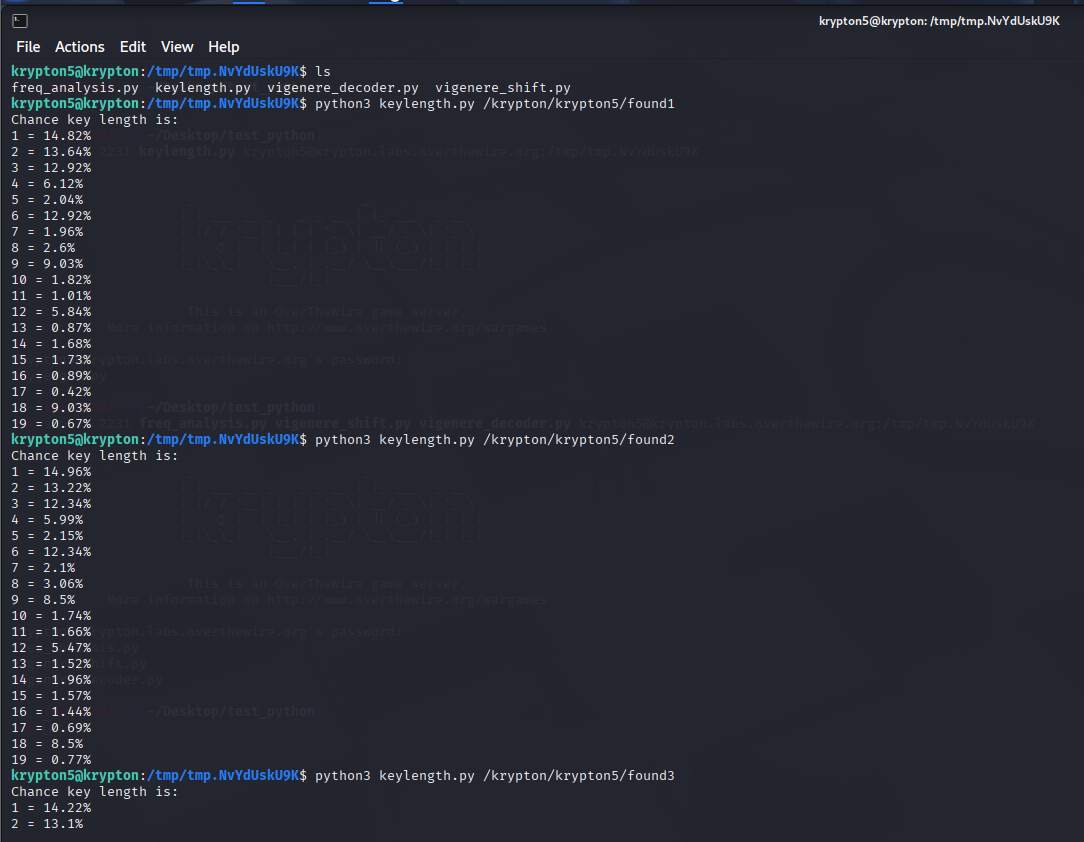
**Method:** **Vigenère Cipher** with unknown key length — solved using **Kasiski examination**

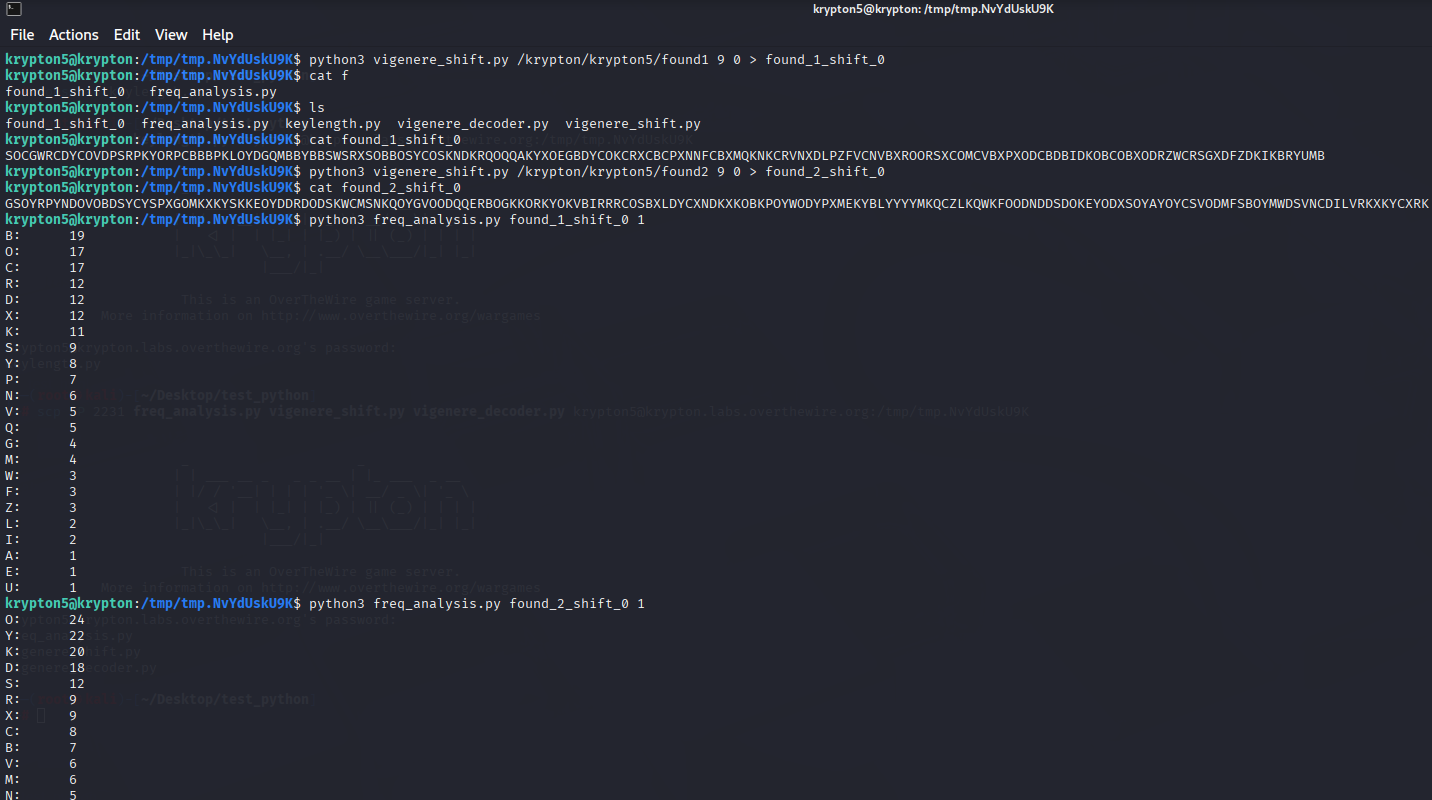
**Details:** Use Kasiski method to estimate possible key lengths (e.g., 3, 6, or 9), then decrypt using a compatible key length.

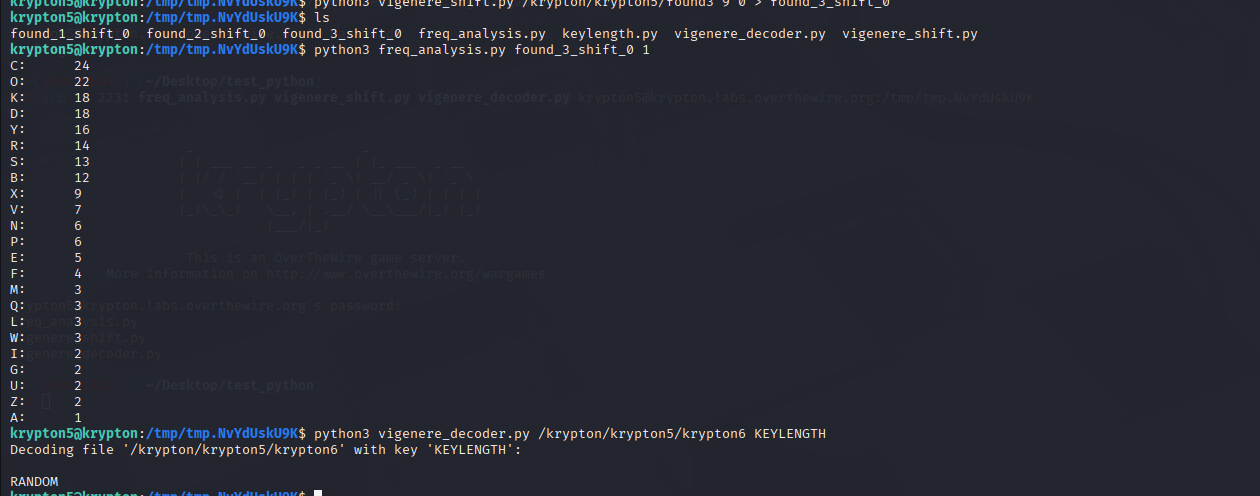
**Screenshot:**









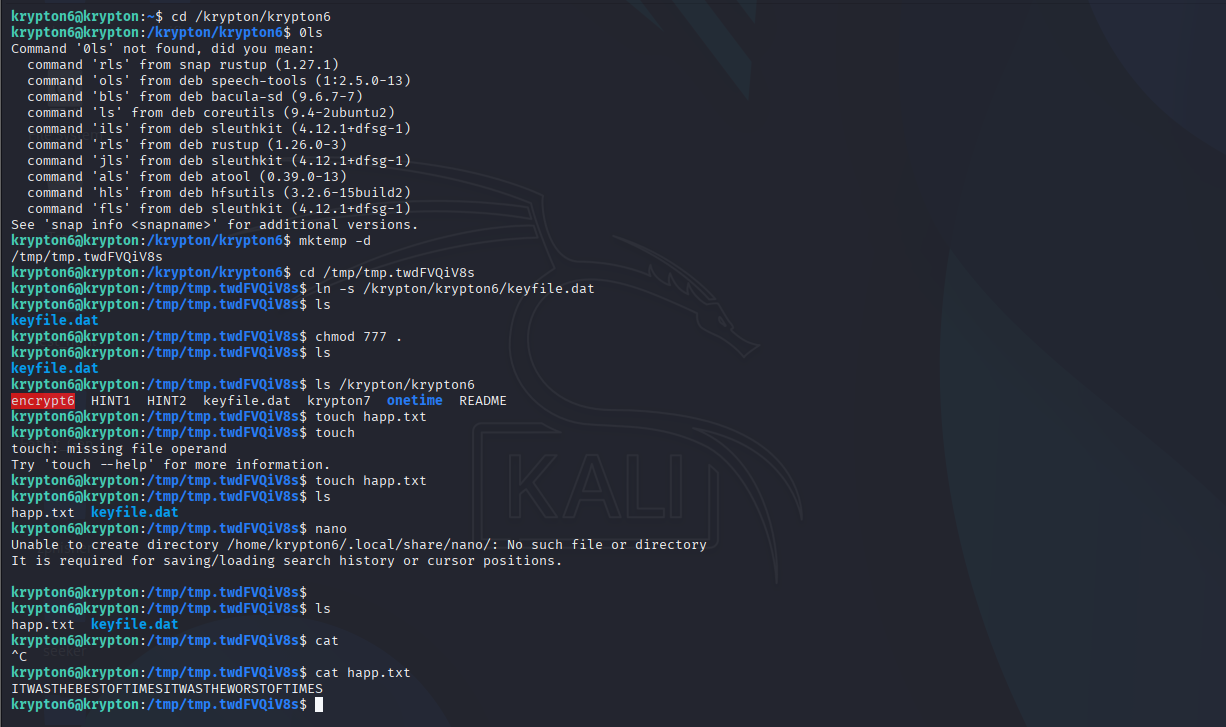


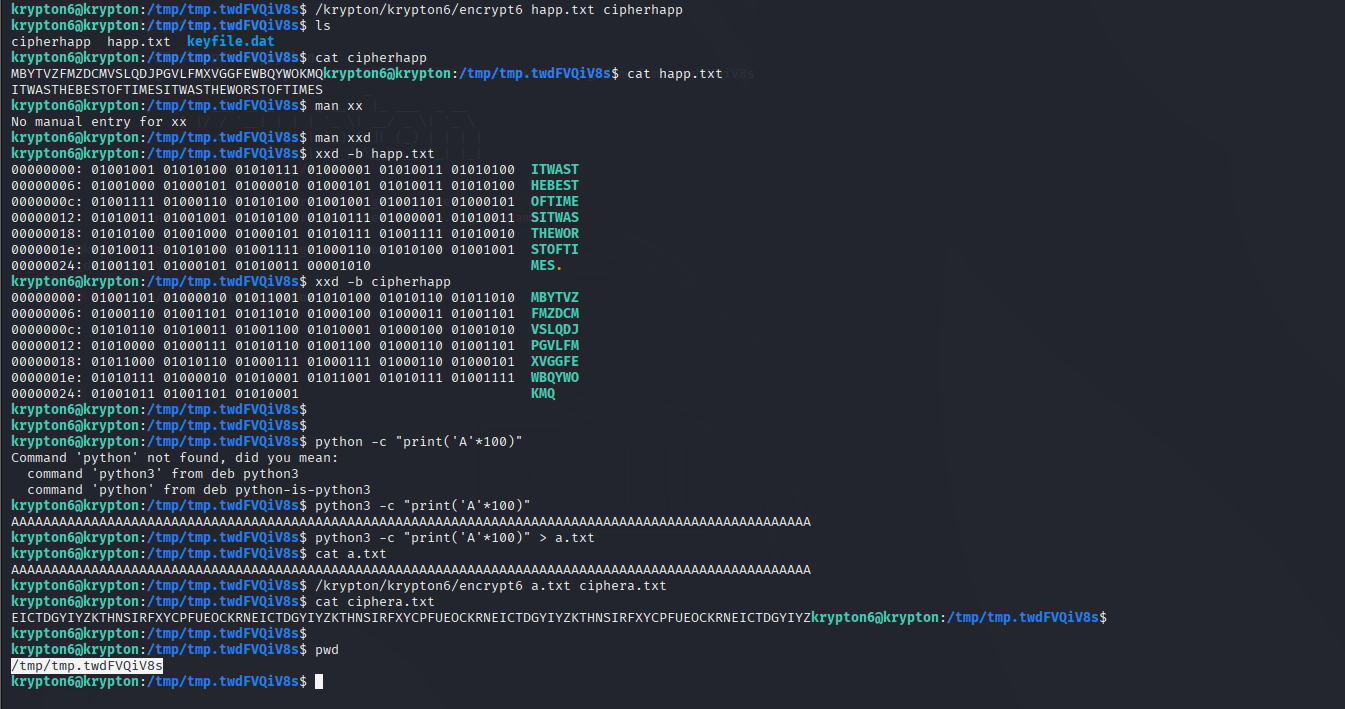
## Level 6 → 7

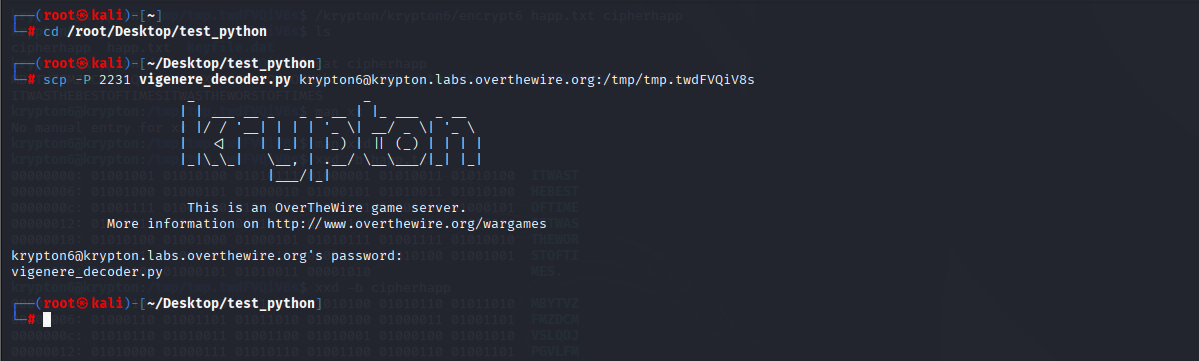
**Method:** Likely **stream cipher decryption** or advanced cryptanalysis

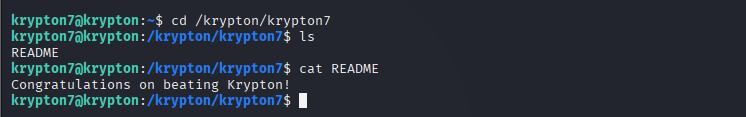
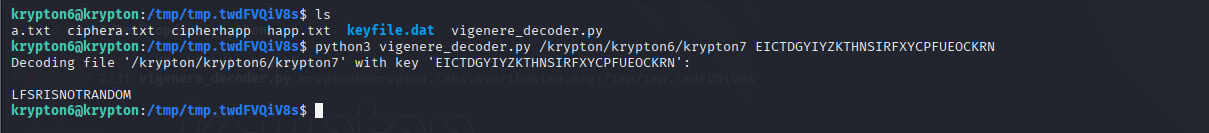
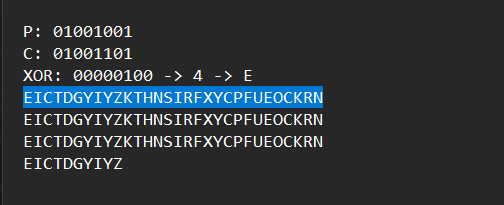
**Details (from video walkthrough):** This final level transitions from block ciphers to stream ciphers.

**Screenshot:**









# 📌 Summary & Learning Outcome

Successfully completing the Krypton wargame strengthened foundational cryptographic and binary analysis skills. Practical exposure to substitution ciphers, brute-force logic, and static analysis provided real-world insight into how encrypted data can be approached and solved methodically.